

Corporation for National & Community Service Policies and Procedures

Policy Number: CIO 2007-001

Effective Date: June 1, 2009

Revision Number: 3

Subject: Information Security Policies

1. Purpose: The Federal Information Security Management Act of 2002 (P.L. 107-347) and Office of Management and Budget (OMB) Circular A-130 require the Corporation to establish a fully integrated security program to ensure Corporation management and staff practice responsible and accountable risk management in all aspects of the Corporation's business processes. This policy sets forth the basic information security program components, identifies areas of vital responsibility, process integration, and communicates key program compliance requirements.
2. Who is Covered: All persons who have access to or use Corporation information resources.
3. Policies Cancelled:
 - a. CIO-2006-001, Information Security Program/Policy
 - b. OAMS-06-001, Safeguarding Sensitive Information and Documents
 - c. Policy Number 375: Internet and E-mail Access and Acceptable Use
 - d. Policy Number 376: Network and Computer Security
 - e. All other previous CNCS/OIT policies regarding information security
4. Originating Office: Office of Information Technology.
5. Location of Revised Text:
 - a. 2009 Revisions (Revision 3):
 1. Updated Effective Dates and revision dates on all policies.
 2. ISP-C-01, Access Control, section 4(k), Modified session timeout requirements.
 3. ISP-C-01, Access Control, section 4(m), Added session authenticity control requirement.
 4. ISP-C-01, Access Control, section 4(n), Added requirement for access to privileged functions.
 5. ISP-C-02, Identification and Authentication, section 5, updated Roles and Responsibilities.
 6. ISP-C-04, Access Tokens, section 4(e), Replaced "periodically" with "in accordance with CNCS audit trail policies"
 7. ISP-C-05 renamed from "Audit Trails" to "Audit Trails & System Monitoring", and added system monitoring requirement - section 4(h).
 8. ISP-C-05, Audit Trails & System Monitoring, sections 4(d) and 5(b), Added requirements for development of audit trail operating procedures.
 9. ISP-C-05, Audit Trails & System Monitoring, section 5, Removed CISO review of audit logs.
 10. ISP-C-06, Personnel Security, section 5, updated Roles and Responsibilities.
 11. ISP-C-07, Physical and Environmental Security, section 4(g)(5) "Periodic" reviews modified to monthly.
 12. ISP-C-08 Backup and Recovery, section 4(f), "Periodic" testing modified to at least annually.

13. ISP-C-10, Asset Management, section 5, updated roles and responsibilities.
14. ISP-C-11, Media Management, section 5(b)(2), updated roles and responsibilities
15. ISP-C-11, Media Management, section 2, clarified scope to exclude hard drives installed inside computers.
16. ISP-C-14, Emerging Threat Defense, section 4(l), Added requirements for restricting use of mobile code.
17. ISP-C-15, Encryption, section 4(d), modified key management requirement to include automated mechanisms.
18. ISP-P-08, Perimeter Protection, section 5(b)(1), Added requirement to develop procedures for monitoring and auditing.
19. ISP-P-10, Certification and Accreditation, section 4(f), Added requirements for annual testing of security controls.
20. ISP-P-11, Contingency Planning, section 4(g)(1), Added annual training to testing requirement.
21. ISP-P-12, Information Privacy, section 5(g)(2), Changed “periodically” to annual requirement.
22. ISP-S-02, Network Security, section 4(o) & 4(p), Added requirements to prevent denial of service and protect confidentiality and integrity of information transmitted on the network.
23. ISP-S-02, Network Security, section 4(q), Added DNS requirements.
24. ISP-S-04, Workstation Security, section 4(k), added prohibition against remote activation of collaborative computing devices.
25. ISP-S-04, Workstation Security, section 4(l), added requirement fro FDCC compliance.
26. ISP-S-05, Web Security, section 4(h), Added requirement to protect the integrity and availability of publicly accessible information.
27. ISP-S-08, Remote Access, section 2, Clarified scope of policy to only apply to non-public-facing systems.
28. ISP-S-08, Remote Access, section 4(b), Added requirement for authorization of personnel for remote access.
29. ISP-S-08, Remote Access, section 4(c) & 4(d), Added requirements for the types of systems and applications that can be accessed remotely.
30. ISP-S-11, Application Security, Sections 4(h),4(i), 4(j), Added error handling, information remnance, and application partitioning requirements.
31. ISP-S-12, External Systems, section 4(c), Modified MOU requirement to only apply to systems with interconnections and replaced the content requirements with reference to NIST SP 800-47.
32. Added new policy ISP-C-18, System Maintenance.
33. Changed “Procedures and Guidelines” heading to “Requirements” to eliminate confusion.
34. Updated references to NIST publications (throughout policies).
35. Propagated above changes to the ISP Handbook.

b. 2008 Revisions (Revision 2):

1. Updated Effective Dates and revision dates on all policies.
2. ISP-P-01 Information Security Governance and Reporting section 5(d) clarified System Owner responsibilities regarding Plans of Actions & Milestones (POA&Ms).
3. ISP-P-02 Security Training & Awareness section 4(b)(9) clarified requirement for system owners to provide security training for their system.
4. ISP-P-04 Incident Response section 4(h) added that level of response would be tailored to nature and severity of incident.
5. ISP-P-04 Incident Response section 5(a)(5) added CISO responsibility for convening response team.
6. ISP-P-04 Incident Response section 5(c)(2) added responsibility for supervisors to ensure cooperation of their staff with investigations
7. ISP-P-07 System Categorization section 2 updated scope
8. ISP-P-09 System Security Plans section 4(a) revised requirement for minor applications so that they can be included in SSPs for other systems instead of requiring their own separate SSP.
9. ISP-P-09 System Security Plans section 4(e) updated labeling requirement for SSPs.
10. ISP-P-09 System Security Plans section 5(c) updated CISO responsibilities for SSPs.
11. ISP-P-10 Certification & Accreditation section 4(c) & (d) updated requirements for Designated Approving Authorities (DAAs) and Certification Agents (CAs).

12. ISP-P-10 Certification & Accreditation section 4(g)(4) and 4(k)(3) updated requirements Certification documentation.
13. ISP-P-10 Certification & Accreditation section 5 updated System Owner, ISSO, and DAA C&A responsibilities.
14. ISP-P-11 Contingency Planning section 5 updated PSO & CISO COOP responsibilities.
15. ISP-P13 Acceptable Use User Rules of Behavior agreement updated to include affirmation that individual has completed the new user security training.
16. ISP-P13 Acceptable Use User Rules of Behavior agreement updated to include additional selections for type of staff.
17. ISP-C-01 Access Controls section 4(j) updated to specify access review period must be at least quarterly and involve System Owners.
18. ISP-C-02 Identification & Authentication section 4(b) updated to include more detail in requirement for account management procedures.
19. ISP-C-02 Identification & Authentication section 4(h) added requirement for session inactivity timeout.
20. ISP-C-06 Personnel Security section 5(f) updated OHC responsibilities.
21. ISP-C-07 Physical & Environmental Security section 5(f) added Administrative Services responsibilities.
22. ISP-C-12 Systems Development LifeCycle Security section 4(b)(2) added reference to systems acquisition policy.
23. ISP-C-13 Change Control section 4(e) added referenced to document management requirements for system changes.
24. Added new policy ISP-C-17 System & Services Acquisition
25. ISP-S-07 Mobile Computing section 4(f) updated requirement for encrypting data on mobile devices.
26. ISP-S-07 Mobile Computing section 4(g) added reference to remote access policy.
27. ISP-S-08 Remote Access section 4(a) updated authentication requirement.
28. ISP-S-11 Application Security section 4(g) added requirement for labeling reports containing sensitive data.
29. Added new policy ISP-S-14 Networked Copier Security
30. Propagated above changes to the ISP Handbook
31. Added additional physical security guidance to section 2.8
32. CNCS Information Security Policies section 8 updated to include the two new policies (ISP-S-14 and ISP-C-17 – see above)
33. CNCS Information Security Policies Appendix C updated to reflect current staff assignments to key roles.

6. Attachments:

- a. CNCS Information Security Policies
- b. CNCS Information Security Program (ISP) Handbook

Corporation employees can access this document electronically at intranet.cns.gov

Approved By:

[signed version on file with CEO and CIO]

Nicola Goren, Chief of Staff

If you need this document in an alternative format, please contact the Administrative Services Help Desk at 202/606-7504 (voice) or 202/565-2799 (TTY). You may also send an e-mail to ashelp@cns.gov or write: Corporation for National Service, Office of Administrative and Management Services, 1201 New York Avenue N.W., Washington D.C. 20525.

1. What does this document do?

This document provides Corporation staff with guidance about information security policies. These policies ensure that CNCS uses the required security methods to protect Corporation information technology assets. Federal laws and regulations require us to have these policies.

You must comply with this policy if you have access to and/or use Corporation systems and/or computer resources.



Corporation for National & Community Service
Office of Information Technology

INFORMATION SECURITY
POLICIES

May 2009

TABLE OF CONTENTS

1	INTRODUCTION	2
2	OBJECTIVES	3
3	SCOPE	3
4	GUIDING PRINCIPLES	4
5	REQUIREMENTS	5
5.A	Federal Government Requirements.....	5
5.B	CNCS Business Requirements.....	6
6	POLICY FRAMEWORK	14
6.A	Hierarchy	14
6.B	Policy Numbering	15
6.C	Policy Structure.....	15
7	INFORMATION SECURITY ROLES AND RESPONSIBILITIES.....	16
7.A	General Information Security Roles.....	16
7.B	Designated Roles	17
8	POLICIES	23
9	APPENDIX A: FEDERAL REQUIREMENTS.....	26
10	APPENDIX B: ACRONYMS AND ABBREVIATIONS	38
11	APPENDIX C: ROLE ASSIGNMENTS	39
12	APPENDIX D: INFORMATION SECURITY POLICY DOCUMENTS	40

1 INTRODUCTION

Information is critical to performing CNCS' mission. CNCS information, in all its forms and throughout its life cycle, must be protected through information management policies and actions that meet applicable federal regulatory requirements and support the Corporation's mission, vision, and values. Measures must be taken to protect CNCS' information resources from unauthorized disclosure, alteration, or destruction (DAD), whether accidental or intentional.

"The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to mission performance for ... government agencies... even as dependence on information technology has grown, so too has the vulnerability of this technology and the range of external threats to it...IT resources also consume a growing share of the Federal budget and are becoming increasingly important to daily life. As a result, a considerable body of applicable policy is in place, consisting of laws, statutes, regulations, Executive Orders, and other directives. [CNCS'] IT Security Program, as well as those of other agencies, must operate within this complex policy landscape to ensure that the Government meets its obligations to the Nation. Providing for the security of IT resources is not only a difficult technical challenge, it is also a human challenge. Ultimately IT security is a human endeavor that depends heavily on the behavior of individual people."¹

CNCS' Information Security Program (ISP) establishes policies and procedures, and designates responsibilities and authorities, for ensuring an adequate level of information security for all information collected, created, processed, transmitted, stored, or disseminated on the agency's information systems. As part of the ISP, there must be explicit and well-defined security policies that establish requirements for minimum safeguards, assign roles and responsibilities, provide accountability, and address penalties for noncompliance.

"Information security investment is pointless without an effective policy. Organizations must adopt a structured framework for policy definition using an inclusive policy management process that enables policies derived from business requirements... Failure to develop a meaningful security policy that maps to business risk seriously compromises the ability to develop effective security solutions and could expose the organization to potentially catastrophic breaches."²

This enterprise information security policy document describes the policies, standards, guidelines, and procedures that CNCS will follow to safeguard its information resources and ensure consistency with government-wide policies and standards.

¹ *GSA Security Action Plan*

² *META Group, Making Information Policy Effective, July 2002*

2 OBJECTIVES

The purpose of this information security policy document is to identify and disseminate the principles and framework that guide the secure use of information usage at CNCS. Specifically, this document discusses:

- The principles on which the information security program at CNCS is based
- Federal regulations and standards with which CNCS must comply
- CNCS business-driven security requirements
- The information security policy framework to be used at CNCS
- The set of CNCS information security policies to be implemented to provide an appropriate level of security to protect CNCS information and information systems.

3 SCOPE

The policies in this document define the minimum set of security requirements for protecting CNCS' information systems and complying with applicable regulations.

CNCS information security policies apply to everyone who uses or has access to CNCS' information assets, including employees, contractors, customers, vendors, volunteers, and visitors. All of these personnel are responsible for understanding and complying with these policies.

The policies apply to the use of all CNCS information resources regardless of time or location. Additionally, they apply to the use of any other information resources used by personnel during CNCS work hours.

4 GUIDING PRINCIPLES

The development of CNCS' information security policies is driven by the following principles:

- CNCS must fully comply with all applicable regulations and federal guidelines regarding information security.
- CNCS' information resources are critical to its mission and worth protecting.
- Information security should support CNCS' mission and business needs.
- CNCS is committed to protecting the private information entrusted to the Corporation by its customers and partners.
- Information security is an essential component of sound IT management.
- CNCS' security program will focus on managing risk effectively and cost efficiently by employing industry best practices.
- Information security is the responsibility of all CNCS information users and can only be successfully achieved through communication and cooperation.
- CNCS' information security policies, procedures, and guidelines should be periodically reassessed to ensure continued effectiveness.
- A comprehensive and integrated approach is required to provide effective information assurance.
- The information security protections used by CNCS shall be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that are operated, maintained, or sponsored by the agency.

5 REQUIREMENTS

As a federal government corporation, CNCS faces a variety of security threats and must comply with a plethora of federal requirements. CNCS must protect customer information, employee data, and its own corporate assets as any corporation would, while also meeting federal government information security mandates such as FISMA, OMB requirements, and presidential directives. Therefore, CNCS' information security program, and the policies that guide it, must address both the business and government agency aspects of CNCS' security needs. The following sections will discuss each of these sets of requirements. The combined set of these requirements forms the basis for CNCS' information security policies.

5.A Federal Government Requirements

CNCS is subject to a variety of federal security requirements, including government regulations, federal standards, and the mandates of oversight agencies. These include, but are not limited to, the following, which are described in more detail in Appendix A:

- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, *Security of Federal Automated Information Resources*
- Privacy Act of 1974, as amended
- Freedom of Information Act
- Clinger-Cohen Act of 1996
- Homeland Security Presidential Directive 7, *Critical Infrastructure Protection*
- Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.
- Computer Abuse Amendments Act of 1994
- Computer Security Act of 1987, PL 100-235, January 8, 1988.
- Computer Fraud and Abuse Act of 1986
- Office of Management and Budget (OMB) Memoranda
- National Institute of Standards and Technology (NIST) Guidance
- Health Insurance Portability and Accountability Act (HIPAA)
- Hatch Act
- Inspector General Act, 5 U.S.C. App 3.
- Federal Managers' Financial Integrity Act of 1982 (31 USC 3512 and 31 USC Ch .11).
- OMB Circular A-123, "Management Accountability and Controls," June 21, 1995.

- OMB Circular A-127, “Financial Management Systems,” July 23, 1993.

5.B CNCS Business Requirements

“The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets... Security, therefore, is a means to an end and not an end in itself. To act on this, managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission.”³

5.B.I CNCS Business Environment

The Corporation for National and Community Service (CNCS) is an independent federal agency. The Corporation has a Board of Directors and Chief Executive Officer appointed by the President and confirmed by the Senate. The Chief Executive Officer oversees the agency, which includes about 600 employees operating throughout the United States and its territories. CNCS is headquartered at 1201 New York Avenue, N.W. in Washington, D.C. which is a mixed use facility containing both federal government and commercial businesses.

CNCS was established in 1993 to connect Americans of all ages and backgrounds with opportunities to give back to their communities and their nation. The mission of CNCS is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. CNCS provides grants and training and technical assistance to developing and expanding volunteer organizations. In addition, the Corporation explores, develops, and models effective approaches for using volunteers to meet the nation's human needs and conducts and disseminates research that helps develop and cultivate knowledge that will enhance the overall effectiveness of national and community service programs.

5.B.II Critical Information Assets

CNCS has various critical assets and sensitive information to protect, including:

- Personnel – federal employees, contractors, interns, members, grantees, etc.
- Property – facilities and office space, physical plant, furniture, etc.
- Data / Information – vital records, sensitive and protected information, etc.

³ NIST Special Publication 800-12 “An Introduction to Computer Security: The NIST Handbook”, p. 11

- Equipment – hardware, infrastructure, mobile devices, etc.
- Software – desktop software, business applications, data management programs, etc.

All of these assets are vital to the continued operational viability and success of CNCS.

Of particular interest to the CNCS Information Security Program is the security and viability of CNCS' critical data and information assets, which include the following categories:

- **Program and Legal Information** is essential for CNCS to carry out its programmatic and legal functions and activities and to protect the U.S. government and the legal and financial rights of CNCS' customers. Examples include client information; grant documentation; working documents; legal agreements; and FOIA information.
- **Financial Information** is essential for CNCS to carry out its financial functions and activities. Examples include accounts payable information, fixed assets, general ledger, grant information, budget and travel information.
- **Administrative Information** is used by CNCS to effectively meet its mission requirements in compliance with existing laws, rules and regulations. Examples include interagency agreements; strategic plans and business plans; management directives and administrative orders; and procurement information.
- **Personnel Information** is necessary for CNCS to administer human resources programs, including compensation and benefits. Examples include payroll information; benefits information; retirement information; time and attendance information; and program information (*e.g.*, staffing, employee relations, etc.).
- **Corporate Governance Information** represents the thinking behind CNCS' major mission and policy decisions and program direction. Examples include the CNCS Board of Directors by-laws; Board meeting minutes; and Board resolutions.
- **Emergency Operating Information** is essential to the continued function or reconstitution of CNCS during and after an emergency. Examples include continuity plans; orders of succession; disaster recovery plan; vital records manual; building plans.
- **Information From Other Federal Agencies** is information that CNCS is privy to in order to carry out its duties to support the goals of the Administration. Examples include White House guidance; Homeland Security/FEMA information; etc.
- **Member/Grantee Information** is collected and used to screen applicants, manage grants, operate programs, and carry out the Corporation's mission. Examples include: social security numbers, contact information, background investigations, medical data, etc.

5.B.III Areas of Risk

“Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of trusted users defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.”⁴ [Table 5-1](#) shows the potential harm or damage that could result from threats to CNCS’ critical information systems:

Table 5-1: Potential Risks to CNCS Information Resources

Critical Information Resource	Potential Harm or Damage
Program and Legal Information	Legal and Financial Liability; Disclosure of Sensitive Data; Loss of Client Confidence; Inability to Perform Mission
Financial Information	Financial loss; Loss of Assets; Disclosure of Sensitive Data; Inability to Perform Mission; Scrutiny by OMB and Congress
Administrative Information	Inability to Perform Mission (Effectively); Disclosure of Sensitive Data
Personnel Information	Financial/Legal Liability; Disclosure of Privacy Act protected information; Loss of Employee Confidence; Scrutiny by OPM;
Corporate Governance Information	Financial /Legal Liability; Loss of Client Confidence; Disclosure of Sensitive Information
Emergency Operating Information	Disclosure of Sensitive Information; Inability to Perform Mission
Information From Other Federal Agencies	Disclosure of Sensitive Data; Loss of Other Agency Confidence
Member/Grantee Information	Financial/Legal Liability; Disclosure of Privacy Act protected information; Loss of Client Confidence; Inability to Perform Mission

Formatted
 Deleted:
 Formatted
 check spel
 Formatted

⁴ NIST Special Publication 800-12 “An Introduction to Computer Security: The NIST Handbook”, p. 25

The primary goal of the CNCS Information Security Program is to mitigate these threats and vulnerabilities by preventing them or reducing their impact when they occur. Without a comprehensive security program, customized to CNCS' specific needs and environment, CNCS is exposed and vulnerable to losing its ability to perform its mission, and may risk liability for not protecting the resources with which it has been entrusted.

CNCS needs to understand the risks and vulnerabilities of its information resources in order to apply cost effective measures to protect them. This section provides a general description of the risks that threaten CNCS' information resources⁵. This information can then be used to determine the information security policies that are needed by CNCS.

CNCS faces a variety information security threats, ranging from terrorist acts to employee theft to accidental exposure/alteration of data. Inherent vulnerabilities also exist in the corporate assets themselves. [Figure 5-1](#) illustrates some of the threats that exist to CNCS information systems. Each of these threats and vulnerabilities, when targeted at CNCS-critical assets, can have a serious impact on the ability of CNCS to perform its mission.

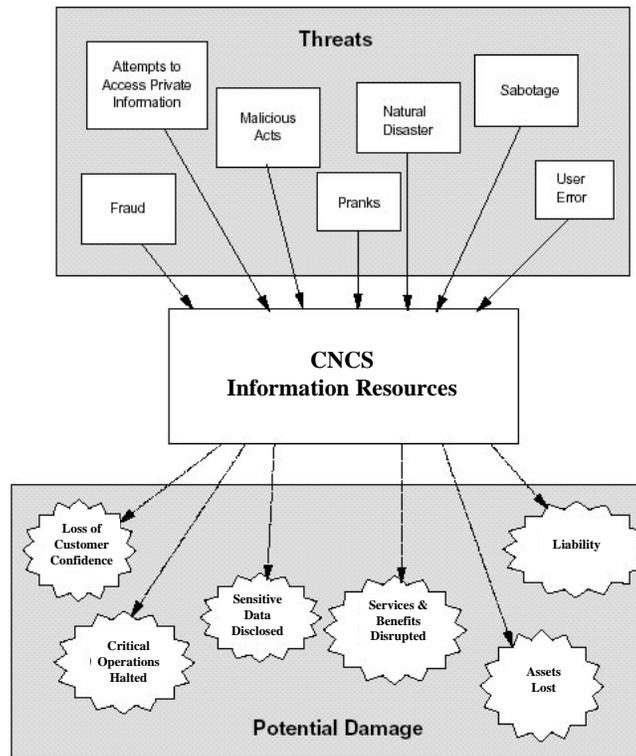


Figure 5-1: Information Security Threats

⁵ This is not intended to be an exhaustive list of all risks to CNCS resources.

Formatte
 Deleted:
 Formatte
 check spel
 Formatte

5.B.III.a Errors and Omissions

One of the most common threats to information security is errors and omissions. Everyone at CNCS is at risk of unintentionally making an error that contributes directly or indirectly to security problems. Examples include incorrect data entry, accidental deletion or modification of data, programming mistakes (*i.e.* “bugs”), system administration errors, and inadvertent overloading of the system. These can compromise all three aspects of information security – confidentiality, integrity, and availability.

To combat this threat, it is imperative that CNCS implement the following measures as part of its information security program:

- Information users must receive adequate security awareness training so they can help CNCS reduce the number and severity of errors and omissions.
- Quality control measures must be implemented for information systems, wherever feasible, to guard against these conditions. This includes both technical and procedural validation and verification techniques.
- Standardized procedures should be implemented for IT management and programming functions to reduce potential errors throughout the system lifecycle.
- Procedures for reporting and correcting errors need to be implemented.
- Changes made to systems must be performed in a carefully controlled and documented manner.

5.B.III.b Fraud and Theft

CNCS’ information resources are susceptible to fraud and theft, both from insiders and outsiders. Not only are the resources themselves at risk of being stolen, but they can also be used to commit these acts against other entities and resources. Insiders may try to steal resources (both equipment and data) for personal use, modify data (such as records in the time and attendance systems), use computers to skim money from financial accounts, commit Internet fraud, or misuse these resources in other illegal ways. Outsiders may also steal money, illegally acquire data, or use CNCS’ resources to commit fraud. Because insiders are statistically responsible for the majority of computer fraud, and have both access to and familiarity with CNCS systems, they are actually the greater threat to CNCS’ information resources.

To guard against fraud and theft, CNCS needs to implement a variety of safeguards, including:

- Define rules of behavior for using CNCS resources (*i.e.* “appropriate use”).
- Educate users on information security policies and the penalties for violating them.
- Ensure that all access to information resources requires identification and authentication of the user, to provide accountability for all system activities.

- Implement audit trails to detect and track fraud and theft.
- Control access to resources to only those who need them to perform their duties.
- Implement personnel security procedures, such as background screening and separation of duties.
- Deploy perimeter protections to safeguard resources from external entities who may want to steal them or use them for fraudulent purposes.
- Implement procedures for prompt removal of access rights for terminated personnel.
- Safeguard mobile computing devices.
- Implement procedures for reporting and responding to incidents of fraud and theft.
- Control physical access to critical information resources (such as the computer room).
- Establish Information Privacy policies and procedures.

5.B.III.c Employee Sabotage

Employee sabotage is less common than fraud or theft, but the cost of such incidents is generally much higher. Common examples of sabotage include deliberate acts of destruction or damage of equipment, deletion or incorrect modification of data, crashing of systems, and distribution of viruses and other malicious programs. Such activities are generally performed by personnel who feel betrayed, cheated, bored, or harassed, particularly those with low job satisfaction or who have been terminated.

Safeguards for the threat of employee sabotage are similar to those for theft and fraud:

- Define rules of behavior for using CNCS resources (*i.e.* “appropriate use”).
- Educate users on information security policies and the penalties for violating them.
- Ensure that all access to information resources requires identification and authentication of the user, to provide accountability for all system activities.
- Implement audit trails to detect and track employee sabotage.
- Control access to information resources to only those who need access to perform their duties.
- Implement personnel security procedures, such as background screening and separation of duties.
- Control physical access to critical information resources (such as the computer room).
- Implement procedures for prompt removal of access rights for terminated personnel.
- Deploy change control measures to protect systems against unauthorized modification.
- Implement procedures for reporting and responding to incidents of fraud and theft.

5.B.III.d Loss of Physical and Infrastructure Support

CNCS' facilities are susceptible to disruptions such as utility failures, fires, floods, terrorist acts, and other situations that may affect the availability of critical infrastructure components. These conditions often result in system downtime.

To mitigate these threats, CNCS needs to:

- Perform disaster recovery and continuity of operations planning.
- Implement physical and environmental security measures, such as fire alarms and backup power.
- Build redundancy into critical infrastructure components, such as network and telephony resources.
- Implement procedures for reporting and responding to physical/infrastructure loss incidents.

5.B.III.e Malicious Hackers

Malicious hackers are people who break into computers without authorization, and may be either outsiders or personnel internal to CNCS. Hackers may have a variety of intentions, including accessing sensitive information, causing damage to systems, theft, modifying data, and causing a denial of service.

To combat hackers, CNCS must address the following security considerations:

- Implement perimeter protections and network security tools to keep unauthorized persons out of the CNCS network.
- Control physical and logical access to CNCS information resources.
- Configure servers and systems according to security standards (baselines) to minimize risk of being hacked (hardening)
- Implement procedures for deploying system updates and security patches in a timely fashion.
- Secure remote access and mobile computing from access by unauthorized persons.
- Utilize encryption and other measures to secure wireless communications.
- Deploy audit trails to track system access.
- Implement procedures for reporting and responding to hacking incidents.

5.B.III.f Malicious Code

One of the most prevalent threats to CNCS information resources is malicious code. This includes viruses, worms, spyware, and other "uninvited" software. Malicious code may be distributed through email, web scripts, software installations, infected data files, and other methods. Affects range from minor annoyance to loss of data or the incapacitation of systems.

To minimize the effects of malicious code, CNCS needs to:

- Deploy antivirus software that can detect and stop viruses and other malicious code
- Employ firewalls, email filters and other tools to limit such code from entering CNCS
- Educate users about how to avoid allowing malicious code into CNCS' environment.
- Carefully control the installation of software within CNCS
- Configure servers and workstations according to security standards (baselines)
- Implement procedures for timely deployment of system updates and security patches
- Implement procedures for reporting and responding to malicious code incidents
- Integrate security into systems development and change control to reduce vulnerabilities

5.B.III.g Threats to Personal Privacy

CNCS has access to a variety of personal information, such as employee payroll and contact information, member social security numbers and medical histories, etc. This information is susceptible to theft and misuse. In addition to providing protection mandated by the Privacy Act, CNCS has an obligation to protect the information it requests from or creates about employees and other individuals. Threats to personal privacy may arise from both insiders and outsiders who wish to sell the information, use it to commit fraud, or simply satisfy curiosity.

In order to protect personal private information, CNCS needs to:

- Develop an Information Privacy program
- Categorize data and protect it in accordance with level of sensitivity
- Utilize encryption to secure sensitive information in transmission and in storage
- Control physical and logical access to information
- Secure remote access and mobile computing from access by unauthorized persons
- Implement procedures for protection of media containing sensitive data
- Deploy audit trails to track system access
- Implement procedures for reporting and responding to privacy violation incidents

6 POLICY FRAMEWORK

Generally speaking, policies are broad statements that summarize management decisions regarding security issues. They provide the basic rules for operating securely within a specific environment. Policies serve to describe what information resources the agency wants to protect. To provide flexibility for use in different systems and situations, policies do not dictate specific technologies or configurations.

Because policies are very high level, CNCS also needs to develop standards, guidelines, and procedures that further define the requirements of the policies and provide guidance on how to implement them.

- *Standards* specify the use of particular technologies, procedures, or configurations in particular situations, and are compulsory. (For example, a standard might be that all Windows XP workstations have specific security settings configured in a certain way.)
- *Guidelines* are recommendations that are meant to assist personnel with complying with policy and effectively securing their resources.
- *Procedures* are specific repeatable instructions for completing a particular process (such as the detailed steps for configuring a server or the process for granting access rights to new employees).

6.A Hierarchy

To facilitate their development, administration, and maintenance, CNCS' information security policies have been organized into a logical hierarchy. As CNCS' information security needs evolve, individual policies may be added or removed from this organizational structure.

The policies and are divided into three primary categories:

- *Security Program* – These policies provide guidance for development and operation of the core components of CNCS' information security program, and are derived from FISMA program requirements.
- *Systems/Information Resources* – These policies provide guidance on securing specific types of information resources, such as servers, applications, databases, and connectivity components.
- *Security Practices* – These policies provide guidance on implementation and operation of security protections that apply across all information resources.

6.B Policy Numbering

Each policy is assigned a unique policy number in the following format:

ISP-A-XX-YYMM

ISP designates the policy as part of the Information Security Program.

A is either 'P' for Program, 'S' for System/Resource, or 'C' for Control

XX is a unique number assigned to each policy.

YYMM is the date that the specific version of the policy was issued.

6.C Policy Structure

The policies are structured to contain the following information:

<i>Policy Name</i>	Formal name of the policy.
<i>Policy Number</i>	Identification number assigned to the policy (see section 6.B).
<i>Subject</i>	Policy statement summarizing the intention of the policy.
<i>Scope</i>	Specification of to whom or what the policy applies.
<i>Description</i>	Explanation of the purpose of the policy.
<i>Requirements</i>	Narrative stating the specific requirements and directions of the policy. This includes any procedures, standards, and guidelines that must be followed in order to be compliant with the policy.
<i>Roles & Responsibilities</i>	Discussion of responsibilities that apply to each information security role for complying with the policy. Not all roles will have responsibilities for all policies.
<i>Definitions</i>	Defines key terms used in the policy.
<i>Enforcement</i>	Describes the potential penalties for non-compliance with the policy.
<i>Point Of Contact</i>	Specifies the person to contact for additional guidance or questions about the policy.
<i>Attachments</i>	Lists any associated documents that are incorporated into the policy by reference.
<i>Authority</i>	Enumerates the federal laws, regulations, standards, and other authoritative requirements from which the policy is derived.
<i>Effective Date</i>	Specifies the date when the policy goes into effect.
<i>Revision History</i>	Lists any revisions that have been made to the policy document.
<i>Review Schedule</i>	Species the frequency with which the policy should be reviewed for potential revision.

7 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Everyone at CNCS has a role in maintaining the security of our information resources. All employees, contractors, and other staff have an obligation to maintain awareness and exercise due diligence in protecting the CNCS resources with which they have been entrusted.

However, there are specific information security duties that apply to each person depending upon their role within the organization. These roles and responsibilities are described in the following sections.

7.A General Information Security Roles

For the purpose of assigning security responsibilities, some general roles have been defined. Each policy specifies the particular responsibilities that are assigned to each of these roles as applicable.

Individuals may serve in multiple roles for different aspects of their jobs. For example, a Program Director may serve as an Information Owner for a particular resource, as a Manager for the employees in his/her department, and as a User of information resources.

The roles specified in the CNCS' information security policies are defined as follows:

- Information Users are individuals who use or have access to CNCS' information resources, including employees, interns, temporary workers, contractors, vendors, and visitors. All individuals who use CNCS information resources are responsible for protecting the resources entrusted to them and complying with CNCS information security policies and procedures.
- Supervisors are employees who have some kind of supervisory relationship over other staff. This can include managers, COTRs, visitor escorts, etc. Supervisors help ensure that their staff understand their security responsibilities, comply with CNCS policies, and maintain security awareness. Supervisors are also responsible for helping to enforce policies and taking appropriate action when there are policy violations. It is crucial that Supervisors serve as a good example for their employees to follow.
- Information Owners are the individuals ultimately responsible for specific information resources. Information/System Owners are usually managers or directors who own resources on behalf of their departments. It is the information owner's responsibility to ensure that the resources they own are compliant with CNCS information security policies and procedures. Information Owners must be federal staff.
- Information Custodians are individuals who maintain or administer information resources on behalf of Information Owners. All individuals who design, develop, maintain, or

administer a CNCS information system or the data it contains are responsible for protecting the CNCS resources under their control and complying with CNCS information security policies and procedures. These individuals can be CNCS employees, contractors, or other kinds of staff.

7.B Designated Roles

In addition to the general roles described above, there are individuals at CNCS who have been assigned additional responsibilities regarding the safeguarding of Corporation information resources. These are derived from NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers, and other relevant guidance. These special roles and their responsibilities are as follows. A list of current assignees at the time of policy issuance is included in Appendix C.

7.B.I Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) of CNCS is responsible for ensuring that “that the information security policies, procedures, and practices of the executive agency are adequate.”

Under FISMA, the CEO is responsible for:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization;
- Ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization’s mission;
- Ensuring that senior agency officials within the organization are given the necessary authority to secure the operations and assets under their control;
- Designating a CIO and delegating authority to that individual to ensure compliance with applicable information security requirements;
- Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines; and

- Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.

7.B.II Chief Information Officer (CIO)

The Chief Information Officer (CIO) oversees the programs of the Office of Information Technology in order to design, develop and implement comprehensive corporate information systems. The CIO plans the nature and extent of IT operations and activities for CNCS, and ensures that IT management directly supports CNCS' strategic mission. The CIO promotes a coordinated, interoperable, secure and shared corporate IT infrastructure. Additionally, the CIO serves as a corporate-wide resource for major policy, program, or operational initiatives, and provides advice on technical information technology issues that may impact the creation and maintenance of cooperative agreements with customers and stakeholders.

Per the Federal Information Security Management Act (FISMA) and OMB implementing directives, the CIO monitors, evaluates and reports the status of information security within the Agency to the Chief Executive Officer (CEO) of CNCS.

Under FISMA, the CIO has the following responsibilities:

- Designating a senior agency information security officer (SAISO);
- Developing and maintaining an agency-wide information security program;
- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;
- Ensuring compliance with applicable information security requirements; and
- Reporting annually, in coordination with the other senior agency officials, to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

7.B.III Chief Information Security Officer (CISO)

The CISO reports to the CIO and is responsible for developing, implementing and maintaining an information security program within CNCS. The CISO ensures the confidentiality, integrity and availability of information and information systems through formal policies, awareness training, monitoring compliance and access controls. The CISO identifies and assesses risk, explores controls and countermeasures, provides recommendations to senior management,

develops and obtains senior management approval of policies and procedures, and implements approved policies and procedures.

As the senior agency information security officer, the CISO has the following responsibilities under FISMA:

- Performing information security duties as the primary duty;
- Heading a team with the mission and resources to assist in ensuring agency compliance with information security requirements;
- Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- Developing and maintaining risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each agency information system to ensure compliance with applicable requirements;
- Facilitating development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- Ensuring that agency personnel, including contractors, receive appropriate information security awareness training;
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
- Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices;
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- Developing and implementing procedures for detecting, reporting, and responding to security incidents;
- Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of the agency; and
- Supporting the agency CIO in annual reporting to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

7.B.IV Privacy Officer

The Privacy Officer is responsible for privacy compliance across an organization, including privacy compliance measures that apply to information security assets and activities. The chief privacy officer works to maintain a balance between security and privacy requirements, and works to ensure that one is not compromised for the sake of the other. To this end, the chief privacy officer serves as the senior official responsible for:

- Developing, promoting, and supporting the organization's privacy programs;
- Encouraging awareness of potential privacy issues and policies; and
- Reviewing and implementing privacy regulations and legislation

7.B.V Information System Security Officers (ISSOs)

- Information System Security Officers (ISSOs) are designated by the System Owners for each major system. An ISSO's responsibilities include defining security policies and procedures for the system, providing security training to system users, assisting with Certification and Accreditation of the system, ensuring that system contingency plans are developed and periodically tested, and performing on-going security reviews of the system.

7.B.VI Physical Security Officer

The facility security officer is responsible for the overall implementation and management of physical security controls across an organization, to include integration with applicable information security controls. As information security programs are developed, senior agency officials should work to:

- Ensure this coordination of complementary controls. In consideration of information security, the physical security officer serves as the senior official responsible for:
- Developing, promulgating, implementing, and monitoring the organization's physical security programs, to include appropriate controls for alternate work sites;
- Ensuring organizational implementation and monitoring of access controls (i.e., authorization, access, visitor control, transmission medium, display medium, logging)
- Coordinating organizational environmental controls (i.e., ongoing and emergency power support and backups, fire protection, temperature and humidity controls, water damage); and
- Overseeing and managing controls for delivery and removal of assets.

7.B.VII Personnel Security Officer

The personnel security officer (Director of Personnel Security) is responsible for the overall implementation and management of personnel security controls across CNCS, to include integration with specific information security controls. In consideration of information security, the personnel security officer serves as the senior official responsible for:

- Developing, promulgating, implementing, and monitoring the organization's personnel security programs;
- Developing and implementing position categorization (including third-party controls), access agreements, and personnel screening, termination, and transfers; and
- Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

7.B.VIII Contracting

The Acquisitions/Contracting function is responsible for managing contracts and overseeing their implementation. Personnel executing this function have the following responsibilities in regards to information security:

- Collaborating with the CNCS CISO or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements;
- Coordinating with the CISO or other appropriate official as required to ensure that all agency contracts and procurements are compliant with the agency's information security policy and contain appropriate information security and privacy clauses;
- Ensuring that all personnel with responsibilities in the agency's procurement process are properly trained in information security; and
- In concert with the CISO, facilitating the monitoring of contract performance for compliance with the agency's information security policy.

7.B.IX Chief Enterprise Architect

The chief enterprise architect or comparable position in an organization is responsible for:

- Leading agency enterprise architecture development and implementation efforts;
- Collaborating with lines of business within the agency to ensure proper integration of lines of business into enterprise architecture;
- Participating in agency strategic planning and performance planning activities to ensure proper integration of enterprise architecture;
- Facilitating integration of information security into all layers of enterprise architecture to ensure agency implementation of secure solutions; and
- Working closely with the program managers, the CISO, and the business owners to ensure that all technical architecture requirements are adequately addressed by applying Federal Enterprise Architecture (FEA) and the Security and Privacy Profile (SPP).

7.B.X Inspector General (IG)

Office of the Inspector General (OIG) investigates, audits, and takes other action in accordance with the Inspector General Act to detect, prevent, and investigate wrongdoing. In accordance with FISMA, the OIG conducts an annual independent assessment of the CNCS information security program to assess the Corporation's security practices and identify additional security measures needed. The IG is responsible for:

- Detecting fraud or instances of waste, abuse, or misuse of an organization's funds;
- Identifying operational deficiencies within the organization;
- Ensuring that the underlying problems that permit such failings are rectified; and
- Offering recommendations for preventing problems in the future.

8 POLICIES

Based on the analysis of the information security requirements presented in section 5, CNCS has developed a set of policies to meet its information security needs. These have been developed in accordance with the framework specified in section 6. Additional policies will be defined as needs arise. The policies currently include:

Policy #	Policy Name	Summary
ISP-P-01	InfoSec Governance & Reporting	CNCS will manage and report on the status of its information security program as required by FISMA and OMB.
ISP-P-02	Security Training & Awareness	CNCS' information security policies and procedures will be communicated to all staff, and will be made available for reference and review by any other persons in a position to impact the security and integrity of CNCS information resources. A program to maintain awareness of information security policies, standards and acceptable practices will also be implemented.
ISP-P-03	Incident Reporting	Personnel are required to report any suspected security incidents in accordance with CNCS incident reporting procedures.
ISP-P-04	Incident Response	The Corporation must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.
ISP-P-05	Vulnerability Testing	In order to assess CNCS' information security posture to determine security risks that should be mitigated, CNCS will conduct periodic Vulnerability Assessments. These assessments will assist in the discovery of security vulnerabilities, determine the threat of these vulnerabilities, and assist CNCS in decreasing security risk.
ISP-P-06	Vulnerability Remediation	Vulnerabilities must be addressed in a timely fashion to minimize risk to CNCS resources. CNCS will identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response.
ISP-P-07	Information Resource Classification	All information resources (including data and systems) must be identified, categorized, and protected according to their level of sensitivity, criticality, and business "need to know".
ISP-P-08	Risk Management	CNCS must develop, implement, and maintain a risk management program to ensure that appropriate safeguards are employed to protect CNCS resources.
ISP-P-09	System Security Plans	Each major system must have an approved System Security Plan.
ISP-P-10	Certification And Accreditation	Each major system will be certified and accredited in accordance with NIST guidance.
ISP-P-11	Contingency Planning	Alternate modes of operation must exist to ensure continuity of critical services in the event of natural disaster, fire, act of terror, or other

		catastrophic event.
ISP-P-12	Privacy	CNCS needs to maintain a Privacy program that ensures the confidentiality of sensitive personal information.
ISP-P-13	Acceptable Use Of Information Resources	Individuals using information resources belonging to the Government must act in a legal, responsible, and secure manner, with respect for the rights of others.
ISP-P-14	InfoSec Policy Waivers	CNCS will have a formal process for evaluating and granting waivers to security policies.
ISP-C-01	Access Control	Access to CNCS information resources will be limited to those that need them to perform their duties. The principle of least privilege will be applied to the allocation of access rights.
ISP-C-02	Identification And Authentication	Access to CNCS information systems will only be granted to identified and authenticated users.
ISP-C-03	Password Management	CNCS will protect access to its information resources by ensuring that any passwords used for authentication are properly assigned and protected.
ISP-C-04	Access Tokens	CNCS will protect access to its information resources by ensuring that any tokens used for authentication are properly assigned and protected.
ISP-C-05	Audit Trails	Audit trails must be maintained to provide accountability and facilitate incident response.
ISP-C-06	Personnel Security	Access to CNCS information resources should be limited to only those persons who have been appropriately screened and authorized.
ISP-C-07	Physical and Environmental Security	Automated systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel.
ISP-C-08	Backup and Recovery	Recoverable backups must be maintained for CNCS information resources.
ISP-C-09	Patch Management	Systems are to be maintained with updated security patches.
ISP-C-10	Asset Management	All information assets must be tracked and managed to ensure that they are not lost or misused.
ISP-C-11	Media Management	Media must be handled, stored, and disposed of properly in order to protect the sensitive or critical data stored upon it.
ISP-C-12	Systems Development Lifecycle Security	Security will be integrated into the systems development lifecycle in order to ensure the efficient and effective implementation of appropriate safeguards.
ISP-C-13	Change Control	All changes made to CNCS information systems will be made in a controlled and coordinated fashion to preserve the confidentiality, integrity, and availability of the system.
ISP-C-14	Emerging Threat Defense	Tools and procedures must be implemented to minimize the impact of computer viruses, spyware, and other emerging threats on CNCS' information resources.
ISP-C-15	Encryption	The use of encryption at CNCS will be limited to those algorithms that have been proven to work effectively and which are approved and

		recommended for government use.
ISP-C-16	Perimeter Security	Access to CNCS systems will be protected from external threats.
ISP-C-17	System Acquisition	Security considerations and requirements must be included in the acquisition of information systems and services.
ISP-C-18	Systems Maintenance	Systems are maintained in accordance with best practices to ensure their availability, integrity, and confidentiality.
ISP-S-01	Server Security	Servers should be made secure before placing them into the CNCS operational environment, and security should be maintained throughout their lifecycle.
ISP-S-02	Network Security	Network devices and connectivity components should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
ISP-S-03	Wireless Security	When using wireless networks or handheld devices, CNCS should assess the risks involved with that technology, to take steps to reduce those risks to an acceptable level, and to ensure that the level of protection is maintained.
ISP-S-04	Workstation Security	Workstations should be made secure before placing them into the CNCS operational environment, and security should be maintained throughout their lifecycle.
ISP-S-05	Web Security	Web servers and web-based systems should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
ISP-S-06	Database Security	Information must remain consistent, complete, and accurate.
ISP-S-07	Mobile Computing	Security controls will be implemented to mitigate the increased risks posed by the use of laptops and other mobile devices outside of the CNCS office.
ISP-S-08	Remote Access	Security controls will be implemented to mitigate the increased risks posed by allowing remote connectivity into the CNCS network.
ISP-S-09	Telephony Security	CNCS' telephony resources will be protected against threats to their confidentiality, availability and integrity.
ISP-S-10	Electronic Mail	Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.
ISP-S-11	Application Security	Applications should be made secure before placing them into the CNCS operational environment, and security should be maintained throughout their lifecycle.
ISP-S-12	External Systems	CNCS must ensure the security of external systems operated on behalf of the Corporation or which provide services to the Corporation.
ISP-S-13	Emerging Technology	CNCS must assess and mitigate risks associated with any new technology prior to initiating its use at the Corporation.
ISP-S-14	Networked Copiers	Networked copiers should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.

9 APPENDIX A: FEDERAL REQUIREMENTS

9.A Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.

FISMA's goal is to improve the security of Federal information and information systems. FISMA was enacted into law as Title III of the E-Government Act of 2002 (P.L. 107-347, December 17, 2002). FISMA, along with OMB policy lays out a framework for annual IT security reviews, reporting, and remediation planning. Under this framework, the Federal government is able to quantitatively determine both IT security progress and problems. This information is essential to ensuring that remediation efforts and IT resources are prioritized, resulting in the timely resolution of IT security weaknesses.

FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. FISMA requires Federal agencies to provide risk-based information security protections for information collected as well as information systems used, operated or maintained by or on behalf of an agency. To provide this protection, FISMA requires agencies to establish risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations. FISMA requires annual independent evaluation of Federal agency information security programs and practices to determine their effectiveness, and requires each Federal agency to report to Congress annually (via OMB) by the first of March. The report must address the adequacy and effectiveness of information security policies, procedures and practices.

Under FISMA, agency information security activities, other than for classified and other national security systems, are guided by OMB policy and the development of information security standards by NIST that are to include minimum mandatory requirements by risk level. OMB (Office of E-Government) and agency responsibilities are detailed in section 301. Standards are addressed in sections 302 and 303.

FISMA requires the agency head to:

- Ensure the agency has a sufficient number of trained personnel to ensure agency-wide information assurance.
- Require annual reports from the CIO regarding the effectiveness of agency IA programs and progress on any required remedial actions.

FISMA requires the agency CIO to carry out the following responsibilities:

- Develop and maintain an agency-wide information assurance (IA) program complete with policies, procedures and control techniques to address information security requirements, including FISMA.
- Ensure that required training is conducted including annual information security training and Internet security training.
- Designate a senior official responsible of agency information security and ensure oversight of personnel with significant responsibilities for information security.
- Assist senior agency officials concerning their awareness and responsibilities for information and information system security.

Specifically, FISMA requires each Federal agency to develop, document and implement an agency-wide information security program, which includes the following:

- Periodic risk assessments.
- Risk assessment policies and procedures that cost-effectively reduce the risk to an acceptable level, ensure that information security is addressed throughout the life cycle of each agency information system and ensure compliance with FISMA.
- Subordinate plans for networks, facilities and groups of systems as appropriate.
- Security awareness training for agency personnel, including contractors and system users.
- Annual independent evaluation of the agency information security program to determine the effectiveness of such program and practices (which must include periodic but at least annual testing and evaluation of the effectiveness of information security policies, procedures and practices).
- Processes for planning, implementing, evaluating and documenting remedial action to address deficiencies in agency information security policies, procedures and practices.
- Procedures for detecting, reporting and responding to security incidents.
- Plans and procedures to ensure continuity of operations for information systems that support agency operations and assets.

Relationship to other laws/directives: FISMA was enacted with the intention of superseding earlier very similar FISMA provisions enacted into law in the Homeland Security Act (P.L. 107-296, Title X, November 25, 2002). FISMA replaces GISRA, the Government Information Security Reform provisions of the FY 2001 National Defense Authorization Act (P. L. 106-398, sec. 1061-1064), which was in effect from November 2000 through November 2002 and required Federal agencies to establish agency-wide risk-based information systems security programs and undergo annual independent evaluations. FISMA replaced GISRA with stronger permanent provisions, including requirements for minimum mandatory information systems security standards.

FISMA also supersedes or repeals provisions of the Computer Security Act of 1987 (P.L. 100-235). The CSA directed NIST to develop information technology standards and directed agencies to identify and develop security plans for computer systems containing sensitive but unclassified information.

9.B OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

OMB Circular A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, (P.L. 104-13 and 44 U.S.C. Chapter 35, which established "a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner"). Appendix III contains guidance on the "Security of Federal Automated Information Systems." The Appendix establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123.

Appendix III defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

Appendix III requires agencies, at a minimum, to include the following controls in their general support systems and major applications:

- Assign responsibility for security.
- Develop System Security Plan, a summary of which must be incorporated into the strategic IRM plan, and which must include rules of the system, training, personnel controls, incident response capability, continuity of support, technical security, and system interconnection.
- Develop Application Security Plan which must include application rules, specialized training, personnel security, contingency planning, technical controls, information sharing, and public access controls.
- Review security controls whenever significant modifications are made to the application/system and at least every three years.
- Re-authorize use of the system at least every three years.

The Appendix requires agencies to provide two reports to OMB:

1. Agencies are required to correct deficiencies identified through the reviews of security for systems and major applications and, if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, to include it in the annual FMFIA report. Less significant deficiencies must be reported and progress on corrective actions tracked at the appropriate agency level.
2. Agencies are also required to include a summary of their system security plans and major application plans in their agency strategic information resources management plans required by the Paperwork Reduction Act (44 U.S.C. 3506).

Finally, Appendix III also defines responsibilities of various agencies, including the Department of Commerce, Department of Defense, Department of Justice, the General Services Administration, The Office of Personnel Management, and the Security Policy Board.

Relationship to other laws/directives: The Appendix incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

9.C The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.

Broadly stated, the Privacy Act seeks to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them. The Act focuses on four basic policy objectives:

- (1) To restrict disclosure of personally identifiable records maintained by agencies.
- (2) To grant individuals increased rights of access to agency records maintained on themselves.
- (3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete.
- (4) To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The Act defines a "system of records" as any group of records under the control of a Federal agency or agent thereof from which information is retrieved by the name of the individual or by some identifying number, symbol, or their identifying particular (*e.g.*, fingerprint). The retrieval does not have to pinpoint a particular John Doe, but rather any John Doe, so this implies that Privacy Act protections apply to virtually any database that collects information on people along with their name (and/or SSN, and/or phone number, etc.), as long as that data is collected on behalf of a Federal agency.

The Act defines twelve specific conditions for disclosure of collected information; requires accurate accounting (audit) of disclosures, changes to data, etc.; defines rules for access to data,

most of which focuses of rights of individuals to access/correct their data; requires agencies to inform each individual who is asked to submit data of routine use, etc.; and requires agencies maintaining systems of records to publish in Federal Register: categories of individuals, records, and sources of records, each routine use of records, and procedures for individual to be notified.

The Act requires agencies to establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and to instruct each person on the rules and the requirements of the Privacy Act. The Act also requires agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

9.D Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, was enacted in 1966 and generally provides that:

- Any person has the right to request access to federal agency records or information.
- All agencies of the U.S. Government are required to disclose records upon receiving a written request for them.
- There are nine exemptions to the FOIA that protect certain records from disclosure.

9.E Homeland Security Presidential Directive / HSPD-7, December 17, 2003.

HSPD-7 established a national policy for Federal agencies for security protection and requires agency heads to identify, prioritize, assess, remediate, and protect their respective internal critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit those resources. Consistent with the Federal Information Security Management Act of 2002, agencies must identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

The Directive requires that by July 2004, the heads of all Federal agencies develop and submit to the Director of OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans must address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

Relationship to other laws/directives: HSPD-7 supersedes Presidential Decision Directive 63, May 22, 1998, Subject: Critical Infrastructure Protection.

9.F Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.

PDD 67 recognizes emerging threats, addresses enduring constitutional government, and introduces continuity of operations planning (COOP) and continuity of government operations. PDD 67, among other things, requires Federal agencies to develop COOP plans for essential operations. These COOP plans are viewed as a unifying concept not to replace existing plans but, instead, to be superimposed if and when a problem threatens a serious disruption of agency operations. PDD 67 designates FEMA as the Executive Agent for COOP.

PDD 67 required that viable COOP capability must be achieved by Oct. 21, 1999. It takes an all hazards approach, requires agencies to address the use of alternate facilities, requires that agencies be able to operate within 12 hours of activation of COOP, and requires agencies to be able to sustain COOP operations for up to 30 days.

Several Federal Preparedness Circulars (FPCs) that detail a series of government policies specific to COOP planning and national security emergency preparedness have been written under the authority of PDD 67. The focus of these documents includes succession, vital records, training, COOP requirements, alternative facility requirements, and communications. They are associated with supporting all Federal organizations with viable COOP programs. [FPC 65](#) provides guidance to all Federal Executive Branch departments, agencies, and independent organizations on the development of viable and executable COOP plans. [FPC 66](#) further supports COOP efforts by providing guidance on the development of test, training, and exercise programs to support the implementation and validation of COOP plans. [FPC 67](#), designed as a supplement to FPC 65, provides guidance on implementing COOP plans, specifically in locating alternate facilities to support COOP efforts.

Relationship to other laws/directives: PDD 67 succeeded NSD 69 “Enduring Constitutional Government” of June 1992.

9.G Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

The Clinger-Cohen Act encourages performance-based and results-based management through the effective use of information technology (IT). It shifts the emphasis from IT acquisition management to IT investment management, and emphasizes information resources management and IT management (not information management). The Act requires the heads of Federal agencies to link IT investments to agency accomplishments. It also requires that agency heads establish a process to select, manage and control their IT investments.

The Clinger-Cohen Act repeals the Brooks Act and returns IT procurement authority to Federal agencies. It transfers day-to-day management of IT from GSA to OMB, with the exception of FTS2000. The effect is to eliminate the Federal Information Resources Management Regulations (GSA has moved some provisions to the Federal Acquisition Regulations) and the General Services Board of Contract Appeals. The law gives OMB responsibility for:

- Developing a process for analyzing, tracking, and evaluating the risks and results of major capital investments,
- Directing executive agencies on establishing an effective, efficient IT capital planning and investment review process, and
- Enforcing accountability through the budget process.

The law gives executive agencies responsibility for:

- Establishing an IT capital planning and investment review process,
- Using performance measures to assess how well IT supports programs, and
- Justifying continuation of systems that deviate from cost, performance, or schedule goals.

The Clinger-Cohen Act establishes a Chief Information Officer (CIO) in executive agencies who:

- Reports directly to the agency head,
- Has IRM as the primary duty,
- Provides advice and assistance to the agency head on IT and information resources management,
- Develops an integrated IT architecture,
- Promotes efficient and effective design and operation of IRM processes,
- Uses performance measures to monitor IT programs,
- Assesses the knowledge and skills of IRM personnel,
- Shares with the CFO responsibility for provision of financial and performance data for financial statements, and
- Assumes the responsibilities of the Designated Senior Official defined in Paperwork Reduction Act.

Clinger-Cohen confirms the responsibility of NIST for standards and guidelines for computer systems and reinforces requirements of the Computer Security Act. It also encourages and provides for modular contracting for IT systems and pilot IT acquisition programs.

Relationship to other laws/regulations: The Clinger-Cohen Act of 1996 renames the Information Technology Management Reform Act and the Federal Acquisition Reform Act.

9.H Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994 [18 USC, Chapter 47, Section 1030].

The Computer Abuse Amendments Act of 1994 expanded the Computer Fraud and Abuse Act of 1986 to address the transmission of viruses and other harmful code. Codified at 18 USC, Chapter 47, Section 1030, it prohibits unauthorized or fraudulent access to government computers, and establishes penalties for such access.

The Act makes six types of activity illegal:

1. Acquiring national defense, foreign relations, or restricted atomic energy information with the intent or reason to believe that the information can be used to injure the United States or to the advantage of any foreign nation. (The offense must be committed knowingly by accessing a computer without authorization or exceeding authorized access.)
2. Obtaining information in a financial record of a financial institution or a card issuer, or information on a consumer in a file of a consumer reporting agency. (The offense must be committed intentionally by accessing a computer without authorization or exceeding authorized access.)
3. Affecting a computer exclusively for the use of a U.S. government department or agency or, if it is not exclusive, one used for the government where the offense adversely affects the use of the government's operation of the computer. (The offense must be committed intentionally by accessing a computer without authorization.)
4. Furthering a fraud by accessing a federal interest computer and obtaining anything of value, unless the fraud and the thing obtained consists only of the use of the computer. (The offense must be committed knowingly, with intent to defraud, and without authorization or exceeding authorization.)
5. Through use of a computer used in interstate commerce, knowingly causing the transmission of a program, information, code, or command to a computer system.
6. Furthering a fraud by trafficking in passwords or similar information which will allow a computer to be accessed without authorization, if the trafficking affects interstate or foreign commerce or if the computer affected is used by or for the government. (The offense must be committed knowingly and with intent to defraud.)

Under the Amendments, prosecutors no longer have to prove "harmful intent," but a less strict "reckless disregard" standard, to convict. The Amendments also broaden the scope of the protection offered in section 1030 (a) (5) (A) in order to close a loophole contained in the earlier Act. "[I]ntentionally accesses a Federal interest computer" is no longer used, and instead the section applies to anyone who "through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or

command to a computer or computer system" As amended, the section now protects not only Federal interest computers, but it also covers privately owned computer systems, used in interstate commerce or communication, but which may be affected by someone acting through means of a computer located within the same state as the affected computer.

The Amendments also remove the "access" requirement from the statute. Instead, a specific intent to perform certain acts that may constitute direct or indirect access is put into the statute. Significantly, the statute also adds a requirement that there be either a specific intent or reckless disregard as to whether the transmission will cause damage or withhold or deny use of a "computer, computer system, network, information, data, or program" in excess of the user's authorization.

9.I Computer Security Act of 1987, PL 100-235, January 8, 1988.

The Computer Security Act of 1987 was enacted to mandate that federal agencies take extra measures to prevent unauthorized access to computers holding sensitive information. It requires each agency to establish a plan for the security and privacy of sensitive information, and requires the submission of such plans to NIST and the National Security Agency for advice and comment. These plans are subject to disapproval by the Office of Management and Budget.

The Act requires Federal agencies to provide for mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency.

The Act directs NIST to establish a computer standards program for Federal computer systems, including guidelines for the security of such systems. It sets forth authorities of NIST in implementing such standards, and requires NIST to draw upon computer system technical security guidelines developed by the National Security Agency regarding protecting sensitive information.

The Computer Security Act also charged NIST, together with the U.S. Office of Personnel Management (OPM), with developing and issuing guidelines for Federal computer security training. This requirement was satisfied by NIST's issuance of *Computer Security Training Guidelines* (Special Publication [SP] 500- 172), in November 1989. In January 1992, OPM issued a revision to the Federal personnel regulations, which made these voluntary guidelines mandatory. This regulation, *Employees Responsible for the Management or Use of Federal Computer Systems*, requires Federal agencies to provide training as set forth in the NIST guidelines.

9.J Computer Fraud and Abuse Act of 1986, PL 99-474, October 1986.

The Computer Fraud and Abuse Act of 1986 was initially aimed at protecting “federal interest” computers as well as computers used by financial institutions but now protects any computer used in interstate commerce. Specifically, the law prohibits the use of "a program, information, code or command" with intent to damage, cause damage to, or deny access to a computer system or network. In addition, the Act specifically prohibits even unintentional damage if the perpetrator demonstrates reckless disregard of the risks of causing such damage.

The Act imposes penalties on individuals who knowingly and with intent to defraud gain unauthorized access to computers. Although the Act does not include provisions for critical information infrastructure protection per se, it has played a major role in prohibiting and sanctioning cyber attacks. Congress has continued to amend the law over the last several years to increase its effectiveness as the threat and technology have evolved.

Relationship to other laws/directives: Amended by the Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994.

9.K Office of Management and Budget (OMB) Memoranda

OMB issues memoranda that provide instructions to agency officials regarding various issues. Some recent memoranda that apply to information security include:

- M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems (March 22, 2007)
- M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials (January 11, 2007)
- Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006)
- M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 17, 2006)
- M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)
- M-06-16, Protection of Sensitive Agency Information (June 23, 2006)
- M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
- M-05-05, Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services (December 20, 2004)
- M-05-04, Policies for Federal Agency Public Websites (December 17, 2004)
- M-04-26, Personal Use Policies and “File Sharing” Technology (September 8, 2004)

- M-04-04, E-Authentication Guidance (December 16, 2003)
- M-01-05, OMB Memorandum Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- M-99-20, Security of Federal Automated Information Resources (June 23, 1999)

9.L National Institute of Standards & Technology (NIST) Guidance

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Under the Computer Security Act of 1987, NIST's Computer Security Division develops security standards and guidelines for sensitive (unclassified) Federal IT systems and works with industry to help improve the security of commercial IT products. The Division has key focused activities in the areas of cryptographic standards and applications, security of emerging technologies, security management, and security testing. The mission of NIST's Computer Security Division is to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs:
 - to promote, measure, and validate security in systems and services
 - to educate consumers and
 - to establish minimum security requirements for Federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation.

FISMA reaffirmed and strengthened NIST's role as the developer of information security standards for use throughout the federal government.

NIST's publications present the results of NIST studies, investigations, and research on information technology security issues. The publications are issued as Special Publications (Spec. Pubs.), NISTIRs (Internal Reports), and ITL (formerly CSL) Bulletins. Special Publications series include the Spec. Pub. 500 series (Information Technology) and the Spec. Pub. 800 series (Computer Security). Computer security-related Federal Information Processing Standards (FIPS) are also included. As a federal agency, CNCS must adhere to these information security standards and guidelines whenever possible.

9.M Hatch Act

The Hatch Act restricts the political activity of executive branch employees of the federal government, District of Columbia government and some [state and local employees](#) who work in connection with federally funded programs. In 1993, Congress passed legislation that significantly amended the Hatch Act as it applies to federal and D.C. employees ([5 U.S.C. §§ 7321-7326](#)). (These amendments did not change the provisions that apply to state and local employees. [5 U.S.C. §§ 1501- 1508](#).) Under the amendments most federal and D.C. employees are now permitted to take an active part in political management and political campaigns. [A small group of federal employees are subject to greater restrictions](#) and continue to be prohibited from engaging in partisan political management and partisan political campaigns.

9.N 1991 U.S. Federal Sentencing Guidelines

The 1991 U.S. Federal Sentencing Guidelines provide punishment guidelines for those found guilty of breaking federal law. Certain of these guidelines are pertinent to information security:

- Treat the unauthorized possession of information without the intent to profit from the information as a crime.
- Address both individuals and organizations.
- Make the degree of punishment a function of the extent to which the organization has demonstrated “Due diligence” (*due care*) in establishing a prevention and detection program.
- Invoke the “prudent man rule” that requires senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances.
- Place responsibility on senior organizational management for the prevention and detection programs.

9.O OMB Circular A-123, Management Accountability and Control

Issued under Federal Managers' Financial Integrity Act of 1982 as codified in 31 U.S.C. 3512. Requires internal controls to prevent fraud, waste, and abuse. Primarily applies to financial systems.

9.P OMB Circular A-127, Financial Management Systems

Provides policies and standards for developing, operating, evaluating, and reporting on financial management systems.

10 APPENDIX B: ACRONYMS AND ABBREVIATIONS

<i>C&A</i>	Certification and Accreditation	<i>IA</i>	Information Assurance
<i>CEO</i>	Chief Executive Officer	<i>InfoSec</i>	Information Security
<i>CFO</i>	Chief Financial Officer	<i>ISC²</i>	International Information Systems Security Certifications Consortium
<i>CFR</i>	Code of Federal Regulations	<i>ISSO</i>	Information Systems Security Officer
<i>CIO</i>	Chief Information Officer	<i>ISP</i>	Information Security Program
<i>CISO</i>	Chief Information Security Officer	<i>IT</i>	Information technology
<i>CM</i>	Configuration Management	<i>ITL</i>	Information technology Laboratory
<i>CNCS</i>	Corporation for National & Community Service	<i>NIST</i>	National Institute of Standards & Technology
<i>COOP</i>	Continuity of Operations Plan	<i>NSA</i>	National Security Agency
<i>COTR</i>	Contracting Officer's Technical Representative	<i>OIG</i>	Office of Inspector General
<i>CSA</i>	Computer Security Act	<i>OIT</i>	Office of Information Technology
<i>DAA</i>	Designated Approving Authority	<i>OMB</i>	Office of Management and Budget
<i>DAD</i>	Disclosure, alteration, or destruction	<i>OPM</i>	Office of Personnel Management
<i>EO</i>	Executive Order	<i>PDD</i>	Presidential Decision Directive
<i>FEA</i>	Federal Enterprise Architecture	<i>PL</i>	Public Law
<i>FISMA</i>	Federal Information Security Management Act	<i>POC</i>	Point of Contact
<i>FMFIA</i>	Federal Managers Financial Integrity Act	<i>SAISSO</i>	Senior Agency Information Systems Security Officer
<i>FOIA</i>	Freedom of Information Act	<i>SDLC</i>	Systems Development Lifecycle
<i>FPC</i>	Federal Preparedness Circular	<i>SETA</i>	Security Education, Training & Awareness
<i>FSO</i>	Facility Security Officer	<i>SP</i>	Special Publication
<i>GAO</i>	Government Accounting Office	<i>SPP</i>	Security and Privacy Profile
<i>GSA</i>	General Services Administration	<i>SSN</i>	Social Security Number
<i>HSPD</i>	Homeland Security Presidential Directive	<i>ST&E</i>	Security Test and Evaluation
<i>IA</i>	Information Assurance	<i>USC</i>	United States Code

11 APPENDIX C: ROLE ASSIGNMENTS

Information Security Role Assignments

May 2009

Role	Assigned To
Chief Executive Officer (CEO)	Nicki Goren (Acting)
Chief Information Officer (CIO)	Mary Cadagin
Chief Information Security Officer (CISO)	Juliette Sheppard
Privacy Officer (PO)	Laurie Young
Physical Security Officer	Norman Franklin
Personnel Security Officer	Norman Franklin
Contracting	Roderick Gaither
Inspector General	Gerald Walpin

12 APPENDIX D: INFORMATION SECURITY POLICY DOCUMENTS

INFORMATION SECURITY GOVERNANCE AND REPORTING

ISP-P-01-0905

1. **SUBJECT:** CNCS will manage its Information Security Program (ISP) to proactively track and mitigate weaknesses, and will report on the status of the program as required under FISMA and other federal mandates.
2. **SCOPE:** This policy applies to management and reporting of the CNCS Information Security Program.
3. **DESCRIPTION:** CNCS relies heavily on information resources to perform its mission. Information Security is critical to protect the Corporation as it uses these resources in a constantly changing threat environment. Information Security must be managed and governed to reduce the risks to CNCS operations and to ensure the Corporations' ability to do business and serve the American public.

“The purpose of information security governance is to ensure that agencies are proactively implementing appropriate information security controls to support their mission in a cost-effective manner, while managing evolving information security risks. As such, information security governance has its own set of requirements, challenges, activities, and types of possible structures. Information security governance also has a defining role in identifying key information security roles and responsibilities, and it influences information security policy development and oversight and ongoing monitoring activities.”

4. **REQUIREMENTS:**

- (a) CNCS will operate an Information Security Program (ISP) in compliance with FISMA and other federal requirements.
- (b) The ISP will be continuously assessed and updated to ensure that risks are adequately mitigated, federal requirements are being met, and the program is operating as intended.
- (c) The CISO will serve as the focal point for reporting and tracking all security related findings and corrective measures identified by any audit, review, scanning, or risk assessments conducted by the IG, OIT, or any other Federal agency directed to conduct such audits and reviews.
- (d) Plans of Actions & Milestones (POA&Ms) are required to track all corrective actions related to security policies, procedures and practices in accordance with FISMA.
 - (1) POA&Ms will be maintained for the security program and for each major system.

- (2) The POA&Ms will be used as management tools to mitigate weaknesses.
 - (3) Any official reports providing specific information on weaknesses or vulnerabilities resulting from Inspector General audits, reviews, or scanning activity related to such work as risk assessments, certification testing, or penetration testing, will be documented as part of the POA&Ms.
 - (4) The CISO will collect and monitor the status of all IT system security related and agency wide security program related corrective actions.
 - (5) System Owners will provide POA&M updates to the CISO regarding system level POA&M items for their system(s) on at least a quarterly basis.
 - (6) Each POA&M will be continuously updated as items are completed and new weaknesses discovered so that it reflects the current state of the Corporation's mitigation status.
- (e) OMB requires reports on the Corporations information security status under FISMA. FISMA reports will be completed and submitted in accordance with the latest OMB guidance.
- (f) Metrics will be used to monitor the progress of the security program
- (1) Information security metrics will align with the Corporation's security strategy, including measuring progress towards FISMA compliance.
 - (2) The metrics will provide input into decision-making and program improvement
- (g) An annual independent assessment of the Corporation's Information Security Program will be performed by the Office of the Inspector General.
- (h) CNCS will integrate the Information Security Program with the Corporation's internal controls procedures.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Information Security Officer (CISO) will:
- (1) Develop and maintain the CNCS Information Security Program
 - (2) Track deficiencies and corrective actions in POA&Ms
 - (3) Coordinate with system owners for resolution of POA&M items
 - (4) Perform FISMA reporting
 - (5) Supply information security metrics to the CIO
- (b) The Chief Information Officer (CIO) will:
- (1) Review and provide input to FISMA reporting
 - (2) Promote the Information Security Program within the Corporation and Executive management
 - (3) Provide resources for the effective implementation of the security program

- (4) Report and advise the CEO and CFO regarding the Information Security Program
- (c) The Office of the Inspector General (OIG) will:
 - (1) Perform independent assessments of the Information Security Program
 - (2) Communicate deficiencies to the CISO and CIO
 - (3) Perform the IG portion of the FISMA reporting to OMB
- (d) System Owners will:
 - (1) Maintain a POA&M for their system.
 - (2) Include all findings communicated by the CISO into their POA&M.
 - (3) Implement corrective actions on their systems as specified in the POA&M.
 - (4) Provide system POA&M updates to the CISO at least quarterly.

6. DEFINITIONS:

- (a) Metrics - Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
- (b) Plan of Actions and Milestones (POA&M) - A tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

- (c) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (d) NIST Special Publication 800-100, Information Security Governance
- (e) OMB Memorandum 06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SECURITY TRAINING AND AWARENESS**ISP-P-02-0905**

1. **SUBJECT:** CNCS will operate a program to maintain effective awareness of information security policies, standards and acceptable practices. All staff will be made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of CNCS information systems. The program will also ensure that personnel are adequately trained to carry out their assigned duties and responsibilities while safeguarding CNCS information resources.
2. **SCOPE:** This policy applies to all CNCS information users, including employees, contractors, interns, grantees, etc, who have access to CNCS information resources. The term "users" will be used in this policy to specify all personnel within this scope.
3. **DESCRIPTION:** The Federal Information Security Management Act (FISMA) requires each federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, the Office of Management and Budget (OMB) Circular A-130 requires that such training be completed prior to the granting of access, and be provided as periodic refreshment.

Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of CNCS information resources. Information security policy and standards cannot be effective unless everyone at CNCS, regardless of position in the organization, is aware of the importance of security, understands CNCS security procedures, and performs required practices. To make information security effective, standards and procedures must be known, understood, believed to be beneficial, and be appropriately and consistently practiced.

Information Security is not a one-time event, but a continuous effort and "state of mind". This is achieved by reinforcing concerns and appropriate behaviors on a continuous basis. Effective information security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

4. **REQUIREMENTS:**
 - (a) Information Security policies will be made available for reference and review by CNCS information users.
 - (b) For internal personnel (on-site personnel and telecommuting federal staff):
 - (1) CNCS will develop and maintain an Information Security Training and Awareness Program to educate employees about information security policies and procedures, and make them aware of their roles and responsibilities in

safeguarding CNCS's information resources. The program will be composed of two major initiatives:

- A Training program designed to build relevant and needed security skills and competencies to facilitate job performance. Persons responsible for administering or securing information resources will have adequate training on the proper implementation of security controls for the systems and data under their control.
 - An Awareness program designed to focus attention on security, and to change behavior or reinforce good security practices. Ongoing development of security awareness builds a culture that encourages good security practices.
- (2) Information users will complete training on CNCS Information security policies and procedures. This mandatory training will consist of three activities:
- Information security training will be incorporated into the orientation processes for all new staff. Training must be completed prior to access to CNCS information systems.
 - All information users will complete annual information security training to refresh their knowledge of information security.
 - Information Custodians, System Owners, and other personnel with additional responsibilities related to administering and securing systems will be provided with enhanced security training applicable to their functions.
- (3) CNCS will maintain and publish an Information Security Handbook documenting policies, procedures, and responsibilities.
- (4) Users will sign a Rules of Behavior agreement that they understand the CNCS Information security policies and procedures and that they will abide by them.
- (5) Employees will be made aware of the penalties for non-compliance with CNCS security policies and procedures.
- (6) Materials will be posted or presented in a variety of formats on a regular basis to maintain user awareness of information security issues.
- (7) Changes to CNCS Information security policies or procedures will be communicated to all information users.
- (8) Security training records will be maintained to document and monitor the training program and individuals' training activities.
- (9) System Owners will provide system specific security training to the users and custodians of their systems, including training on any procedures and standards that must be followed for the system. They should also ensure that custodians are provided technical security training as appropriate.

- (10) CNCS personnel with significant InfoSec responsibilities (including information custodians) will subscribe to and participate in professional associations, news lists, peer groups, specialized forums and other activities to stay up to date with the latest security practices, techniques, and technologies.
- (c) For external personnel (including members, grantees, and volunteers) who do not have accounts on CNCS internal systems:
 - (1) Rules of behavior and relevant policy information will be posted on systems accessible to these users
 - (2) Users will be required to electronically accept a rules of behavior prior to being allowed access to a CNCS information system.
 - (3) Changes to security policies will be communicated to these users by updating the posted information and requesting the users to electronically accept the updated policies.
- (d) CNCS will adhere to NIST guidance as set forth in NIST Special Publication 800-50, Building an Information Technology Security Training and Awareness Program, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Information Security Officer (CISO) is responsible for developing and operating the Information Security Training & Awareness program, including:
 - (1) preparing policy on security awareness and training,
 - (2) developing and presenting security training courses and briefings,
 - (3) developing and distributing awareness material and bulletins,
 - (4) ensuring all personnel receive the appropriate security training associated with their security roles, and
 - (5) maintaining training records
- (b) Supervisors are responsible for:
 - (1) Ensuring that their staff understand their roles and responsibilities under CNCS' Information Security program.
 - (2) Communicating changes in policies and procedures to their staff.
 - (3) Providing opportunities for staff to complete information security training.
- (c) Information Users are responsible for:
 - (1) Completing annual security training.
 - (2) Reviewing and understanding CNCS information security policies and procedures.
 - (3) Completing and abiding by the CNCS Information Security Rules of Behavior agreement.

- (4) Complying with all CNCS information security policies and procedures.
- (d) Information Owners are responsible for ensuring that personnel who use their resources are appropriately trained to fulfill their security responsibilities for those resources.
- 6. DEFINITIONS:**
- (a) Awareness – A state of focused attention on security that allows individuals to recognize IT security concerns and respond accordingly.
- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.
- 8. POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)
- 9. ATTACHMENTS:** None
- 10. AUTHORITY:**
- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (e) Computer Security Act of 1987, PL 100-235, January 8, 1988.
- (f) NIST Special Publication 800-50, Building an Information Technology Security Training and Awareness Program.
- (g) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (h) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (i) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

INCIDENT REPORTING

ISP-P-03-0905

1. **SUBJECT:** All CNCS information users are required to report any suspected information security incidents in accordance with CNCS incident reporting procedures.
2. **SCOPE:** This policy applies to all users of CNCS information resources.
3. **DESCRIPTION:** Maintaining the security of CNCS information resources requires cooperation and participation from everyone. It is important that all information users maintain vigilance regarding information security, and immediately report any suspected incidents in order to minimize potential damage to CNCS.

CNCS's security incident reporting policy and procedures enable CNCS to quickly and efficiently recover from security incidents; respond in a systematic manner to incidents and carry out all the necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission-critical information.

4. **REQUIREMENTS:**

(a) All suspected security incidents must be reported immediately.

(1) Incidents include, but are not limited to:

- Suspected violations of any CNCS information security policies, including inappropriate usage of resources.
- Loss or theft of laptops, mobile devices (such as phones, PDAs), security tokens, or other CNCS information resources.
- Attempts by unauthorized personnel to gain access to CNCS information or systems.
- Accidental disclosure, modification, or destruction of information.
- Distribution of/infection with malicious code (e.g. viruses, spyware, etc.)
- Compromised passwords or accounts.
- Serious disruptions to CNCS information systems caused by reasons other than natural equipment failure.
- Social engineering attempts.

- (b) Incidents may be reported to the CISO, the OIT Help Desk, the system owner for the affected system, the user's supervisor, or any OIT director.
- (c) Supervisors, the OIT Help Desk, and OIT Directors must immediately pass on any incident reports received to the CISO and the system owner.
- (d) All reported incidents will be handled in accordance with CNCS Incident Handling policies and procedures.
 - (1) An CNCS incident report form must be completed and submitted for each incident.
- (e) The CISO will maintain a log of all reported incidents.
- (f) CNCS will adhere to NIST guidance as set forth in Special Publication 800-61, Computer Security Incident Handling Guide, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Users are responsible for reporting suspected incidents to the CISO, Help Desk, system owner, or their supervisor immediately, using CNCS incident reporting procedures.
- (b) Supervisors are responsible for ensuring that their employees understand and adhere to incident reporting policies and procedures, and for ensuring that security incidents are reported as quickly as possible.
- (c) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Developing and maintaining incident reporting and handling procedures.
 - (2) Researching, documenting, resolving and tracking reported incidents.
 - (3) Reporting incidents to upper management and the OIG.
 - (4) Determining if incident follow-up is needed.
- (d) Information Custodians are responsible for:
 - (1) Reporting any incidents they encounter to the CISO.
 - (2) Researching and resolving incidents within their administrative domain.
 - (3) Providing documentation of incidents and steps taken to resolve them to the CISO.
 - (4) Fully cooperating with and assisting the CISO with incident handling as requested.
- (e) System Administrators are responsible for assisting the CISO with researching, documenting, resolving and tracking reported incidents.

6. DEFINITIONS:

- (a) Security Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) NIST Special Publication 800-61, Computer Security Incident Handling Guide.
- (c) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (d) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

INCIDENT RESPONSE

ISP-P-04-0905

1. **SUBJECT:** CNCS will maintain an operational incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate organizational officials and/or authorities.
2. **SCOPE:** This policy applies to all CNCS information users, owners, and custodians.
3. **DESCRIPTION:** The Corporation must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident. A formally documented and clearly understood incident response process will make it possible for CNCS to respond quickly and effectively to situations that might compromise the agency's information resources.
4. **REQUIREMENTS:**
 - (a) CNCS will maintain Information Security Incident Response procedures to address computer security incidents.
 - (1) Procedures will include incident detection, analysis, containment, eradication, and recovery.
 - (b) Each major information system will have a system specific incident response plan that conforms to the Corporation's overall incident handling procedures.
 - (c) Personnel with incident handling responsibilities will be trained on the incident response procedures.
 - (d) All reported security incidents will be responded to quickly and in adherence to CNCS information security incident handling procedures.
 - (e) All incidents and their resolutions will be fully documented and the reports retained for at least one year after the incident.
 - (f) CNCS will report incident information to appropriate authorities such as US-CERT.
 - (g) Priority in incident handling should be given to containing the incident and preventing further damage.
 - (h) The type of response and the level of documentation will be tailored to the nature and severity of the specific incident.
 - (i) If a system was compromised, or may have been compromised, by an incident, the system should be removed from the production network and reformatted and

reloaded to ensure a clean configuration prior to being placed back into the production environment.

- (j) CNCS will adhere to NIST guidance as set forth in Special Publication 800-61, Computer Security Incident Handling Guide, and subsequent publications, as well as relevant guidance from US-CERT.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Information Security Officer (CISO) is responsible for:
- (1) Establishing and implementing an information security incident response capability including developing Corporation-wide incident response procedures
 - (2) Providing guidance and assistance to system owners and custodians regarding incident response
 - (3) Notifying the information owners, and CNCS management of significant incidents and the response plan
 - (4) Ensuring that all incidents and resolution activities are appropriately documented and tracked
 - (5) Convening an appropriate incident response team for each incident as needed.
 - (6) Providing information on incidents to appropriate authorities
 - (7) Coordinating with the Office of General Counsel and the Office of the Inspector General for the investigation of incidents involving illegal activity.
- (b) Information Users are responsible for:
- (1) Performing the following if they suspect a security incident may have occurred:
 - Documenting all relevant information about the suspected incident
 - Sharing information about the suspected incident with their manager and/or the CISO
 - Fully cooperating with and assisting the CISO, system administrators, and other designated personnel with resolution of the incident as requested
- (c) Supervisors are responsible for:
- (1) Ensuring that their employees understand CNCS incident response policy and procedures
 - (2) Ensuring that their staff fully cooperates with investigations.
 - (3) Contacting the CISO upon being notified of an incident by their staff
 - (4) Providing incident-related information to the CISO when requested
- (d) Information Owners are responsible for:

- (1) Ensuring that incident response procedures are in place for their resources
 - (2) Informing the CISO and CNCS management of any incidents.
 - (3) Providing follow up to ensure that incidents have been resolved
- (e) Information Custodians are responsible for:
- (1) Assisting with evaluation and resolution of the incident
 - (2) Working with the CISO, system owner, and/or users, to formulate and implement a response plan,
 - (3) Documenting steps taken to handle the incident and reporting this to the CISO.
- (f) The Office of General Counsel is responsible for assisting with the determination of whether an incident should be escalated to OIG.
- (g) The Office of the Inspector General is responsible for performing investigations of fraud, waste, and abuse within the Corporation's programs and operations.
- (h) The Facility Security Officer and Personnel Security Officer are responsible for assisting with investigations that involve personnel or physical security issues.

6. DEFINITIONS:

- (a) Attack – An attempt to bypass security controls on a computer.
- (b) Security Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- (c) Critical Incident – An incident that will result in a severe impact to CNCS resources if not addressed quickly.

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

- 8. POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

- 9. ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.
- (d) NIST Special Publication 800-61, Computer Security Incident Handling Guide.
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems
- (g) NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

VULNERABILITY TESTING

ISP-P-05-0905

1. **SUBJECT:** In order to assess CNCS' information security posture and determine the security risks that should be mitigated, CNCS will conduct periodic vulnerability assessments. These assessments will assist in the discovery of security vulnerabilities, gauge the threat posed by these vulnerabilities, and assist CNCS with mitigating security risks.
2. **SCOPE:** This policy applies to all systems owned by or operated on behalf of CNCS.
3. **DESCRIPTION:** Today's information systems are complex and composed of many interdependent and interconnected components. No matter how well they have been developed, all systems have some inherent vulnerabilities or exploitable weaknesses. Over time, these vulnerabilities are likely to be exploited, either intentionally or accidentally.

Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand security attacks. A vulnerability testing program provides the crucial details to help CNCS avoid the significant financial costs or damage to its reputation that could result from security malfeasance.

Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires CNCS to perform security testing on a periodic basis. A systematic, comprehensive, ongoing, and priority-driven security testing program will assist CNCS with determining its security priorities and making prudent investments to enhance the security posture of its information resources.

4. **REQUIREMENTS:**
 - (a) Vulnerability testing will be conducted on a periodic basis to detect potential weaknesses in CNCS systems and provide assurance that security controls are adequately protecting systems.
 - (b) The depth and breadth of testing will be commensurate with the level of risk of the system to be tested.
 - (c) Procedures for testing will be clearly defined and documented to ensure repeatable and reliable test results
 - (1) Roles and responsibilities for testing will be clearly defined.
 - (2) The frequency of testing will be identified

- (3) Assessment methods and tools will be specified
- (d) Controls common to multiple systems will be identified to eliminate redundant testing
- (e) All test results will be well documented.
- (f) The “rules of engagement” should be documented and communicated to the system owners.
- (g) Information Owners and Information Custodians will be informed of the results to ensure that vulnerabilities are patched or mitigated.
- (h) Vulnerabilities discovered will be tracked and remediated in accordance with the CNCS Vulnerability Remediation policy (ISP-P-06).
- (i) Systems will be retested once vulnerabilities are addressed to ensure that they have been effectively addressed.
- (j) Testing should not disrupt critical business operations.
- (k) Vulnerability testing will be integrated into CNCS’ Risk Management processes.
- (l) Vulnerability scanning or password-checking software shall only be used with the written permission of the CISO or CIO and all execution of such software shall be coordinated through the OIT.
- (m) CNCS will adhere to NIST guidance as set forth in Special Publications 800-42, Guideline on Network Security Testing; 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme; 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Developing testing procedures.
 - (2) Performing periodic testing.
 - (3) Documenting test results.
 - (4) Communicating vulnerabilities to Information Owners and Custodians.
 - (5) Auditing to ensure that vulnerabilities have been mitigated.
 - (6) Providing advice to Information Owners and Custodians regarding potential mitigation strategies.
- (b) Information Owners are responsible for:
 - (1) Allowing vulnerability testing to be performed on their resources.
 - (2) Ensuring that any identified vulnerabilities are resolved for their resources.
 - (3) Ensuring that resolutions are reported back to the CISO

- (c) Information Custodians are responsible for:
- (1) Assisting the CISO with performing security testing, as requested.
 - (2) Helping Information Owners with selecting and implementing mitigation strategies.
 - (3) Documenting mitigations that are implemented.
 - (4) Informing the CISO about mitigations performed.

6. DEFINITIONS:

- (a) Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
- (b) Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- (c) Vulnerability Assessment (or Vulnerability Testing) – Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. **POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

9. **ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-42, Guideline on Network Security Testing

- (d) NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems
- (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (f) NIST Special Publication 800-40, Creating A Patch & Vulnerability Management Program
- (g) GAO-07-65, Agencies Need To Develop And Implement Adequate Policies for Periodic Testing

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

VULNERABILITY REMEDIATION

ISP-P-06-0905

1. **SUBJECT:** Vulnerabilities must be addressed in a timely fashion to minimize risk to CNCS resources. CNCS will identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response.
2. **SCOPE:** This policy applies to all systems owned by or operated on behalf of CNCS.
3. **DESCRIPTION:** Today's information systems are complex and composed of many interdependent and interconnected components. No matter how well they have been developed, all systems have some inherent vulnerabilities or exploitable weaknesses. Over time, these vulnerabilities are likely to be exploited, either intentionally or accidentally.

CNCS must have an effective and efficient methodology for tracking and resolving reported vulnerabilities.

4. **REQUIREMENTS:**

- (a) All deficiencies or vulnerabilities within any CNCS IT system must be addressed and mitigated in a timely manner.
- (b) Vulnerabilities may be detected or reported through a variety of sources, including:
 - (1) Periodic vulnerability testing
 - (2) Vendor alerts
 - (3) US-CERT, NIST, or other reputable organization alerts
 - (4) IG or audit findings
- (c) System Custodians will immediately assess reported vulnerabilities to determine level of impact on CNCS systems and develop a mitigation strategy. This assessment will be provided to the Chief Information Security Officer (CISO) and the System Owner.
- (d) Corrective actions will be documented and scheduled in accordance with Patch Management and Change Control procedures.
- (e) Once corrective actions have been taken, they will be validated to ensure the vulnerability has been adequately mitigated.

- (f) Completion of vulnerability resolution will be reported back to the CISO and the system owner.
- (g) CNCS will subscribe to the US-CERT National Cyber Alert System and will take advantage of other publicly available vulnerability resources provided by the US government.
- (h) Any official reports providing specific information on weaknesses or vulnerabilities resulting from Inspector General audits, reviews, or scanning activity related to such work as risk assessments, certification testing, or penetration testing, will be documented and tracked as part of the specific system POA&M documentation.
- (i) Information about vulnerabilities in CNCS systems and programs will be treated as sensitive information and its distribution will be limited.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Subscribing to US-CERT alerts and other vulnerability information.
 - (2) Communicating vulnerability alerts to system owners/custodians.
 - (3) Auditing to ensure vulnerabilities are being remediated.
- (b) Information Owners are responsible for:
 - (1) Ensuring that vulnerabilities are remediated for the resources they own.
 - (2) Ensuring that the resolution is documented and reported back to the CISO
- (c) Information Custodians are responsible for:
 - (1) Helping Information Owners with selecting and implementing mitigation strategies.
 - (2) Documenting mitigations that are implemented.
 - (3) Informing the System Owner and CISO about mitigations performed.
 - (4) Reporting to the CISO any vulnerability they discover on their systems.

6. DEFINITIONS:

- (a) POA&M - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
- (b) Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or

- denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
- (c) **Vulnerability – Weakness** in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
 - (d) **Vulnerability Assessment (or Vulnerability Testing)** – Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.
- 8. POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)
- 9. ATTACHMENTS:** None
- 10. AUTHORITY:**
- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
 - (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
 - (c) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
 - (d) NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems
 - (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
 - (f) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
 - (g) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems
 - (h) NIST Special Publication 800-40, Creating A Patch & Vulnerability Management Program

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SECURITY CATEGORIZATION

ISP-P-07-0905

1. **SUBJECT:** All information resources (including data and systems) must be identified, categorized, and protected according to their level of sensitivity, criticality, and business “need to know.”
2. **SCOPE:** This policy applies to all CNCS information systems and data created, owned, stored, or transferred by CNCS that are not designated as national security classified, as well as any system operated on behalf of CNCS.
3. **DESCRIPTION:** CNCS information systems vary in size, complexity, sensitivity, criticality, and importance to the corporation. Applying equal levels of concern and resources to all information systems is not possible or cost-effective. In order to ensure that appropriate levels of protection are applied to information resources, those resources must be categorized based on their criticality to the organization and the sensitivity of the data that they contain. This includes assessing the criticality and sensitivity of the systems, and determining minimum security requirements based on those classification levels.
4. **REQUIREMENTS:**
 - (a) All CNCS information resources will be categorized based on CNCS’ information classification framework.
 - (b) Risks and threats to information resources will be assessed, and security measures will be applied, based on the resource’s classification level, in accordance with CNCS risk management procedures.
 - (c) CNCS information systems will be categorized as one of the following:
 - (1) *Major Applications (MAs)* - An information system that requires special attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. An MA requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
 - (2) *General Support Systems (GSS)* - A GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people, and provides support for a variety of users and applications.

(3) *Minor Applications* – An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system and depend on the GSS for most of their security controls.

(d) Based on FIPS Publication 199, each CNCS information resource will be categorized based on level of potential impact to confidentiality, integrity and availability:¹

(1) The rating criteria for each security objective are shown in the following table:

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

(2) The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on CNCS operations, organizational assets, or individuals.

¹ Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- (3) The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on CNCS operations, organizational assets, or individuals.
- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- (4) The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on CNCS operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- (5) The categorization of a resource is expressed in the following format:
- $$\text{SC information type} = \{(\text{confidentiality}, \text{impact}), (\text{integrity}, \text{impact}), (\text{availability}, \text{impact})\}$$
- (e) The minimum categorization level of a system for each security objective (confidentiality, integrity, and availability) will be that of the highest categorized information resource contained in the system. (e.g., if the system contains both Medium and Low confidentiality items, the system confidentiality level must be at least Medium)
- (f) The overall categorization level of a system will be that of the highest of the levels specified for each security objective (e.g., if Confidentiality is Medium and Integrity and Availability are Low, the overall categorization of the system will be Medium).
- (g) CNCS' information resources will be categorized in accordance with NIST guidance, including FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems; Special Publication 800-60,

Guide For Mapping Types of Information and Information Systems to Security Categories; and subsequent relevant publications.

- (h) Security controls will be applied to CNCS information resources in accordance with the security categorization of each resource, as prescribed by FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems; Special Publication 800-53, Recommended Security Controls for Federal Information Systems; and other NIST guidance.

5. **ROLES & RESPONSIBILITIES:**

- (a) Information Owners are responsible for:
 - (1) Categorizing their resources in accordance with the guidance in this policy and NIST publications.
 - (2) Ensuring that their resources are protected commensurate with their categorization level.
- (b) Information Custodians are responsible for:
 - (1) Assisting Information Owners with categorizing resources they manage.
 - (2) Assisting Information Owners with implementing appropriate security controls for resources they manage.
- (c) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Providing guidance on the categorization of information resources.
 - (2) Auditing to ensure compliance with this policy.

6. **DEFINITIONS:**

- (a) Availability - Ensuring timely and reliable access to and use of an information resource
- (b) Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- (c) Federal Information System - An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
- (d) Information Resources – The equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.
- (e) Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- (f) **Information Type** - A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
- (g) **Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (e) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- (f) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (g) NIST Special Publication 800-60, Guide For Mapping Types of Information and Information Systems to Security Categories.
- (h) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

RISK MANAGEMENT

ISP-P-08-0905

1. **SUBJECT:** CNCS will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
2. **SCOPE:** This policy applies to all CNCS information resources.
3. **DESCRIPTION:** In determining a security strategy for a system or the organization, CNCS must determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business, while addressing financial and operational concerns. The objective of performing risk management is to enable CNCS to accomplish its mission by:
 - Better securing the IT systems that store, process, or transmit organizational information.
 - Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget.
 - Assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Risk management is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel for implementation. Effective risk management processes support sound *risk-based decision-making*. The CIO and other CNCS executives need to ensure implementation of an effective and comprehensive risk management program, which encompasses all segments of the enterprise, in order to support CNCS' mission.

4. **REQUIREMENTS:**

- (a) CNCS will use a risk-based approach to determine information security requirements to ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, CNCS information.
- (b) CNCS management will make information technology decisions based on a thorough analysis of the risks involved.
- (c) Risk management procedures must be integrated into CNCS' systems development life cycle (SDLC). Risk management is an iterative process and has

- activities relevant to every phase of the life cycle. Security considerations must be included in the initiation, development/acquisition, implementation, operation/maintenance, and disposal of all CNCS information resources.
- (d) Risk management is a cyclical process and must be performed on an ongoing basis for all information resources.
 - (1) A risk analysis must be performed before the design specifications for new systems are approved, whenever a significant change occurs to the system hardware or software, in response to a major security incident, after certification, and at least every three years.
 - (e) OMB policy requires that agencies conduct E-Authentication Risk Assessments on systems that are used to conduct electronic commerce. An E-Authentication Risk Assessment shall be conducted for all GSS and MAs and for Minor Applications that are not supported by a GSS. The completed E-Authentication Risk Assessment will be included in the Risk Assessment for a MA and a GSS and will be separately retained by the System Owner when completed for a Minor System. A copy of the completed E-Authentication Risk Assessment will be submitted to Chief Information Security Officer (CISO).
 - (f) Privacy Impact Assessments (PIAs) will also be conducted in accordance with CNCS Privacy policies to assess the privacy risks of each system.
 - (g) CNCS will adhere to NIST guidance as set forth in Special Publication 800-30 and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners and CNCS Executives are responsible for:
 - (1) Committing to performing on-going periodic risk management of information resources.
 - (2) Considering the results of a risk assessment in making decisions about the use of information resources.
 - (3) Implementing appropriate safeguards based on the results of risk analysis.
 - (4) Information Custodians are responsible for assisting with the assessment and mitigation of risks for the information resources with which they have been entrusted.
- (b) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Identifying potential threats to the confidentiality, integrity, and availability of CNCS information resources.
 - (2) Performing vulnerability testing in accordance with CNCS policies and procedures.
 - (3) Providing recommendations for the cost-effective mitigation of risks to information resources.

- (c) The CIO will ensure that risk management is incorporated into the IT decision process.

6. DEFINITIONS:

- (a) Availability - Ensuring timely and reliable access to and use of an information resource
- (b) Confidentiality - Preserving authorized restrictions on information access and disclosure, including a means for protecting personal privacy and proprietary information.
- (c) Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- (d) Risk – The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- (e) Risk Assessment - The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk.
- (f) Risk Management – The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:
 - (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- (g) Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
- (h) Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- (i) Vulnerability Testing – Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

(a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

(b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000

(c) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

(d) NIST Special Publication 800-30, Risk Management

(e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems

(f) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

(g) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

(a) Original Publication June 2007

(b) Reviewed and updated July 2008

(c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SYSTEM SECURITY PLANS

ISP-P-09-0905

1. **SUBJECT:** CNCS will develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
2. **SCOPE:** This policy covers all CNCS information systems.
3. **DESCRIPTION:** System Security Plans are critical for ensuring an appropriate level of security and risk mitigation for CNCS systems. A security plan lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures.
4. **REQUIREMENTS:**
 - (a) Each major application and general support system must have an approved System Security Plan before going into operation.
 - (1) Minor applications may be an appendix or addressed as part of the System Security Plan for the applicable general support systems or, in some cases, the applicable major application.
 - (b) Each System Security Plan must be reviewed and updated annually or when there is a major change to the system, whichever is earlier.
 - (c) NIST minimum security requirements and recommended security controls will be applied to each system based on the system's categorization level and documented in the SSP.
 - (d) System Security Plans will include a copy of or reference to the security configuration checklists used on the system.
 - (e) System Security Plans must be handled and controlled as sensitive information, and marked "NON-PUBLIC Contains Sensitive Information"
 - (f) System Security Plans will adhere to NIST guidance as set forth in Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems; Special Publication 800-53, Recommended Security Controls for Federal Information Systems; FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems; and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for:
 - (1) Ensuring that System Security Plans are developed for the systems that they own.
 - (2) Formally approving and accepting System Security Plans for their systems.
- (b) Information Custodians are responsible for assisting Information Owners with the development and implementation of System Security Plans.
- (c) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Providing guidance on development of System Security Plans
 - (2) Assisting with the review of System Security Plans.
 - (3) Auditing systems to ensure that their System Security Plans have been effectively implemented.

6. DEFINITIONS:

- (a) Accreditation – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- (b) Certification – A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- (c) General Support System – An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and applications.
- (d) Major Application – An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
- (e) Memorandum of Understanding (MOU) - A document providing a general description of the responsibilities that are to be assumed by two or more parties in their pursuit of some goal(s).
- (f) Minor Application – An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the

application. Minor applications are typically included as part of a general support system.

- (g) System Security Plan - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Circular A-123, Internal Control Systems, August 4, 1986
- (e) NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
- (f) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (g) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008

(c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

CERTIFICATION AND ACCREDITATION

ISP-P-10-0905

1. **SUBJECT:** CNCS will periodically assess the security controls of its information systems to determine if the controls are effective in their application, develop and implement plans of action designed to correct deficiencies, authorize the operation of organizational information systems and any associated information system connections, and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
2. **SCOPE:** This policy applies to all major applications (MA) and general support systems (GSS) at CNCS.
3. **DESCRIPTION:** The purpose of Certification and Accreditation (C&A) is to ensure that system owners have implemented adequate security controls commensurate with the level of risk. To this end, C&A is the formalized process used to assess the risks and security requirements of each system, and to determine whether the system's security needs are being met.

The Federal Information Security Management Act (FISMA) requires CNCS to perform C&A of its information systems. For each system, this process must be completed either every 3 years or when there is a change that affects the system's security posture, whichever comes first.

4. REQUIREMENTS:

- (a) All CNCS systems contained in the CNCS System Inventory will be examined at least annually to determine if they should be classified as a MA, GSS, or Minor Application, in accordance with the CNCS Security Categorization policy.
- (b) CNCS will designate a System Owner for each MA and GSS. The System Owner is responsible for ensuring that the MA/GSS for which they are responsible has in place an Approval to Operate (ATO). The System Owner is also responsible for maintaining a current System Security Plan (SSP) and other supporting documentation.
- (c) CNCS shall assign a senior executive to act as the Designated Approving Authority (DAA) for each major CNCS system to be C&A'd. The DAA is nominated by the Chief Information Officer (CIO) and appointed by the Chief Executive Officer (CEO). These appointments will be formally made in writing.
- (d) Each MA and GSS will have a designated Certification Agent (CA). The CA is responsible for providing a technical assessment of the system security requirements and evaluating the associated in place and planned security controls/countermeasures.

- (e) Each of CNCS' Major Applications (MA) and General Support Systems (GSS), will be certified and accredited every 3 years or upon each major change to the system (whichever comes first).
- (f) Information system security controls will be monitored on an ongoing basis to ensure the continued effectiveness of the controls.
 - (1) A subset of the systems security controls will be assessed annually to determine if they are effective.
 - Those security controls that are volatile or critical to protecting the information system must be assessed at least annually.
 - All other controls must be assessed at least once during the information system's three-year accreditation cycle.
 - (2) Plans of action will be developed and implemented to correct any determined deficiencies.
- (g) All new information systems will be Certified and Accredited prior to being placed into production operation.
- (h) Certification:
 - (1) CNCS shall implement a Certification program to test and assess technical and non-technical IT security features and other safeguards used by CNCS systems, in support of the Accreditation process.
 - (2) Certification shall not only address software and hardware security safeguards, but also procedures, physical protections, and personnel security measures.
 - (3) Security controls will be tested and evaluated during the Certification process to evaluate the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This will be performed in accordance with NIST guidance as specified in Special Publication 800-53A.
 - (4) The CA shall prepare a security assessment report. The security assessment report provides the findings of the assessor, recommendations for correcting any weaknesses or deficiencies in the security controls, and a summary providing the list of all security controls assessed and the overall status of each control.
- (i) Accreditation:
 - (1) CNCS shall implement an Accreditation process used for obtaining official management authorization for the operation of an IT system.
 - (2) Accreditation will be in the form of a formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards.

- (3) The Accreditation determination shall be based on findings, facts, and support documents produced during the Certification process, as well as other management considerations.
- (4) An Accreditation statement, which affixes security responsibility with the accrediting authority (DAA), will be used to certify that proper attention has been afforded to the security of the IT resource.
 - The statement shall address the residual risks associated with the respective system or network, subsequent to the implementation of countermeasures applied during the system test and evaluation.
- (j) The DAA will allow the System Owner to review the Certification and Accreditation statements before they are signed by the DAA.
- (k) An IATO may be issued in those cases in which systems must be implemented expeditiously, but the IATO should last no longer than 6 months and should only be granted if it does not pose a significant risk to CNCS information resources.
 - (1) The IATO must have an expiration date specified
 - (2) The system must be fully certified by the end of the IATO period. No extensions will be granted.
- (l) The assembled C&A Package will include the following:
 - (1) Appointment Letters for the DAA, System Owner, and Information System Security Officer (ISSO).
 - (2) System Categorization in accordance with the CNCS Security Categorization policy (ISP-P-07).
 - (3) Security Assessment Report
 - (4) Signed Accreditation Letter
 - (5) Risk Assessment in accordance with the CNCS Risk Management policy (ISP-P-08).
 - (6) System Security Plan developed in accordance with the CNCS System Security Plan policy (ISP-P-09).
 - (7) Interconnection Security Agreements (ISA) for each major system, external system, or general support system with which the system interfaces.
 - (8) E-Authentication Risk Assessment
 - (9) Privacy Impact Assessment in accordance with CNCS Privacy policy
 - (10) System Rules of Behavior
 - (11) A System POA&M containing any residual items that need to be resolved and their current status.
- (m) CNCS will adhere to NIST Certification and Accreditation guidance as set forth in Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) System Owners are responsible for:
- (1) Developing and maintaining the system security plan.
 - (2) Identifying all information systems for which they are the owner, and assisting the CISO with maintaining an accurate inventory of their systems.
 - (3) Categorizing their systems in coordination with the CISO.
 - (4) Ensuring that C&A requirements are met for any major information system(s) they own.
 - (5) Notifying the CISO when there is a major change to a major information system.
 - (6) Reviewing C&A statements before they are signed by the DAA.
 - (7) Addressing any remedial action that must be taken subsequent to the controls assessment.
 - (8) Maintaining Points of Contact and backups for their system's C&A activities.
 - (9) Obtaining C&A documentation, MOU's, and other relevant supporting documents for external system's they own in accordance with the CNCS External Systems policy.
 - (10) Ensuring that personnel involved in the management of security for their systems (including themselves, DAAs, and other relevant personnel) have sufficient information security training in order to make appropriate risk decisions regarding the C&A of the system.
 - (11) Ensuring that the system is deployed and operated according to the agreed-upon security requirements in the system security plan.
 - (12) Assembling the security accreditation package and submit it to authorizing official.
 - (13) Appointing an Information System Security Officer (ISSO) in writing for the system.
- (b) Information Custodians are responsible for:
- (1) Assisting information owners in ensuring that major information systems are certified.
 - (2) Assisting the CA with conducting the security controls assessment.
- (c) The Chief Information Security Officer (CISO) is responsible for:
- (1) Developing and communicating CNCS' C&A procedures
 - (2) Ensuring that all major information systems and general support systems have been certified and accredited
 - (3) Providing guidance on the development of System Security Plans.

- (d) Information System Security Officers are responsible for:
 - (1) Serving as the principal advisor to the authorizing official, information system owner, or CISO on all matters relating to the security of the information system.
 - (2) Assisting the System Owner with developing and updating the System Security Plan
 - (3) Helping to facilitate the Certification by providing documentation to the CA and coordinating with system administrators.
- (e) The Designated Approving Authority (DAA) is responsible for:
 - (1) Acting as the authorizing official for Accreditation of the systems they have been assigned.
 - (2) Completing and signing C&A statements and forwarding them to the CISO.
 - (3) Making and issuing final or interim decision on granting, conditionally granting, or denying authority to operate the system.
 - (4) Developing timeframes in which remedial actions must be taken.

6. DEFINITIONS:

- (a) Accreditation - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- (b) Approval to Operate (ATO) - Full accreditation (see above)
- (c) Certification - A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- (d) Contingency Plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of an emergency, such as a system failure or disaster.
- (e) Designated Approving Authority (DAA) – The senior management official or executive with the authority to approve the operation of an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
- (f) External System – Any system that is hosted outside of CNCS facilities.
- (g) General Support Systems (GSS) - A GSS is an interconnected set of information resources under the same direct management control that shares common

- functionality. It normally includes hardware, software, information, data, applications, communications, and people, and provides support for a variety of users and applications.
- (h) Information system – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
 - (i) Interconnection Security Agreement (ISA) - An agreement established between owners/operators of connected IT systems that documents the requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
 - (j) Interim Authority to Operate (IATO) – Temporary granting of authority to operate under certain conditions and for a specific limited period of time while issues preventing full accreditation are being addressed.
 - (k) Major Application (MA) - An information system that requires special attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. An MA requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
 - (l) Major change – Any change to the hardware, software, or firmware components of an information system that may have an impact on the protection capabilities of that system and the enforcement of the system security policy.
 - (m) Memorandum of Understanding (MOU) - A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.
 - (n) Privacy Impact Assessment (PIA) - An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
 - (o) Risk Assessment - The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk.
 - (p) System Security Plan - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000
- (c) NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- (g) Draft Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- (h) NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

CONTINGENCY PLANNING

ISP-P-11-0905

1. **SUBJECT:** CNCS will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for its information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
2. **SCOPE:** This policy applies to all mission-critical information resources.
3. **DESCRIPTION:** In addition to being a legal mandate for federal agencies, contingency planning is simply a good business practice, and part of the fundamental mission of CNCS as a responsible and reliable public institution. For the success of CNCS' programs, the agency's information systems must be made available within an appropriate period of time in the event of a disruption.

CNCS' information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While much vulnerability may be minimized or eliminated through technical, management, or operational solutions as part of CNCS' risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside CNCS' control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

4. **REQUIREMENTS:**

- (a) CNCS will develop and maintain viable IT contingency plans for its mission-critical systems.
 - (1) Contingency planning will yield documented plans on how CNCS would continue data processing if service, use, or access was disrupted for an extended period of time.
 - (2) The IT contingency plans will support the Corporation's Continuity of Operations (COOP) Plan.
- (b) Each major application will have its own Contingency/Disaster Recovery Plan.
- (c) Preventive measures will be identified to reduce the effects of system disruptions and increase system availability for critical systems.
- (d) Recovery strategies and procedures will be developed to ensure that systems may be recovered quickly and effectively following a disruption.

- (e) System contingency plans will address roles, responsibilities, and contact information for individuals involved in the contingency process.
- (f) CNCS will employ mechanisms and procedures to recover and reconstitute systems to a known secure state after a disruption.
- (g) Contingency plan testing and training will be performed to address deficiencies and to prepare Information Owners, Custodians, and Users for plan activation.
 - (1) Testing and training will occur at least annually or when a significant change occurs to CNCS' mission-critical systems.
- (h) Contingency plans will be reviewed regularly and updated as needed to remain current.
- (i) CNCS will adhere to NIST guidance as set forth in Special Publication 800-34, Contingency Planning Guide for Information Technology Systems and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Information Security Officer (CISO) is responsible for:
 - (1) reviewing system contingency plans to ensure they align with information security policies.
 - (2) monitoring the IT contingency planning process and reporting progress to management as required.
- (b) The Personnel Security Officer is responsible for reviewing contingency plans for alignment with the overall Corporation COOP plan.
- (c) Information Owners are responsible for:
 - (1) developing, reviewing, and testing system contingency plans for the systems they own.
 - (2) maintaining a list of the personnel involved in the disaster planning/recovery process, including their functions, roles, and assigned tasks.
 - (3) ensuring that system contingency plans are updated and tested annually.
 - (4) ensuring that personnel are adequately trained on the contingency plan.
 - (5) maintaining current copies of all contingency plans, tests, evaluations, and subsequent follow-up actions and making this information available as required.
- (d) Information Custodians are responsible for:
 - (1) working with Information Owners to develop contingency plans
 - (2) implementing contingency plans
 - (3) participating in contingency plan testing

6. DEFINITIONS:

- (a) Contingency Plan – Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
- (b) Continuity Of Operations Plan (COOP) – A predetermined set of instructions or procedures that describe how an organization’s essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.
- (c) Disaster Recovery Plan (DRP) – A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
- (d) Disruption – An unplanned event that causes the system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
- (e) Major Application – An information system that requires special management attention because of its importance to an agency mission (and in this case mission critical business processes).

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.
- (d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (e) NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems
- (f) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

- (g) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems
- (h) NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

INFORMATION PRIVACY**ISP-P-12-0905**

1. **SUBJECT:** CNCS will establish and maintain an Information Privacy Program to protect private information collected about individuals, organizations, and businesses.
2. **SCOPE:** This policy applies to everyone who uses or has access to CNCS information resources.
3. **DESCRIPTION:** Government agencies require that individuals provide information about their lives, financial status, health status, and other activities in support of the many missions assigned to them by Congress. This information may be required to support hiring actions for employees or to qualify for participation in various contract, grant, and volunteer activities. Individuals provide information to government agencies with the expectation that agencies will exercise due care to protect the information entrusted to their care from unauthorized access and will use that information only for the purpose for which it was provided.

The government has a responsibility to protect information entrusted to it. Individuals and businesses trust that agencies will protect the information that they provide to the government. If agencies lose that trust, they will not be able to complete their assigned missions. Recognizing the need for individuals to continue to voluntarily provide government with their personal information, Congress and the Office of Management and Budget (OMB) enacted laws and regulations requiring that federal agencies establish Privacy Programs to monitor the collection of personal information and to protect that information once it has been collected.

4. REQUIREMENTS:

- (a) CNCS will operate an Information Privacy program which includes the following:
 - (1) Information privacy policies and procedures with defined roles and responsibilities
 - (2) Role-based information privacy training
 - (3) Privacy incident reporting and response integrated with CNCS' information security Incident Response procedures.
- (b) CNCS will minimize the use and collection of privacy protected information to only what is necessary.
- (c) CNCS will identify privacy information and ensure that appropriate controls are implemented to protect the confidentiality of this information.
- (d) CNCS will perform periodic reviews to ensure that controls are adequately

- implemented.
- (e) Privacy Impact Assessments will be conducted on information systems in accordance with OMB guidance.
 - (f) Privacy notices will be developed and posted on CNCS web sites in machine readable format.
 - (g) CNCS will comply with all relevant Privacy laws, including those for the identification, protection, disclosure, and tracking of privacy information.
 - (h) CNCS will report on the status of information privacy at the Corporation as directed by OMB memoranda.
 - (i) The use and management of privacy information will comply with all CNCS Information Security policies.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Executive Officer (CEO) is responsible for:
 - (1) Ensuring that senior agency officials provide security for privacy information
 - (2) Delegating responsibility to appropriate agency officials to serve in Privacy roles.
- (b) The Senior Agency Official for Privacy (SAOP) is responsible for:
 - (1) Overseeing the development and implementation of the Information Privacy program
 - (2) Helping to promote Information Privacy within the Corporation.
 - (3) Reviewing documents and reports developed under the Privacy program
- (c) The Privacy Officer (PO) is responsible for:
 - (1) Developing the CNCS Information Privacy program, including assessing program requirements and developing a Privacy framework
 - (2) Providing Information Privacy training to staff
 - (3) Coordinating with appropriate CNCS staff for development and implementation of Information Privacy procedures
 - (4) Working with Information Owners to conduct Privacy Impact Assessments (PIAs) on CNCS systems
 - (5) Providing Information Privacy expertise and advice to CNCS staff
 - (6) Ensuring CNCS compliance with federal Privacy guidelines.
 - (7) Reporting on the Corporation's Information Privacy program
- (d) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Ensuring the protection of all Corporation information resources
 - (2) Working with the Privacy Officer to coordinate the Information Privacy

program with the CNCS Information Security Program

- (e) The Office of General Counsel (OGC) will:
 - (1) Provide guidance regarding Privacy law
 - (2) Review and approve Privacy Act notices, Privacy Impact Assessments, and other relevant documents
- (f) The Office of Human Capital (OHC) will ensure that appropriate personnel controls are implemented to protect privacy information
- (g) Information Owners are responsible for:
 - (1) Ensuring that their information resources comply with CNCS Information Privacy policies and procedures
 - (2) Assessing the use and collection of privacy information in their systems at least annually.
- (h) Supervisors are responsible for ensuring that their staff understand and are trained on CNCS Information Privacy policies and procedures
- (i) Information Users are responsible for:
 - (1) Completing information privacy training and ensuring that they understand and their privacy responsibilities
 - (2) Complying with CNCS information privacy policies and procedures.

6. DEFINITIONS:

- (a) Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- (b) Privacy Impact Assessment (PIA) - An analysis of how information is handled:
 - (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) Freedom of Information Act (5 U.S.C. § 552)
- (d) Section 208 of the E-Government Act of 2002 (44 U.S.C. Ch 36)
- (e) Children’s Online Privacy Protection Act (“COPPA”) (15 USC 6501-06)
- (f) Paperwork Reduction Act (PRA) of 1995 (44 USC 3501 et seq.)
- (g) Trade Secrets Act (18 USC 1905)
- (h) Health Insurance Portability and Accountability Act (HIPAA)
- (i) OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
- (j) OMB Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006)
- (k) OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information (July 12, 2006)
- (l) OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003
- (m) OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy (December 20, 2000)
- (n) OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000)
- (o) OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999)
- (p) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

ACCEPTABLE USE OF INFORMATION RESOURCES

ISP-P-13-0905

1. **SUBJECT:** Individuals using information resources belonging to the Federal government must act in a legal, ethical, responsible, secure manner, and with respect for the rights of others.
2. **SCOPE:** This policy applies to all users of CNCS information resources.
3. **DESCRIPTION:** Inappropriate use of information resources exposes CNCS to risks including compromise of systems and services, legal issues, financial loss, and damage to reputation. The purpose of this policy is to protect CNCS' staff and the government from illegal or damaging actions by individuals, either knowingly or unknowingly.

Access to computers, computing systems and networks owned by the government is a privilege which imposes certain responsibilities and obligations, and which is granted subject to CNCS policies and guidelines, and governing laws. This policy sets forth the principles that govern appropriate use of information resources, and is intended to promote the efficient, ethical and lawful use of these resources.

4. REQUIREMENTS:

- (a) Information Users shall use CNCS-provided information resources for CNCS-related business in accordance with their job functions and responsibilities, except as otherwise provided by other CNCS policies.
- (b) Users are permitted limited personal use of information resources if the use does not result in a loss of employee productivity, does not interfere with official duties or CNCS business, and involves minimal additional expense to the government.
- (c) When using government information resources, Users are expected to:
 - (1) Act responsibly so as to ensure the ethical use of CNCS information resources in compliance with the Standards of Ethical Conduct for Federal Employees.
 - (2) Acknowledge the right of CNCS to restrict or rescind computing privileges at any time.
 - (3) Use security measures to protect the confidentiality, integrity, and availability of information, data, and systems.
 - (4) Refrain from using government information resources for activities that are inappropriate or unprofessional.
 - (5) Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information.

- (6) Use good judgment in accessing the Internet. Each use of the Internet should be able to withstand public scrutiny without embarrassment to CNCS or the federal government.
 - (7) Safeguard their user IDs and passwords, and use them only as authorized. Any actions taken under an assigned identification (*e.g.*, userid) are the responsibility of the user.
 - (8) Respect government property.
 - (9) Make only appropriate use of data to which they have access.
 - (10) Exercise good judgment regarding the reasonableness of personal use.
 - (11) Use information resources efficiently.
- (d) The following activities are strictly prohibited:
- (1) Intentionally corrupting, misusing, or stealing software or any other computing resource.
 - (2) Accessing sensitive CNCS information resources that are not necessary for the performance of the employee's duties.
 - (3) Making unauthorized changes to CNCS computer resources, including installation of unapproved software or hardware.
 - (4) Copying CNCS proprietary software or business data for personal or other non-government use.
 - (5) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CNCS does not have an active license.
 - (6) Disseminating trade secrets or business sensitive information, except as permitted by law or regulation.
 - (7) Unauthorized access to other computer systems using CNCS information resources.
 - (8) Accessing information resources, data, equipment, or facilities in violation of any restriction on use.
 - (9) Using government computing resources for personal or private financial gain. Examples include, but are not limited to, using resources to perform work for another job, operating a personal business, stock trading, selling items on auction sites, etc.
 - (10) Using another person's computer account, with or without their permission, unless you are performing authorized systems administration for that person and they are present to supervise the usage.
 - (11) Implementing any computer systems without authorization from OIT.
 - (12) Knowingly, without written authorization, executing a program that may hamper normal CNCS computing activities.

- (13) Introducing malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, e-mail bombs, etc.).
 - (14) Revealing account passwords to others or allowing the use of one's account by others, including family and other household members.
 - (15) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
 - (16) Unauthorized security scanning, network monitoring, or data interception that is not part of the employee's regular job duties.
 - (17) Circumventing or interfering with any CNCS information security measures.
 - (18) Interfering with or denying service to other information resource users.
 - (19) Providing information about, or lists of, CNCS staff to parties outside of the government that are not required for CNCS business.
 - (20) Sending spam.
 - (21) Any form of harassment via email, telephone, pager, IRC, SMS, or other communication method, whether through language, frequency, or size of messages.
 - (22) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
 - (23) Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity without specific permission from CNCS.
 - (24) Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment.
 - (25) Using government office equipment or information resources for activities that are illegal, inappropriate, or offensive to fellow staff or the public. This includes, but is not limited to, materials related to:
 - Sexually explicit or sexually oriented content
 - Ethnic, racial, sexist, or other offensive comments
 - Anything that is in violation of sexual harassment or hostile workplace laws
 - Fraud
 - Gambling
 - Illegal weapons or terrorist activities
 - Planning or commission of any crime
 - (26) Forging or misrepresenting one's identity.
- (e) Auditing and Privacy:

- (1) All use of CNCS information resources may be monitored by CNCS.
- (2) Users do not have any expectation of privacy or anonymity while using any government information resource at any time, including accessing the Internet and email.
- (3) Users agree to be governed by acceptable usage policies and to have their usage audited. By using government office equipment, users imply their consent to disclosing the contents of any files or information maintained or passed-through government office equipment.
- (4) To the extent that staff wish that their private activities remain private, they should avoid using government office equipment such as their computer, telephone, the Internet, or E-mail, for those activities.
- (5) Auditing procedures will be implemented to ensure compliance with CNCS security policies.
- (6) System administrators have the ability to audit network logs, employ monitoring tools, and perform periodic checks for misuse.
- (f) Users agree to be bound by the following conditions for continued use of CNCS information resources:
 - (1) Users will sign an agreement to comply with CNCS information security policies (Rules of Behavior).
 - (2) Personnel with administrative access or elevated privileges to any IT resources will sign an Elevated Privileges Usage Agreement.
- (g) Usage of CNCS IT resources for illegal purposes will be reported to appropriate authorities.

5. ROLES & RESPONSIBILITIES:

- (a) Information Users are responsible for:
 - (1) Using information resources responsibly and in compliance with all CNCS information security policies and guidelines.
 - (2) Reporting any suspected inappropriate use of information resources to either their manager or the ISSO.
- (b) Supervisors are responsible for:
 - (1) Ensuring that their personnel understand CNCS policy regarding acceptable usage of information resources.
 - (2) Monitor their staff's use of information resources.
 - (3) Taking appropriate action when notified of inappropriate usage by their staff.
- (c) Information Owners are responsible for implementing measures to protect their resources against inappropriate use.
- (d) Information Custodians are responsible for:

- (1) Assisting information owners with implementing measures to protect their resources against inappropriate use.
- (2) Reporting to the CISO any inappropriate usage that they discover.
- (e) The Chief Information Security Officer (CISO) is responsible for auditing usage of the CNCS information resources to ensure compliance with policies and guidelines.

6. DEFINITIONS:

- (a) Access - The right to enter or make use of a computer system. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.
- (b) Administrative Access – Enhanced privilege level that allows the user to perform administration of the system.
- (c) Account - A set of privileges for authorization to system access, which are associated with a userid.
- (d) Audit Trail - A record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
- (e) Copyrighted software - software for use only in accordance with licensing agreements.
- (f) Information Custodians - Individuals (*e.g.*, IT staff) who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource.
- (g) Information Owner - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
- (h) Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.
- (i) Information Users - Individuals who use or have access to CNCS' information resources, including employees, vendors, and visitors.
- (j) Password - Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).
- (k) Personal Use - Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.
- (l) System Administrator - A designated individual who has special privileges to maintain the operation of a computer application or system.

(m) Unauthorized Access - The use of an information resource without permission.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS:

(b) User Rules of Behavior

(c) Information Custodian Rules of Behavior

10. AUTHORITY:

(a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

(b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

(c) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(d) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(e) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(f) 5 C.F.R. Part 735, Employee Responsibilities and Conduct

(g) 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

(h) Part 1 of Executive Order 12674, Implementing Standards of Ethical Conduct for Employees of the Executive Branch

(i) Title 17, U.S. Code, Section 106

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

(b) Original Publication June 2007

(c) Reviewed and updated July 2008

(d) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

Elevated Privileges/Information Custodian Agreement

It is the responsibility of all CNCS information users to comply with information security policies and procedures. Persons entrusted with responsibilities for administering information systems have a particularly important role in protecting these systems. By signature below, the user hereby acknowledges and agrees to the following:

1. As a person who has responsibilities for the development, maintenance, or administration, of an information resource, I am an "information custodian" (custodian) under CNCS' information security program. .
2. I acknowledge I have been granted enhanced privileges in order to perform specific administrative functions on specific CNCS information systems, and that these privileges are only to be used in order to perform my assigned job responsibilities.
3. I will not use my privileges to grant myself or any other persons unauthorized privileges, or to modify any access accounts, privileges, system configurations, or data in an unauthorized manner.
4. I accept that I have a special duty to safeguard CNCS information resources, and will implement and operate appropriate measures to protect those resources.
5. I will report all potential incidents I discover to the CISO and system owner.
6. I will exercise maximum care in protecting the elevated access credentials with which I have been entrusted.
7. I agree to abide by CNCS' information security policies and the "CNCS Information Security Handbook," and perform the responsibilities assigned to information custodians..
8. I understand that access privileges to CNCS information systems may be changed or revoked at the discretion of management, and may be modified as roles and responsibilities change.
9. This document may be amended from time to time. CNCS will notify me of amendments. I will keep abreast of amendments as they are made available.
10. I understand that anyone found to violate these policies is subject to disciplinary and/or legal action, including but not limited to:
 - Loss or limitation of use of information resources,
 - Termination of employment, and/or
 - Referral for criminal prosecution.

ACKNOWLEDGMENT: CNCS INFORMATION TECHNOLOGY POLICY

Information Custodian's Signature

Date

Print Information Custodian's Name

Employee / Contractor / Grantee
(circle one)

INFOSEC POLICY WAIVERS**ISP-P-14-0905**

1. **SUBJECT:** CNCS will have a formal process for evaluating and granting waivers to security policies.
2. **SCOPE:** This policy applies to all users and systems.
3. **DESCRIPTION:** CNCS information security policies have been developed in accordance with federal guidance and will be implemented consistently to ensure effectiveness. However, there are occasional circumstances in which it is not completely feasible or in the best interests of the Corporation to comply with a particular policy provision or to do so within a particular timeframe. In such cases, a formal waiver process is needed evaluate and approve exceptions to the policies. These waivers will be granted in rare situations under specific circumstances and will be based on an analysis of risk.
4. **REQUIREMENTS:**
 - (a) In circumstances where it is not feasible or prudent to comply with a particular information security policy, a waiver request may be submitted to the CISO.
 - (1) For systems, the request should be submitted by the system owner.
 - (b) The CISO will provide a waiver request form template for use by persons requesting a waiver.
 - (c) The waiver request must provide:
 - (1) A legitimate justifiable reason for waiving a security requirement.
 - (2) The specific scope and circumstances of the waiver (e.g., time period of waiver, specific resources or persons for which the requirement is waived, etc.)
 - (3) An understanding of the risks involved
 - (4) A recommendation for compensating security control(s) to mitigate the risk resulting from the waiver.
 - (d) The CISO, in consultation with applicable personnel (e.g., the CIO, CFO, General Counsel, etc.) will evaluate and respond to waiver requests.
 - (1) In the specific cases prescribed by federal guidance that require signature of the agency head for a particular waiver situation, the request will be escalated to the CEO.

- (2) Waivers of policy provisions that are recommended but not strictly required (as specified in the policy language) will be addressed through the Certification and Accreditation risk acceptance process rather than via a formal policy waiver. (see ISP-P-10)
- (e) Waiver requests will be evaluated based on the following criteria:
 - (1) Waivers will only be granted if it is within the Corporation's right to do so. Waivers cannot be approved that would violate legal requirements.
 - (2) An assessment of whether the reason for the waiver is truly accurate and justified, and whether there are alternatives for meeting the requirement that could be pursued.
 - (3) An analysis of the risks and proposed mitigation strategy
- (f) Each waiver is approved for a specific period of time.
 - (1) Upon expiration of the granted waiver period, the waiver can be submitted for renewal if it is still needed.
 - (2) If a waiver is not renewed prior to the expiration of the period specified in the waiver, it will cease to be in effect at the end of the period.
 - (3) If you or your system simply need additional time to implement a policy, your waiver request should include the amount of time you need to achieve compliance.
 - (4) Waivers granting exceptions to policies (rather than delays) will be good for a period of 1-3 years depending on the nature of the exemption. This will allow for periodic re-evaluation of the need for the waiver.
- (g) Waivers are not intended to be used to pardon offenses that have already been committed. Requests are to be submitted as far in advance as possible.

5. ROLES & RESPONSIBILITIES:

- (a) All personnel are responsible for:
 - (1) Submitting and obtaining approval of waiver requests when compliance with a policy provision is not feasible or prudent for the Corporation.
 - (2) Requesting waivers only when absolutely needed and justified.
 - (3) Providing the required information for each waiver request.
 - (4) Abiding by the terms of the approved waiver.
 - (5) Complying with all policies unless granted an approved waiver.
- (b) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Reviewing and responding to waiver requests in a timely manner.
 - (2) Assessing waiver requests in accordance with the above specified criteria.

- (3) Escalating waiver requests to appropriate Corporation personnel when necessary.
- (c) Corporation officials (including the CIO, CFO, CEO, General Counsel, and other personnel) are responsible for assisting with the assessment and approval of waivers as requested.

6. DEFINITIONS:

- (a) Accreditation - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- (b) Certification - A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- (c) Policies - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
- (d) Risk - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- (e) Security Controls - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) NIST Special Publication 800-100, Information Security Governance

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (d) Original Publication June 2007
- (e) Reviewed and updated July 2008
- (f) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SERVER SECURITY

ISP-S-01-0905

1. **SUBJECT:** Servers should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all CNCS information servers, including file and print servers, application servers, and database servers. All operating systems associated with these servers are also included.
3. **DESCRIPTION:** No server should ever be placed on the production network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.
4. **REQUIREMENTS:**
 - (a) Standard base security configurations will be developed for and applied to each type of server. These baselines will conform to NIST guidance or other appropriate federal standards if not available from NIST.
 - (b) Enhanced security will be applied to servers that require higher levels of security due to the sensitivity or criticality of the data and services that they provide.
 - (c) Where possible, security configurations will be enforced through automated policies (such as Windows Group Policies).
 - (d) Server images will be scanned to ensure they have been securely configured before they are placed into production.
 - (e) System patches and security updates must be applied in a timely fashion in accordance with the CNCS Patch Management policy.
 - (f) Any unnecessary services will be disabled (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).
 - (g) Access to all CNCS servers must adhere to the CNCS Access Control and Identification and Authentication policies.
 - (h) Auditing and logging must be enabled in accordance with CNCS auditing policies and procedures.
 - (i) All servers must run approved antivirus software configured in accordance with CNCS antivirus policies and procedures.
 - (j) Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.

- (k) Each server must be inventoried and tracked in accordance with CNCS asset management policies and procedures.
- (l) Each server's configuration must be thoroughly documented, and this documentation must be kept up to date.
- (m) Any changes made to the configuration of a server must be performed in accordance with CNCS change management policies and procedures.
- (n) Servers will be located in access-controlled and environmentally protected facilities, in accordance with CNCS physical and environmental security policies and procedures.
- (o) Procedures will be implemented to provide verifiable backups of all servers, in accordance with CNCS data backup policies and procedures.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any servers they own are in compliance with the guidelines provided by this policy.
- (b) Information Custodians are responsible for assisting Information Owners with implementing the guidelines provided by this policy.
- (c) The Chief Information Security Officer (CISO) is responsible for auditing servers to ensure that they are configured in accordance with the guidelines provided by this policy.

6. DEFINITIONS:

- (a) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.
- (b) Patch – An additional piece of code developed to address a problem in an existing piece of software.
- (c) Server – Computer that provides a service or application that users access through a network connection.
- (d) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (d) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (g) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (h) NIST Special Publication 800-123, Guide to general Server Security

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

NETWORK SECURITY

ISP-S-02-0905

1. **SUBJECT:** Network devices and connectivity components should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all routers, switches, and other network components that are part of CNCS' connectivity infrastructure.
3. **DESCRIPTION:** It takes only one incorrectly configured system to allow an intruder into CNCS' network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.
4. **REQUIREMENTS:**
 - (a) Standard baseline security configurations will be developed for each type of network component (*i.e.* routers, switches, etc.) and applied to all such components.
 - (1) CNCS will adhere to NIST hardening guidance for routers and other networking components.
 - (b) The level of security applied to each network component should be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.
 - (c) Patches and security updates must be applied in a timely fashion in accordance with CNCS patch management procedures.
 - (d) Any unnecessary services will be disabled.
 - (e) Access to all CNCS network devices must adhere to the CNCS Access Control and Identification and Authentication policies.
 - (f) Remote administration of network devices can only be performed using encrypted and authenticated connections.
 - (g) Logging must be enabled in accordance with CNCS auditing policies and procedures.
 - (h) Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network or device.
 - (i) Each device must be inventoried and tracked in accordance with CNCS asset management policies and procedures.

- (j) Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.
- (k) Any changes made to the configuration of a device must be performed in accordance with CNCS change management policies and procedures.
- (l) Physical access to Network devices will be controlled in accordance with CNCS physical and environmental security policies.
- (m) No network device may be connected to the CNCS network without approval from the Deputy CIO.
- (n) No non-CNCS computers (e.g., contractor-owned or personal laptops) may be directly connected to the CNCS network without special approval from the Deputy CIO or CISO.
- (o) Appropriate controls will be implemented to protect against or limit the effects of denial of service attacks.
- (p) CNCS will implement appropriate controls to protect the confidentiality and integrity of information transmitted over the network, and will explicitly accept the additional risk when sufficient controls are not feasible.
- (q) Domain Name Service
 - (1) CNCS will comply with federal DNSSec requirements, including NIST SP 800-81.
 - (2) Name/address resolution systems will provide data origin and integrity information along with the authoritative information they return.
 - (3) Systems providing name/address resolution service for the organization will be fault tolerant and will implement role (e.g., internal vs. external) separation.

5. **ROLES & RESPONSIBILITIES:**

- (a) Information Owners are responsible for ensuring that any network components they own are in compliance with the guidelines provided by this policy.
- (b) Information Custodians are responsible for assisting information owners with implementing the guidelines provided by this policy.
- (c) The Chief Information Security Officer (CISO) is responsible for auditing network components to ensure that they are configured in accordance with the guidelines provided by this policy.

6. **DEFINITIONS:**

- (a) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (e.g., anti-virus software), tuning the operating system, and documenting the system.
- (b) Network Device – Any physical component which forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

- (c) Patch – An additional piece of code developed to address a problem in an existing piece of software.
- (d) Router – A device that interconnects networks and directs and filters traffic between them.
- (e) Switch – A physical component that connects multiple computers and devices to a network.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (d) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (g) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (h) NIST Special Publication [SP800-81](#), Secure Domain Name System (DNS) Deployment Guide

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

WIRELESS SECURITY

ISP-S-03-0905

1. **SUBJECT:** When using wireless connectivity, CNCS should use its risk management processes to assess the risks involved with that particular technology, to take steps to reduce those risks to an acceptable level, and to ensure that a satisfactory level of protection is maintained.
2. **SCOPE:** This policy covers all wireless data communication devices connected to CNCS networks or which are used to transmit or store CNCS data.
3. **DESCRIPTION:** Many CNCS users have found that wireless communications and devices are convenient, flexible, and easy to use. From sending email on a handheld device to using wireless connectivity in their homes, users can benefit from the increased flexibility and availability of wireless access. There may also be potential opportunities to utilize wireless LAN and WAN connectivity in the CNCS office environment.

In addition to the risks that apply to all networks, wireless connectivity is exposed to additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users. Additionally, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to CNCS networks via the hijacked device.

Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

4. **REQUIREMENTS:**
 - (a) The use of any wireless connectivity or wireless device for accessing or transmitting CNCS information must be approved by OIT.
 - (1) Wireless networking will not be used on the CNCS production network.
 - (b) All CNCS wireless devices must be labeled and inventoried.
 - (1) Users must report any lost or stolen wireless or handheld devices to their supervisor or the CISO immediately.
 - (2) Access to CNCS and other systems and networks must be immediately terminated for any lost or stolen devices.

- (c) Access to any CNCS systems or networks using wireless devices or wireless networks must be authenticated.
 - (1) Handheld wireless devices that provide data services must have an inactivity lockout with a pin/password.
- (d) Robust cryptography must be used whenever sensitive data is stored or transmitted on a wireless device.
- (e) Security risks and controls should be evaluated more frequently for wireless technologies than for other networks and systems.
- (f) Periodic security testing and assessment should be performed for any CNCS wireless networks.
- (g) Ongoing, randomly timed security audits should be used to monitor and track wireless and handheld devices.
- (h) Patches and security enhancements should be applied to wireless networks in accordance with CNCS system security policy.
- (i) The SSID for each device should be configured such that it does not reveal any identifying information about CNCS.
- (j) Inherent security features such as authentication and encryption methods that are available in wireless technologies should be tested and used.
- (k) CNCS will adhere to NIST guidance as set forth in Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Users are responsible for:
 - (1) Adhering to CNCS procedures and guidelines regarding the use of wireless technologies, both within CNCS and when connecting to CNCS from remote locations.
 - (2) Safeguarding wireless devices in their possession.
 - (3) Safeguarding CNCS information resources being accessed or transmitted via any wireless technology.
 - (4) Promptly reporting the loss or theft of wireless devices, or any other breach of wireless security, to their supervisor or OIT.
- (b) System Owners are responsible for:
 - (1) Using CNCS risk management procedures to ensure that risks have been analyzed and appropriately mitigated prior to, and during, use of any wireless technology resources that they own.
 - (2) Obtaining security approval prior to deploying any wireless technologies.

- (3) Communicating wireless security policies and procedures to the users of their resources.
- (c) System Custodians are responsible for:
 - (1) Safeguarding wireless information resources with which they have been entrusted.
 - (2) Adhering to CNCS policies and procedures for the administration of wireless devices, including:
 - Labeling all wireless devices prior to deployment.
 - Maintaining an inventory of all wireless devices.
 - Disabling access or service for wireless devices that have been lost or stolen.
- (d) The Chief Information Security Officer (CISO) is responsible for auditing the use of wireless technologies at CNCS.

6. DEFINITIONS:

- (a) Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- (b) Cryptography – A coding method in which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format by someone with a secret key) using an algorithm. Cryptography is used to send or store information securely.
- (c) Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.
- (d) Service Set Identifier (SSID) – A unique identifier that acts as a password on a wireless network.
- (e) Wireless Technology – Any type of connectivity that transmits data without the use of physical cabling. Wireless systems include radio transmissions, satellite links, cell phones, and devices such as wireless headphones. Infrared (IR) devices such as remote controls, cordless computer keyboards, and cordless mouse devices are also included.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices.
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (e) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (f) NIST Special Publication 800-97, Establishing Wireless robust Security Networks: A Guide to IEEE 802.11i
- (g) NIST Special Publication 800-121, Guide to Bluetooth Security

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

WORKSTATION SECURITY

ISP-S-04-0905

1. **SUBJECT:** Workstations must be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all CNCS owned or managed workstations. This policy does not apply to external workstations not under CNCS control.
3. **DESCRIPTION:** No workstation should ever be placed on the network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the workstations must continually be updated to maintain security vigilance.
4. **REQUIREMENTS:**
 - (a) Standard base security configurations will be developed for and applied to each workstation operating system version (e.g., Windows XP, Windows 2000) used by CNCS. These baselines will conform to NIST guidance or other appropriate federal standards if not available from NIST.
 - (b) Enhanced security will be applied to workstations that require higher levels of security due to the sensitivity of the data and services that they access/provide (e.g., badging workstation).
 - (c) Where possible, security configurations will be enforced through automated policies (such as Windows Group Policies).
 - (d) Workstation images will be scanned to ensure they have been securely configured before they are placed into production.
 - (e) System patches and security updates must be applied in a timely fashion in accordance with the CNCS Patch Management policy.
 - (f) Access to all CNCS workstations must adhere to the CNCS Access Control and Identification and Authentication policies.
 - (g) Audit trails must be enabled in accordance with CNCS auditing policies and procedures.
 - (h) All workstations must run approved antivirus software configured in accordance with CNCS antivirus policies and procedures.
 - (i) Each workstation must be inventoried and tracked in accordance with CNCS asset management policies and procedures.

- (j) Changes made to the workstation baselines must be performed in accordance with CNCS change management policies and procedures.
- (k) CNCS will prevent remote activation of collaborative computing devices, such as video and audio conferencing capabilities, and will ensure that such devices provide an explicit indication to users when they are activated.
- (l) CNCS will comply with Federal Desktop Core Configuration requirements.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any workstations they own are in compliance with the guidelines provided by this policy.
- (b) Information Custodians are responsible for assisting Information Owners with implementing the guidelines provided by this policy.
- (c) The Chief Information Security Officer (CISO) is responsible for auditing workstations to ensure that they are configured in accordance with the guidelines provided by this policy.

6. DEFINITIONS:

- (a) Audit Trail - A record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
- (b) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.
- (c) Patch – An additional piece of code developed to address a problem in an existing piece of software.
- (d) Workstation – Includes desktop computers, laptops, and other computers used to access CNCS systems.

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

- 8. POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

- 9. ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals.
- (d) NIST Special Publication 800-43, Systems Administration Guidance for Windows 2000 Professional.
- (e) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (g) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (h) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

WEB SECURITY

ISP-S-05-0905

1. **SUBJECT:** Web servers and web-based systems should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all CNCS owned or managed web servers and web-based systems.
3. **DESCRIPTION:** No system should ever be placed on the production network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the web systems must continually be updated to maintain security vigilance.
4. **REQUIREMENTS:**
 - (a) Standard base security configurations will be developed for and applied to each web server platform (e.g., Windows IIS, Apache, etc.) used by CNCS. These baselines will conform to NIST guidance or other appropriate federal standards if not available from NIST.
 - (b) Enhanced security will be applied to web systems that require higher levels of security due to the sensitivity of the data and services that they access/provide.
 - (c) Where possible, security configurations will be enforced through automated policies (such as Windows Group Policies).
 - (d) System patches and security updates must be applied in a timely fashion in accordance with the CNCS Patch Management policy.
 - (e) Audit trails must be enabled in accordance with CNCS auditing policies and procedures.
 - (f) Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the system.
 - (g) Changes made to the web systems must be performed in accordance with CNCS change management policies and procedures.
 - (h) Appropriate controls will be developed, documented, and implemented effectively to protect the integrity and availability of publicly accessible CMS information and applications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any web systems they own are in compliance with the guidelines provided by this policy.
- (b) Information Custodians are responsible for assisting Information Owners with implementing the guidelines provided by this policy.
- (c) The Chief Information Security Officer (CISO) is responsible for auditing systems to ensure that they are configured in accordance with the guidelines provided by this policy.

6. DEFINITIONS:

- (a) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.
- (b) Patch – An additional piece of code developed to address a problem in an existing piece of software.
- (c) Web Server - A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, Transport Control Protocol (TCP)/Internet Protocol (IP), and the Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an “intranet server.”
- (d) Web System – A web server or web-based service or application that runs on a web server

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. **POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

9. **ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-95 (Draft), Guide to Secure Web Services.

- (d) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (e) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (f) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (g) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (h) NIST Special Publication 800-95, Guide to Secure Web Services

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

DATABASE SECURITY**ISP-S-06-0905**

1. **SUBJECT:** Securing information, so that it remains consistent, complete, and accurate, is essential to CNCS' reputation, mission, and critical business objectives.
2. **SCOPE:** This policy applies to all CNCS databases.
3. **DESCRIPTION:** CNCS has been entrusted with a variety of sensitive data to accomplish its goals. The success of Corporation programs depends on the availability, integrity and confidentiality of this data. In order to protect this data, CNCS must implement data security measures, such as data validation and verification controls. These controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets the expectations about its quality and that it has not been altered.
4. **REQUIREMENTS:**
 - (a) Data will be secured commensurate with its level of sensitivity and criticality.
 - (b) Only the individual designated as an Oracle Database Administrator (DBA) shall have network and Oracle accounts with DBA rights and privileges.
 - (c) Databases, and applications that interface with databases, will be configured in accordance with security best practices:
 - (1) Integrity verification programs, such as consistency and reasonableness checks, shall be used to look for evidence of data tampering, errors, and omissions.
 - (2) Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure software and data have not been modified.
 - (3) If users are allowed to make updates to a database via a web page, these updates should be validated to ensure that they are warranted and safe.
 - (4) For databases containing sensitive information, table access controls should be applied. Access to specific information within the database should be limited to only those personnel who need access to that information, and access should be limited to only those functions (e.g., read, write, modify, etc.) required for the person to perform his or her duties.
 - (5) Database servers should be configured to only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).
 - (6) For sensitive data, audit trails should be created and maintained within the

database to track transactions and provide accountability.

- (7) Securing sensitive information by selectively encrypting data within the database is encouraged.
- (d) Programs or utilities that may be used to maintain and/or modify sensitive databases and other software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully controlled.
- (e) Databases containing non-public information should never be on the same physical machine as a web server.
- (f) Integrity errors and unauthorized or inappropriate duplications, omissions, and intentional alterations will be reported to the Information Owner.
- (g) Database servers and database software must adhere to all CNCS information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.
- (h) CNCS will follow NIST guidance regarding database security.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for the following for data that they own:
 - (1) Ensuring the confidentiality, integrity, and availability of the data.
 - (2) Ensuring that data integrity and validation controls are installed, operated and maintained.
 - (3) Authorizing and limiting access to data they own.
 - (4) Reporting database security incidents to the CISO.
- (b) Information Custodians are responsible for:
 - (1) Assisting Information Owners with maintaining the confidentiality, integrity, and availability of their data.
 - (2) Assisting Information Owners with implementing the prescribed database security controls.
 - (3) Immediately reporting breaches of database security to the Information Owner and the CISO.
- (c) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Providing guidance to Information Owners and Custodians regarding database security.
 - (2) Auditing CNCS databases, servers, and applications to ensure compliance with this policy.
- (d) Information Users are responsible for:
 - (1) Not accessing data that they are not authorized to access and/or for which they do not have a legitimate business need to know.

- (2) Exercising due diligence to prevent accidental misentry, modification or deletion of data.
- (3) Immediately reporting any security incidents.

6. DEFINITIONS:

- (a) Availability - Ensuring timely and reliable access to and use of an information resource
- (b) Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- (c) Data - A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.
- (d) Database - An organized collection of logically related information stored together in one or more computerized files.
- (e) Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- (f) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
- (g) Validation - The checking of data for correctness and/or for compliance with applicable standards, rules, and conventions.
- (h) Verification - The process of ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. **POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

9. **ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.

- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook." October 1995.
- (d) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

MOBILE COMPUTING

ISP-S-07-0905

1. **SUBJECT:** Laptops and other mobile computing devices require additional security controls to mitigate the risks posed by using them outside the CNCS office environment.
2. **SCOPE:** This policy applies to all laptops and other mobile computing devices that are used to store or process CNCS data.
3. **DESCRIPTION:** The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow CNCS personnel to be more productive. However, the use of these devices outside of the CNCS office poses risks to those devices, the information they contain, and the systems to which they connect. These devices may also present a hazard to other CNCS resources upon their return to the CNCS office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of the CNCS network which lack the protections afforded by CNCS' corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.
4. **REQUIREMENTS:**
 - (a) Laptops and other mobile computing devices must be inventoried and tracked.
 - (b) Laptops must use approved antivirus software.
 - (c) Access to mobile devices which store or transmit sensitive data, or which can be used to connect to other sensitive CNCS systems, must be authenticated.
 - (d) All security policies applied in the CNCS office environment must also be applied when using or connecting to CNCS resources outside the CNCS office environment.
 - (e) Mobile computer users are responsible for backing up their data that is stored on the mobile computer on a regular basis.
 - (f) All data on mobile computers/devices which carry agency data must be encrypted unless the data is determined to be non-sensitive, in writing, by the CEO or an individual he/she may designate in writing.
 - (g) Mobile devices must abide by ISP-S-08 Remote Access when connecting to CNCS systems from outside CNCS' offices.

- (h) The loss of a mobile computing device must be reported immediately in accordance with the CNCS Incident Reporting policy.
- (i) CNCS will adhere to NIST guidance as set forth in Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any mobile computing resources they own are being managed and used in accordance with the procedures and guidelines set forth in this policy.
- (b) Information Custodians are responsible for assisting information owners with managing and protecting their mobile computing devices, including inventorying and tracking them, as well as defining security countermeasures (such as encryption technologies) that will be applied.
- (c) Information Users are responsible for:
 - (1) Taking all reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
 - (2) Backing up the data stored on their laptop.
 - (3) Immediately reporting the loss, theft, tampering, unauthorized access, or damage of any mobile device covered by this policy.
 - (4) Following any encryption procedures provided by information custodians.
- (d) The Chief Information Security Officer (CISO) is responsible for auditing the use of mobile computing devices to ensure compliance with the procedures and guidelines set forth in this policy.

6. DEFINITIONS:

- (a) Antivirus Software – Software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus caused.
- (b) Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- (c) Mobile Computing Device – A laptop, PDA, or other *portable* device that can store or process data.
- (d) Personal Firewall – Software installed on a computer or device which helps protect that system against unauthorized access.

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
- (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (g) NIST Special Publication 800-124, Guidelines on Cell Phone and PDA security

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

REMOTE ACCESS**ISP-S-08-0905**

1. **SUBJECT:** Remote access requires additional security controls to mitigate the increased risks posed by allowing connectivity from outside the CNCS network.
2. **SCOPE:** This policy applies to all remote connectivity to CNCS information resources other than public facing systems designed specifically to be accessed from outside CNCS (such as CNCS public websites).
3. **DESCRIPTION:** Remote access to the CNCS network provides many benefits. It allows personnel traveling on business to connect to CNCS information resources and provides the capability for telecommuting. However, remote access to CNCS poses a risk of intrusion into the CNCS network by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of CNCS also lacks the protections afforded by CNCS' corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.
4. **REQUIREMENTS:**
 - (a) All remote connectivity must be authenticated using at least "two-factor authentication where one of the factors is provided by a device separate from the computer gaining access"¹ (such as the use of passwords in conjunction with tokens).
 - (b) Only authorized personnel will be allowed remote access to CNCS systems.
 - (1) Employees will apply for remote access via the process defined in CNCS' telecommuting policy.
 - (2) Contractors and other non-CNCS personnel may be granted remote access only when necessary to perform their CNCS work. Their remote access must be approved by both their CNCS COTR/Supervisor and the system owner.
 - (c) Remote access is limited to those systems with a FIPS 199 classification of Low or Moderate.
 - (d) Remote access to a system, and any applications contained therein, will only be allowed upon authorization of the System Owner and/or the DAA.
 - (e) All sensitive information transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.

¹ OMB Memorandum M-06-16, Protection of Sensitive Agency Information

- (f) All security policies for use in the CNCS office environment must also be observed when using or connecting to CNCS resources while outside the CNCS office environment.
- (g) Any personal equipment, including personal home computers, used to connect to CNCS' information resources must meet CNCS remote access requirements, including having an approved antivirus program installed and configured with the latest updates.
- (h) CNCS sensitive data is not to be stored on any non-CNCS computers.
- (i) It is the responsibility of employees to ensure that their access accounts and remote connections are not used by unauthorized persons (including family members).
- (j) To prevent unauthorized users from accessing sensitive CNCS information via open sessions, CNCS information users should log out rather than hang up after completing a remote session. They should also wait until they receive a confirmation of their log-out command from the remotely connected CNCS machine before they leave the computer they are using.
- (k) Session time-outs will be used to disconnect idle sessions after an inactivity period of no more than 30 minutes.
- (l) CNCS will adhere to NIST guidance as set forth in Special Publication 800-46, Security for Telecommuting and Broadband Communications, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any remote access to their information resources is conducted in accordance with the procedures and guidelines set forth in this policy.
- (b) Information Custodians are responsible for assisting information owners with implementing the guidelines outlined in this policy.
- (c) Information Users are responsible for:
 - (1) Protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons.
 - (2) Immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of CNCS computer hardware, software, or data that has been entrusted to their care.
- (d) The Chief Information Security Officer (CISO) is responsible for auditing the use of remote access to ensure compliance with the procedures and guidelines set forth in this policy.

6. DEFINITIONS:

- (a) Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- (b) Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.
- (c) Remote Access – Any access to CNCS’ corporate network through a network, device, or medium that is not controlled by CNCS (such as the Internet, public phone line, wireless carrier, or other external connectivity).
- (d) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy
- (e) Strong Authentication - An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (f) OMB Memo M-99-20, Security of Federal Automated Information Resources, June 1999.

- (g) NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications
- (h) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (i) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (j) NIST Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access
- (k) NIST Special Publication 800-113, Guide to SSL VPNs

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

TELEPHONE SECURITY**ISP-S-09-0905**

1. **SUBJECT:** CNCS telephony resources are subject to the same security requirements and protections as other information resources.
2. **SCOPE:** This policy governs the use of telephones, modems, VoIP equipment, and other telephony resources at CNCS.
3. **DESCRIPTION:** Telephone services are intended to support the objectives and operations of CNCS, and are critical to fulfilling CNCS' mission. These telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.
4. **REQUIREMENTS:**
 - (a) When using the CNCS phone system or CNCS-issued cellular phones, users should adhere to the following guidelines to protect the information communicated:
 - (1) Understand that there should be no expectation of privacy when using these resources.
 - CNCS may audit use of these resources.
 - It is possible for third parties to tap or redirect phone calls outside of CNCS.
 - (2) No sensitive data should ever be discussed over a mobile phone because of the ease of intercepting such communications.
 - (3) Make sure that the person on the other end of the conversation is who they say they are. Do not give out sensitive information (including agency credit card information) unless you are sure of the person on the other end of the line.
 - (4) Be cautious when discussing sensitive information that the conversation cannot be overheard by unauthorized persons (such as visitors to CNCS). Minimize use of speakerphones.
 - (5) Obey relevant laws regarding the recording of phone conversations, including informing the other party that you are recording.
 - (6) Follow CNCS' Acceptable Use policy in using phone resources, just as you would with email or other information resources.
 - (b) The agency VoIP and other critical telephony components must be protected:

- (1) This equipment should be stored in a secure, environmentally controlled location in accordance with CNCS physical security policy.
 - (2) Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, Auditing, Patch Management, Server Security, Network Security, etc.
 - (3) Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk, and criticality/sensitivity of those resources.
- (c) The use of mobile phones and PDAs must comply with CNCS' wireless and mobile device security policies.
- (d) Modems or other telephony equipment may not be installed without the explicit approval of the Deputy Chief Information Officer.
- (e) Analog Phone Lines - As a rule, the following applies to requests for fax and analog lines. Waivers to the policy will be granted on a case-by-case basis.
- (1) Fax machines must be placed in centralized administrative areas designated for departmental use, and away from other computer equipment.
 - (2) The fax line is used solely for the fax machine that it has been assigned to.
 - (3) Only persons authorized to use the analog line have access to it.
 - (4) When not in use, analog lines are to be physically disconnected from the computer.
 - (5) Computer-to-Analog Line Connections - The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within CNCS will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the agency, and active penetrations have been launched against such lines by hackers. Waivers to the policy will be granted on a case-by-case basis.
 - Requesting an Analog/ISDN Line - Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to OIT:
 - (i) A clearly detailed business case of why other secure connections available at CNCS cannot be used.
 - (ii) The business purpose for which the analog line is to be used.
 - (iii) The software and hardware to be connected to the line and used across the line.
 - (iv) The sensitivity of the data to be transferred over the line.
 - (v) To what external connections the requester is seeking access.
 - (vi) A description of where the analog line will be placed.
 - (vii) Whether dial-in from outside of CNCS will be needed.

- (6) Lines must be terminated as soon as they are no longer in use.
 - (7) Computers are not to be connected to both an analog line and the CNCS network simultaneously.
- (f) Voice over IP (VoIP)
- (1) When feasible Voice and Data should be logically separated onto different subnets.
 - Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VOIP firewall protection
 - At the voice gateway, which interfaces with the PSTN, H.323, SIP, or other VOIP protocols should be disallowed from the data network.
 - Use strong authentication and access control on the voice gateway system, as with any other critical network component.
 - (2) A mechanism to allow VOIP traffic through firewalls is required.
 - Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call.
 - VOIP-ready firewalls and other appropriate protection mechanisms should be employed.
 - (3) Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
 - If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. See the CNCS Encryption policy (ISP-C-15) for requirements.
 - (4) Physical controls are especially important in a VOIP environment and should be deployed accordingly.
 - (5) Additional power backup systems may be required to ensure continued operation during power outages.
 - (6) The security features that are included in VOIP systems are to be enabled, used, and routinely tested.
 - (7) The use of “softphone” systems, which implement VOIP using an ordinary PC with a headset and special software, should be tightly limited.
 - (8) If mobile units are to be integrated with the VOIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).
 - (9) CNCS will maintain awareness of and compliance with laws regarding the interception or monitoring of VOIP lines, and retention of call records.
- (g) CNCS will adhere to NIST guidance as set forth in Special Publication 800-24, PBX Vulnerability Analysis; 800-58, Security Considerations for Voice Over IP Systems, and other publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for deploying, managing, and protecting their telephony resources in compliance with CNCS information security policy.
- (b) Information Custodians are responsible for assisting information owners with deploying, managing, and protecting their telephony resources in compliance with CNCS information security policy.
- (c) The Chief Information Security Officer (CISO) is responsible for auditing the use and management of CNCS telephony resources to ensure compliance with CNCS information security policies.
- (d) Employees are responsible for using CNCS telephony resources in an ethical, responsible, and secure manner, in accordance with this policy and existing CNCS policies.

6. DEFINITIONS:

- (a) Analog - A method of transmitting information in a continuous fashion via energy waves.
- (b) ISDN - A type of communication line which can carry voice, digital network services and video.
- (c) Modem - A device that enables a computer to transmit data over telephone lines by converting data between the computer's digital format and the phone line's analog format.
- (d) Private Branch Exchange (PBX) - A private telephone switchboard that provides on-premises dial service and may provide connections to public communications networks.
- (e) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
- (f) Telephony - The technology associated with the electronic transmission of voice, fax, or other information between distant parties using systems historically

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.
- (d) NIST Special Publication 800-24, PBX Vulnerability Analysis
- (e) NIST Special Publication 800-58, Security Considerations for Voice Over IP Systems
- (f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (g) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

ELECTRONIC MAIL SECURITY

ISP-S-10-0905

1. **SUBJECT:** Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.
2. **SCOPE:** This policy applies to the use of any CNCS information resource to transmit, receive or store electronic mail, as well as use of any non-CNCS email systems to transfer CNCS data.
3. **DESCRIPTION:** Electronic mail is an essential tool used by CNCS to conduct its business. Email is a vital method of exchanging messages and data files over computer networks.

However, email is inherently insecure and presents many risks to CNCS information security. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to CNCS resources. Information users might also send inappropriate, proprietary, or other sensitive information via email, thus exposing CNCS to legal action or damage to its reputation. After web servers, an organization's mail servers are typically the most frequent targets of attack. Therefore, it is crucial to take prudent security precautions in administering and using email.

4. **REQUIREMENTS:**
 - (a) Information Users must understand that email can be intercepted or altered without the knowledge of the sender or recipient when it is transferred over the Internet.
 - (b) Sensitive information may not be sent over the Internet (via email or other means) without being encrypted. Sensitive information should be encrypted when transferred outside of the CNCS network.
 - (c) CNCS personnel should only send CNCS data using CNCS owned or operated email systems. CNCS information users should not forward sensitive CNCS email or attachments to their personal email accounts. When these messages are stored on other email systems and servers, including that of someone's personal internet service provider (ISP), CNCS cannot protect the data or prevent the ISP or email system provider from accessing the data.
 - (d) Information users are prohibited from using any CNCS email systems (or any other email systems accessed from CNCS computers) for prohibited purposes, as outlined in CNCS' Acceptable Use of Information Resources policy.

- (e) Information users may not direct unauthorized or personal messages to the All CNCS distribution group or other large groups of users. The sending of spam is prohibited.
- (f) The following procedures should be used to avoid potential damage caused by email-borne computer viruses:
 - (1) All incoming emails must be scanned for viruses in accordance with the CNCS Antivirus policy.
 - (2) The Corporation will employ spam filtering tools to minimize potentially harmful unsolicited email.
 - (3) Information users should not open attachments or click on links in messages from senders they do not know.
 - (4) Information users should report all suspicious emails to the CNCS Help Desk.
 - (5) Emails containing executable attachments are to be filtered and quarantined from entering the CNCS network.
- (g) To minimize spam, information users should avoid using their CNCS email addresses for personal correspondence on the Internet, particularly if they do not know or have a trust relationship with the other party. This especially includes giving out one's official email address to Internet shopping sites and mailing lists.
- (h) As discussed in the Acceptable Use policy, information users shall have no expectation of privacy while using CNCS' email system.
- (i) CNCS will adhere to NIST guidance as set forth in Special Publication 800-45, Guidelines on Electronic Mail Security, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any email system they own, and the data they own which is transmitted via email, adhere to this policy and its associated procedures and guidelines.
- (b) Information Custodians are responsible for assisting information owners in implementing the procedures and guidelines specified in this document.
- (c) Information Users are responsible for adhering to the procedures and guidelines provided in this document.
- (d) The Chief Information Security Officer (CISO) is responsible for auditing email systems and usage to ensure compliance with the procedures and guidelines provided in this document.

6. DEFINITIONS:

- (a) Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

- (b) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
- (c) Spam – Unauthorized and unsolicited electronic mass mailings.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) 5 U.S.C. 552A, Records Maintained on Individuals and The Privacy Act of 1974, as amended
- (d) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (e) NIST Special Publication 800-45, Guidelines on Electronic Mail Security.
- (f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

APPLICATION SECURITY

ISP-S-11-0905

1. **SUBJECT:** Applications must be made secure before placing them into the CNCS operational information technology environment, and security must be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all CNCS applications, including custom developed and Commercial-Off-The-Shelf (COTS) applications.
3. **DESCRIPTION:** No application should ever be placed on a production server or workstation without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the applications must continually be updated to minimize risk.
4. **REQUIREMENTS:**
 - (a) Security will be incorporated into all phases of the application lifecycle in accordance with the CNCS System Development Lifecycle (SDLC) Security policy.
 - (b) Applications will be categorized in accordance with CNCS' Security Categorization policy and secured commensurate with the level of categorization.
 - (c) Each application's configuration must be thoroughly documented, and this documentation must be kept up to date.
 - (d) Any changes made to the configuration of an application must be performed in accordance with CNCS change control policies and procedures.
 - (e) Application patches and security updates must be applied in a timely fashion in accordance with the CNCS Patch Management policy.
 - (f) Audit trails should be enabled in accordance with CNCS auditing policies and procedures for any application that processes or stores sensitive information.
 - (g) Any reports containing sensitive information that are generated must be marked with an appropriate header or footer, such as "Sensitive Information – For Official Use Only".
 - (h) Applications will identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.
 - (1) The structure and content of error messages will be carefully considered as part of the design of any application.

- (2) Error messages generated by the system will provide timely and useful information, without divulging potentially harmful information to unauthorized persons (i.e. information that could be used to exploit the system).
- (3) Sensitive information (e.g., account numbers, SSNs, passwords, etc.) will not be shown in any error messages or error logs.
- (i) Applications will prevent unauthorized and unintended information transfer via shared resources by controlling object reuse (information remnance).
 - (1) No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.
- (j) User interface services (e.g., web services) shall be physically or logically partitioned from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any applications they own are in compliance with the guidelines provided by this policy.
- (b) Information Custodians are responsible for assisting Information Owners with implementing the guidelines provided by this policy.
- (c) The Chief Information Security Officer (CISO) is responsible for auditing applications to ensure that they are managed in accordance with the guidelines provided by this policy.

6. DEFINITIONS:

- (a) Application - A self-contained software program designed to perform a defined set of tasks for a user, such as word processing, communications, or database management.
- (b) Audit Trail - A record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
- (c) Change Control - Documented procedures used to control the revision of applications, operating systems, and hardware configurations in computing environments.

- (d) Patch - An additional piece of code developed to address a problem in an existing piece of software.
- (e) Systems Development Lifecycle - The system development life cycle (SDLC) starts with the initiation of the system planning process, and continues through system acquisition/development, implementation, operations and maintenance, and ends with disposition of the system.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.
- (c) Homeland Security Presidential Directive / HSPD-7, December 17, 2003.
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (e) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

EXTERNAL SYSTEMS

ISP-S-12-0905

1. **SUBJECT:** CNCS must ensure the security of external systems operated on behalf of the Corporation.
2. **SCOPE:** This policy applies to external systems that contain CNCS information, or which operate, use, or have access to federal information on behalf of CNCS. This does not apply to systems or services that do not have access to or contain federal information or do not operate on behalf of CNCS.
3. **DESCRIPTION:** FISMA and OMB guidance require agencies to ensure the security of all systems that are operated on their behalf or which have access to the agency's data. These systems must meet FISMA requirements and follow NIST guidance as would internal agency systems.
4. **REQUIREMENTS:**
 - (a) CNCS will maintain an inventory of all external systems managed or used on behalf of the Corporation.
 - (b) A CNCS employee will be assigned as the CNCS Information Owner for the external system and will be responsible for coordinating with the external system operator to ensure compliance with this policy. This will generally be someone from the business unit that owns the contract or uses the external system.
 - (c) CNCS will have a signed Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) with the operator of each external system that has a direct interconnection with a CNCS operated system.
 - (1) These documents will adhere to the requirements specified in NIST Special Publication 800-47.
 - (d) CNCS will follow NIST guidance, including Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, regarding connecting to external systems.
5. **ROLES & RESPONSIBILITIES:**
 - (a) Information Owners are responsible for:
 - (1) Obtaining a signed MOU with the external system operator for any external system they own.
 - (2) Providing system inventory info to OIT and keeping it updated.

- (3) Ensuring that any external systems they own are in compliance with this policy.
 - (4) Obtaining a signed ISA for any CNCS system they own which interfaces with an external system.
 - (5) Forwarding any incident reports they receive regarding the external system to the CNCS CISO.
- (b) The Chief Information Security Officer (CISO) is responsible for:
- (1) Reviewing MOUs, ISAs, and other security documents for external systems to verify they meet CNCS needs
 - (2) Providing guidance to CNCS system owners regarding external systems

6. DEFINITIONS:

- (a) Accreditation - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- (b) Certification - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- (c) Contingency Plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
- (d) Contractor - Any non-Federal employees working on any U.S. Government contract
- (e) External System – Any system that is hosted outside of CNCS facilities.
- (f) Interconnection Security Agreement (ISA) - An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
- (g) Memorandum of Understanding (MOU) - A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.
- (h) Privacy Impact Assessment (PIA) - An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic

information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (d) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (e) NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

EMERGING TECHNOLOGY

ISP-S-13-0905

1. **SUBJECT:** CNCS must assess and mitigate risks associated with any new technology prior to initiating its use at the Corporation.
2. **SCOPE:** This policy applies to all emerging technologies to be used at the Corporation, including hardware, software, and connectivity services.
3. **DESCRIPTION:** Technology is constantly evolving. Along with new functionality and the promise of enhanced productivity, new technology also presents new risks to CNCS information. These risks must be assessed and appropriately mitigated before emerging technologies are introduced into the Corporation. Emerging technologies should not be installed without careful consideration of the security issues introduced by them.

“An especially challenging security environment is created when new technologies are deployed. Risks often are not fully understood, administrators are not yet experienced with the new technology, and security controls and policies must be updated. Therefore, agencies should carefully consider such issues as their level of knowledge and training in the technology, the maturity and quality of their security practices, controls, policies, and architectures, and their understanding of the associated security risks.” (NIST SP 800-58)

4. REQUIREMENTS:

- (a) Prior to implementing any emerging technology into the CNCS production information technology environment, a risk analysis will be performed to ensure that the technology does not introduce undue risk to the Corporation’s information and systems.
- (b) The new technology will be assessed to determine:
 - (1) Whether any other federal government entity is using it, and if so, with what level of success, and what security issues they have encountered
 - (2) Whether the technology is really ready for production use. For example, if new bugs, vulnerabilities, and patching are being introduced at a fast rate, adoption of the technology should be delayed
 - (3) Whether there is sufficient benefit to the use of this technology over more established technologies to warrant the additional risks.
- (c) CNCS will determine whether it can acceptably manage and mitigate the risks to its information and operations due to the proposed technology.

- (d) The proposed technology will first be tested and evaluated in a non-production environment before being recommended for production use.
- (e) Use of the technology will be documented and evaluated as part of the CNCS system development lifecycle procedures, including:
 - (1) Development/Update of a System Security Plan
 - (2) Development/Update of a system Risk Assessment
 - (3) Completion of Certification and Accreditation
- (f) CNCS will stay abreast of vulnerabilities reported for the new technology and take steps to address them in a timely fashion, in accordance with the CNCS Vulnerability Remediation and Patch Management policies.
- (g) CNCS will adhere to NIST and OMB guidance regarding the security of emerging technologies.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for:
 - (1) Performing a risk assessment for the emerging technology they wish to implement.
 - (2) Submitting the risk assessment and a technology proposal to the Technical Review Board
 - (3) Updating the System Security Plan, Certification and Accreditation (C&A), and other security documentation for any existing system that will incorporate the emerging technology
 - (4) Developing a System Security Plan, and undergoing Certification & Accreditation for any new system.
- (b) Information Custodians are responsible for:
 - (1) Assisting the Information Owner with performing risk assessment
 - (2) Testing the technology in a non-production environment
 - (3) Assisting the Information Owner with developing/updating the System Security Plan
- (c) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Providing guidance regarding the assessment and mitigation of risks associated with emerging technologies
 - (2) Reviewing risk assessments and other security documents for the systems incorporating the emerging technology
 - (3) Performing C&A of systems

6. DEFINITIONS:

- (a) Emerging Technology - A new technology not yet fully exploited by businesses
- (b) Risk - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- (c) Risk Assessment - The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (d) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

NETWORKED COPIER SECURITY**ISP-S-14-0905**

1. **SUBJECT:** Networked copiers should be made secure before placing them into the CNCS operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all copiers that are connected to a CNCS computer network.
3. **DESCRIPTION:** "The networked copier that all companies have in the hallway or backroom is no longer the 'old school' device most IT managers still assume it to be. On the contrary, it's quickly evolved into a sophisticated computing platform that can grant access into the heart of the network. Copiers have been reborn as document distribution centers, enabling users to scan paper and send images via email or to, for example, document management, financial, or human resources systems. Integration with business applications allows for efficient distribution, editing, and storage of what was traditionally paper-based information. However, most networked copiers have not been secured in the same rigorous way as other end points, such as mobile devices and office workstations. In many companies, network-attached copiers could be used to distribute unauthorized documents or even distribute documents using identities that impersonate company executives."¹

"The most common threats to digital copiers and printers stem from intruders stealing the hard drives containing confidential data, or reprinting documents directly from the machine after the earlier print command was canceled... Today's multifunctional copiers and printers store documents in memory... They might not just retain the last job, but the last 20 to 30."²

This policy addresses the security issues related to the use of networked copiers.

4. REQUIREMENTS:

- (a) Configure the copier to require authentication in order to access the administrator or core configuration functions on the copier.
 - (1) It is recommended that copiers also be configured to require network passwords for all functions to prevent unauthorized persons from accessing

¹ "Seven Deadly Sins of Copier Security", Bill DeStefanis, AIIM E-DOC Magazine, February 9, 2007

² IT Administrators May Be Overlooking Copier/Printer Security Risks, Marcia Savage, ChannelWeb, August 2001

them.

- (2) Configure the copier to log out the user after a brief period of inactivity.
- (3) Employ intruder lockout features.
- (b) Where possible, configure the copier to encrypt any scanned documents before transmitting them across the network.
- (c) Configure the copier to securely delete temporary files rather than keeping them in memory. This will protect sensitive documents that have been copied or scanned. This should include automatic clearing of hard drives, RAM, and flash memory.
- (d) Configure an audit trail on the copier to track all user activity including copying, printing, scanning, etc.
- (e) Allow documents to be sent from the copier only to CNCS email addresses and internal applications (i.e. don't allow send from copier directly to outside CNCS).
- (f) Prevent access to/from the copier from outside the firewall except through CNCS VPN.
- (g) Copier operating system vulnerabilities should be tracked and addressed, including the periodic implementation of patches, like any other device on the network.
- (h) Copiers must not be simultaneously connected to both the network and a phone line (for faxing) as this could provide a hacker with access into the network from the phone line.
- (i) When selecting new copiers, the risks and vulnerabilities inherent in each model should be considered as part of the selection criteria. Things to look for include:
 - (1) Resistant to viruses and Denial of Service attacks
 - (2) Less vulnerable operating systems.
 - (3) SSL and other encryption options.
 - (4) Ability to automatically securely delete documents from memory
 - (5) Robust access control features.
 - (6) Build in firewall capabilities
 - (7) Common Criteria certification
 - (8) Consider buying any additional security kit offered by the vendor.
- (j) Security features that are provided with the copier should be activated to the greatest extent possible.
 - (1) If the copier has internal firewall features, filtering should be configured to prevent unauthorized use both incoming and outgoing.
 - (2) If the copier has a hard drive encryption feature, use it.
- (k) Securely dispose of the copier when it is no longer needed.

- (1) CNCS security and privacy policies apply to copiers as they would to any other system/device on the network.

5. ROLES & RESPONSIBILITIES:

- (a) The CNCS owner of a networked copier is responsible for:
 - (1) Selecting copiers with sufficient security features
 - (2) Ensuring that the copiers are configured securely in accordance with this policy.
 - (3) Ensure that the acquisition and disposal of the copier complies with CNCS policies.
- (b) Information Users are responsible for using copiers only as authorized and in accordance with CNCS' security and privacy policies, including compliance with intellectual property laws.

6. DEFINITIONS: None

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication July 2008
- (b) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

ACCESS CONTROL**ISP-C-01-0905**

1. **SUBJECT:** Access to CNCS information resources will be limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
2. **SCOPE:** This policy applies to all CNCS information users, owners, and custodians, as well as access to any CNCS information resources.
3. **DESCRIPTION:** Users must have access to the information resources required to do their jobs. However, excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability for negligence in protecting those resources. Therefore, access to specific resources is only to be granted to authorized personnel who have a legitimate need to use those resources, and their access privileges will be limited to those required to perform their duties.
4. **REQUIREMENTS:**
 - (a) Users must be granted specific access privileges on each system, limited to those required to perform their job functions.
 - (b) Users must be authorized by the information owner prior to being granted access to a particular resource.
 - (c) The principles of separation of duties and least privilege will be applied to the allocation of access rights.
 - (d) Users will only access resources to which they have been authorized, regardless of actual system permissions.
 - (e) Users will not circumvent the permissions granted to their accounts in order to gain access to unauthorized information resources.
 - (f) Users will protect their own accounts:
 - (1) Users will not allow anyone else to use their account, or use their computers while logged in under their account, except as required for system administration by the Help Desk.
 - (2) When leaving their computer unattended, users will either log out or invoke a password-protected screensaver.
 - (3) Users are responsible for any activity initiated by their own userID.

- (g) The level of access control will depend on the classification of the resource and the level of risk associated with the resource.
- (h) Criteria must be established for account eligibility, creation, maintenance, and expiration for each system.
- (i) Procedures will be implemented for outgoing or transferring employees. These shall include, but are not limited to, the following:
 - (1) The removal of access privileges, computer accounts, and authentication tokens.
 - (2) The return of any CNCS information resources (property or data).
 - (3) Procedures for unfriendly termination (when needed) that include the immediate removal of all access.
- (j) Information Owners and Custodians (i.e. system administrators) will periodically review user privileges and modify, revoke, or deactivate as appropriate, based on the above criteria, at least quarterly.
- (k) Inactivity timeouts will be implemented for systems with a FIPS 199 categorization of moderate or higher.
 - (1) The timeout period will be set to the minimum time period feasible for the particular system, but will not exceed one hour.
- (l) Information systems will display an appropriate notification message (aka Warning Banner) before granting access to the system. The message will inform users (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.
- (m) Controls will be implemented to protect the authenticity of communications sessions. Where needed, session-level protections, such as encryption, will be used to secure sessions.
- (n) Access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information will be restricted to explicitly authorized personnel. This includes access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for:
 - (1) Determining who should have access to their resources.

- (2) Establishing and maintaining procedures for authorizing access to information systems and data for which they are responsible.
 - (3) Ensuring that their resources are protected against unauthorized access.
 - (4) Periodically reviewing access permissions.
 - (5) Ensuring that information users have undergone appropriate background checks and security training, as specified in policies ISP-C-06 and ISP-P-02.
- (b) Information Custodians are responsible for:
- (1) Assisting information owners with controlling access to their resources.
 - (2) Promptly removing access from a system when requested.
 - (3) Reporting any unauthorized accesses that they discover.
- (c) Information Users are responsible for:
- (1) Adhering to CNCS procedures for obtaining and removing access to information resources for themselves.
 - (2) Safeguarding their access credentials.
 - (3) Accessing only those resources for which they are authorized and using information in accordance with job function and agency policy.
 - (4) Immediately reporting suspected violations of this policy to their supervisor or the CISO.
 - (5) Providing immediate notification to their supervisor when it is known they are to leave CNCS employment, transfer to another position, or otherwise need to change the basis for which access to a CNCS information system has been granted.
- (d) Supervisors are responsible for:
- (1) Adhering to CNCS procedures for obtaining and removing access to information resources for their staff.
 - (2) Ensuring that their staff are authorized to access the resources needed to perform their duties.
 - (3) Immediately notifying the CISO or OIT Help Desk when access privileges or accounts are to be removed or modified.
 - (4) Immediately reporting suspected violations of this policy.
- (e) The Chief Information Security Officer (CISO) is responsible for:
- (1) Auditing to ensure compliance with the requirements specified in this policy.
 - (2) Ensuring that all personnel are trained on their computer security responsibilities.
- (f) The CNCS Facility Security Officer (FSO) is responsible for ensuring that staff and contractors have undergone the appropriate background checks.

6. DEFINITIONS:

- (a) Access – The right to enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of specific information resources.
- (b) Access Control – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.
- (c) Access Privilege (Privilege) – A specific activity that a user has been granted access to perform on an information resource (e.g. view or modify).
- (d) Account – A set of privileges for authorization to system access, which are associated with a UserID.
- (e) Authorization – The formal granting of access to an individual to perform certain activities.
- (f) Information Owner - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
- (g) Least Privilege – Granting users only the minimum privileges required to provide the level of access needed to perform their official duties.
- (h) Separation of Duties – Concept that provides the necessary checks and balances to mitigate against fraud, errors and omissions by ensuring that no individual or function has control of the entire process.
- (i) System Permissions – The technical configuration that provides an individual the ability to perform certain actions on information resources.
- (j) UserID – Character string (i.e. logon name) that uniquely identifies a computer user.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
- (f) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

IDENTIFICATION AND AUTHENTICATION

ISP-C-02-0905

1. **SUBJECT:** CNCS will identify information users, processes acting on behalf of users, and devices; and verify the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information resources.–Access to CNCS information systems (other than those specifically designed to provide public information) will only be granted to identified and authenticated users.
2. **SCOPE:** This policy applies to all CNCS owned or operated information systems.
3. **DESCRIPTION:** In order to ensure that unauthorized persons do not have access to sensitive CNCS information resources, it is necessary to first establish the identity of the user who is attempting to access the resource. Access controls can then be used to allow or limit access based on the established user identity.

The specific method(s) of authentication used for each system shall be commensurate with the level of sensitivity of the system to be accessed (*i.e.* more sensitive systems should use stronger authentication methods). Multiple authentication methods (*e.g.* use of both a password and a token) may be required for high-sensitivity or high-risk situations.

4. REQUIREMENTS:

- (a) Each CNCS system shall incorporate proper user authentication and identification to ensure that access is not granted to unauthorized persons. Users will not have access to CNCS information resources without identifying and authenticating themselves (*i.e.* “logging on”).
- (b) CNCS will develop and follow detailed procedures for the creation, removal, and modification of user accounts and authentication credentials for each system. These procedures will also address automatic termination of temporary and emergency accounts; disabling of inactive accounts; automated mechanism(s) to audit account creations, modification, disabling, and termination actions;
- (c) User accounts must adhere to the following guidelines:
 - (1) Allow only one user per account; User IDs are never to be shared.
 - (2) Never activate a guest account. Remove any guest accounts that are created by default by the system unless absolutely required and approved by the system owner and the CISO.
 - (3) No accounts will be named with easily guessed generic names (such as “anonymous”, “guest”, “admin”, “ftp”, “telnet”, “www”, “host”, “user”,

- “test”, “bin”, “nobody”, etc.) unless absolutely technically required by the system.
- (4) Default accounts that are present upon initial installation of the system should be removed or renamed unless technically required by the system to keep the name.
 - (5) Accounts should be deactivated immediately upon termination of user.
 - (6) Unused accounts will be deactivated on at least a monthly basis.
 - (7) Accounts for contractors and other temporary staff will be configured to expire on the final date of their contract/employment, or 1 year from activation, whichever is earlier.
- (b) Administrator accounts must adhere to the following guidelines:
- (1) The names of the administrator accounts should be renamed, if possible, to make it more difficult for attackers to guess the names of these accounts.
 - (2) Each person who has a legitimate need to use Administrator privileges should have their own separate administrative account that they will use to perform administrative functions. Usage of the main administrator account for each system should be limited to emergencies, and is to be limited to specific designated OIT staff. This will protect the main administrator account and also provide an audit trail of administrative activities.
 - (3) All accounts with administrator privileges must have strong passwords or other alternative strong authentication methods.
- (d) If passwords are used for authentication, they must adhere to the CNCS Password Management policy.
- (e) If authentication methods other than passwords (e.g., biometrics, smartcards, tokens, etc) are used, then:
- (1) They must be approved by the CISO and the CIO.
 - (2) Additional policies and procedures will be developed to govern their usage.
- (f) Account credential information (e.g., User IDs, passwords) that are stored on devices (such as enable passwords in router configuration files) must be encrypted.
- (g) To preclude brute force attacks, an intruder lockout feature must be implemented on each system to temporarily suspend the account after several invalid logon attempts.
- (h) Session lock/termination features should be used to lock or terminate sessions after a designated period of inactivity.
- (i) New users should complete basic information security training and sign the User Rules of Behavior prior to being given their account credentials.
- (j) System administrators must sign the Elevated Privileges Agreement prior to receiving administrative credentials.

- (k) CNCS will have documented procedures for account management, including establishing, activating; modifying, reviewing, disabling, and removing accounts on each system.
- (l) The Chief Information Security Officer and Deputy Chief Information Officer have the authorization to disable user accounts due to administrative or security reasons, based upon a written or verbal request from a Department head.
- (m) CNCS will restrict access to authentication data. Authentication data will be protected with access controls and encryption to prevent unauthorized individuals from obtaining the data.
- (n) CNCS will adhere to NIST guidance as set forth in NIST Special Publication 800-63, Recommendations for Electronic Authentication; Special Publication 800-53, Recommended Security Controls for Federal Information Systems; and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Users shall:
 - (1) Understand their responsibilities for safeguarding User IDs and passwords
 - (2) Immediately notify a supervisor or the Information Custodian (e.g., the OIT department) if they suspect that a password or other system credential has been compromised.
 - (3) Comply with Corporation exit procedures.
- (b) Supervisors shall:
 - (1) Ensure that their staff understand and comply with the requirements contained in this policy
 - (2) Promptly notify Information Custodians of accounts that should be deactivated
 - (3) Report any suspected violations or compromises of credentials to the CISO and the Information Owner.
- (c) Information Custodians shall:
 - (1) Implement appropriate identification and authentication methods for the information resources in their care
 - (2) Instruct users on use of identification and authentication methods
 - (3) Document procedures for managing identification and authentication methods
 - (4) Report any compromises of these resources to the CISO and the Information Owner.
- (d) Information Owners shall:

- (1) Ensure that appropriate identification and authentication methods are implemented for the resources that they own, based on the classification and level of risk assigned to the resource.
- (e) System Developers must ensure that their systems support the procedures and guidelines specified in this policy document.

6. DEFINITIONS:

- (a) Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- (b) Brute Force Attack - attack where the attacker attempts to systematically “guess” a password or other secret by trying all possible values.
- (c) Identification – The process of determining who a user claims to be; usually performed by presenting a user ID (*i.e.*, “jsmith”).
- (d) Information Resources – The equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.
- (e) Password – Any secret string of characters which serves as authentication of a person’s identity, and which may be used to grant or deny access.
- (f) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.
- (g) User ID - Character string that uniquely identifies a computer user or computer process.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.

- (c) NIST Special Publication 800-63, Recommendations for Electronic Authentication.
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PASSWORD MANAGEMENT**ISP-C-03-0905**

1. **SUBJECT:** CNCS will protect access to its information resources by ensuring that any passwords used for authentication are properly assigned and protected.

2. **SCOPE:** This policy applies to all CNCS owned or operated information systems

3. **DESCRIPTION:** In order for passwords to be an effective tool for providing security, they must be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

4. **REQUIREMENTS:**
 - (a) In systems that use passwords as their authentication method, every account (including newly issued accounts) will have a password.
 - (b) Passwords must be changed:
 - (1) Immediately upon initial user logon.
 - (2) At least every 90 days.
 - Individual systems may set a shorter expiration period for their users.
 - Systems will have an automated mechanism to ensure that passwords expire.
 - Accounts for external users (members, grantees, volunteers) who have access only to their own information or that of their organizations, and who do not have access to any other sensitive CNCS information, are exempt from this requirement.
 - (3) If it is suspected that the password has been compromised.
 - (4) For administrator accounts, immediately upon the departure of personnel with access to those accounts.
 - (c) The following guidelines apply to password storage and visibility:
 - (1) Passwords will not be visible on a screen, hardcopy or other output device.
 - (2) Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.

- (3) Passwords will not be sent via unsecured (i.e., unencrypted and unauthenticated) email.
 - (4) Passwords will not be stored in written form (e.g. sticky notes).
- (d) Passwords are never to be lent or divulged to other persons, including individuals purporting to be system administrators.
- (e) A poorly chosen password could compromise the entire CNCS computer network. The object when choosing a password is to make it as difficult as possible for someone to guess what you have chosen. The following guidelines should be used to select strong, effective passwords:
- (1) Users with multiple accounts on the same CNCS system (e.g. an administrative account and a regular user account) must use completely different passwords for each account. Generic passwords will not be used.
 - (2) Users are not to use the same password at CNCS that they use for any non-CNCS computer accounts (e.g. an account on an Internet website).
 - (3) Passwords must be at least 8 characters and contain a combination of letters, numbers, and special characters.
 - (4) Passwords cannot be reused for at least 24 changes.
 - (5) Never assign a login account a password that is the same string as the User ID or that contains the User ID (e.g., “bob123” is not an appropriate password for user “bob”).
 - (6) Never set any password equal to the null string (i.e., a blank password), which is equivalent to no password at all.
 - (7) Passwords should not be a dictionary word in *any* language.
 - (8) Passwords should not contain any proper noun or the name of any person, pet, child, or fictional character.
 - (9) Passwords shall not contain any employee serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.
 - (10) Passwords should not contain any simple pattern of letters or numbers, such as “xyz123.”
 - (11) Passwords should not share more than 3 sequential characters in common with a previous password (i.e., do not simply increment the number on the same password, such as fido1, fido2, etc.).
 - (12) Use a password that is easy to remember (e.g., a phrase, line from a song, or nonsense words) and that you can type quickly.
- (f) The assignment of passwords for specific CNCS systems should adhere to the following:

- (1) Each system should have its own password selection standard that adheres to the above guidelines while being commensurate with the level of security required by the level of sensitivity of the system.
- (2) The system will be configured to enforce the password selection criteria specified in the system criteria.
- (g) Users will avoid using the “remember password” feature on web sites and other applications.
- (h) If SNMP is used, the community strings should follow the same selection guidance provided for passwords.
- (i) CNCS will adhere to NIST guidance as set forth in Special Publication 800-63, Recommendations for Electronic Authentication, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners shall ensure that the resources they own comply with the guidelines set forth in this policy.
- (b) Information Custodians shall:
 - (1) Assist Information Owners with implementing measures to enforce policy selection and management on their systems.
 - (2) Instruct users regarding system password policy.
 - (3) Report any password compromises of CNCS information resources to the CISO and the Information Owner.
- (c) Employees shall understand their responsibilities for selecting and safeguarding their passwords, and immediately notify a supervisor or the Information Custodian if they suspect that a password has been compromised.
- (d) The Chief Information Security Officer (CISO) shall:
 - (1) Provide advice to Information Owners and Custodians regarding system-specific password policies.
 - (2) Audit systems to ensure compliance with this policy.
- (e) System Developers must ensure that their systems support the procedures and guidelines specified in this policy document.

6. DEFINITIONS:

- (a) Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- (b) Identification - The process of determining who a user claims to be; usually performed by presenting a user ID (*i.e.*, “jsmith”).

- (c) Password – Any secret string of characters which serves as authentication of a person’s identity, and which may be used to grant or deny access.
- (d) User ID - Character string that uniquely identifies a computer user or computer process.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.
- (c) Homeland Security Presidential Directive / HSPD-7, December 17, 2003.
- (d) NIST Special Publication 800-63, Recommendations for Electronic Authentication.
- (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (f) NIST Special Publication 800-118, Guide to Enterprise Password Management

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

ACCESS TOKENS

ISP-C-04-0905

1. **SUBJECT:** CNCS will protect access to its information resources by ensuring that any tokens used for authentication are properly assigned and protected.
2. **SCOPE:** This policy applies to all CNCS owned or operated information systems that utilize access tokens.
3. **DESCRIPTION:** In order for tokens to be an effective tool for providing authentication, they must be properly managed.
4. **REQUIREMENTS:**
 - (a) Tokens will be used only in conjunction with another authentication factor, such as a password or PIN.
 - (b) CNCS will have procedures for distributing, tracking, and reclaiming access tokens:
 - (1) Tokens will only be given to personnel upon verification of their identity to ensure that tokens are not given to unauthorized persons.
 - (2) CNCS will maintain an inventory of tokens and their assignments.
 - (3) Upon exiting the Corporation, users will return their tokens to CNCS.
 - (4) If tokens are lost, stolen, or not returned upon staff termination, they will be immediately disabled.
 - (c) If a token is lost or stolen, an incident report will be completed by the assigned user.
 - (d) CNCS systems will require that the token PIN be changed upon first use and on a periodic basis.
 - (e) An audit trail of token usage will be enabled and reviewed in accordance with CNCS audit trail policy.
 - (f) Tokens will be issued only for exclusive use by a single individual. Users may not share their tokens or allow anyone else to use them or the access they provide.
5. **ROLES & RESPONSIBILITIES:**
 - (a) Information Owners will ensure that any access tokens used for systems they own are in compliance with this policy.

- (b) Information Custodians will assist Information Owners with complying with this policy, including administering and tracking tokens on their behalf.
- (c) The Chief Information Security Officer (CISO) will audit the use and management of tokens to ensure compliance with this policy.

6. DEFINITIONS:

- (a) Access – The right to enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of specific information resources.
- (b) Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- (c) Identification – The process of determining who a user claims to be; usually performed by presenting a user ID (*i.e.*, “jsmith”).
- (d) Password - Any secret string of characters which serves as authentication of a person’s identity, and which may be used to grant or deny access.
- (e) Token - Something that the user physically possesses which is used to authenticate the user’s identity. Examples include access cards, secureIDs, and dongles.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. **POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

9. **ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.
- (c) Homeland Security Presidential Directive / HSPD-7, December 17, 2003.
- (d) NIST Special Publication 800-63, Recommendations for Electronic Authentication.
- (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

(f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

AUDIT TRAILS & SYSTEM MONITORING

ISP-C-05-0905

1. **SUBJECT:** Audit trails will be created, protected, and retained to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
2. **SCOPE:** This policy applies to all CNCS information systems and all information users.
3. **DESCRIPTION:** In order to enforce information usage policies and security measures, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or “audit trail”) of system and application processes and user activity of systems and applications must be maintained. This is used to investigate security incidents, monitor use of CNCS resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
4. **REQUIREMENTS:**
 - (a) Audit Trails will be maintained for CNCS information systems:
 - (1) At minimum, the following transactions should be logged for each server (where possible given the constraints of the logging capabilities of the operating system and application software):
 - Server startup and shutdown
 - Manual loading and unloading of services
 - Installation and removal of software
 - User logon and logoff
 - System administration activities (e.g., configuration changes, account management, modifications of privileges and access controls, etc.)
 - (2) At minimum, the following transactions should be logged for each major application:
 - Modifications to the application

- User sign on and sign off
 - System administration activities (e.g., account management, modifications of privileges and access controls, etc.)
- (3) At minimum, the following transactions should be logged for each router, firewall, or other major network device (where possible given the constraints of the logging capabilities of the device):
- Device startup and shutdown
 - Administrator logon and logoff
 - Configuration changes
 - Account creation, modification, or deletion
 - Modifications of privileges and access controls
- (4) Type of event, date, time, and user identification are to be recorded for each logged transaction.
- (5) Sensitive information, such as passwords and actual system data, should not be stored in the logs.
- (b) Periodic reviews of audit logs will be conducted by designated personnel.
- (c) Only designated personnel should have access to the audit logs.
- (d) Auditing procedures will be developed for each system which include at least the following:
- (1) Auditable events for the system
 - (2) Audit trail level of detail
 - (3) Audit trail retention period
 - (4) Audit trail monitoring, analysis, and reporting process
 - (5) Audit event notification and escalation process (including personnel to notify and actions to be taken)
- (e) Audit trail files are to be kept for at least one (1) year.
- (1) Audit trails associated with known incidents (including those used for legal action) are to be kept for three (3) years.
- (f) Audit trails must be protected from unauthorized access, modification, and deletion.
- (g) CNCS will adhere to NIST guidance as set forth in Special Publication 800-92, Guide to Computer Security Log Management, and subsequent publications, as appropriate to CNCS systems based on level of risk.
- (h) Automated tools will be used to monitor and correlate system events and provide real-time alerts of system anomalies and potential security incidents.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that audit trails are implemented and maintained for their resources.
- (b) Information Custodians are responsible for assisting information owners with implementing and maintaining audit trails for the resources for which they are responsible, including developing operating procedures compliant with this policy.
- (c) Information Users are responsible for understanding and acknowledging that their use of CNCS systems may be logged and audited.

6. DEFINITIONS:

- (a) Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
- (b) Log Files - Files that show the status of the system and are accessed via Event Viewer, which lists the severity and a brief description of the logged event.
- (c) Security Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

- (c) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (d) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (f) NIST Special Publication 800-92, Guide to Computer Security Log Management
- (g) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (h) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (i) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PERSONNEL SECURITY**ISP-C-06-0905**

1. **SUBJECT:** Access to CNCS information resources is to be limited to only those persons who have been appropriately screened and authorized. CNCS will ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensure that information resources are protected during and after personnel actions, employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
2. **SCOPE:** This policy applies to all information owners, users and custodians.
3. **DESCRIPTION:** The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. Users, designers, implementers, administrators, and managers are involved in many important issues in securing information. It is important to ensure that the personnel who have access to CNCS' information resources can be trusted, to institute controls over the access provided to those personnel, and to implement procedures that minimize the personnel-related risks to CNCS' resources.
4. **REQUIREMENTS:**
 - (a) Any access granted to CNCS information resources will be based on the principles of separation of duties and least privilege, and in compliance with CNCS access control policies and procedures.
 - (b) Information users must have appropriate clearance for the sensitivity level of the resources which they are given access.
 - (1) Prior to being granted access to sensitive information resources, information users with no previous investigation and/or no recent, documented positive suitability determination must initiate and undergo an appropriate background investigation.
 - This does not include external users such as members, volunteers, and grantees accessing only information about themselves or their organizations.
 - (2) Contract language will be added to CNCS contracts to require background screening of all contractors who will have access to CNCS information or systems.

- (c) CNCS will assign a risk designation to all positions and establish screening criteria for individuals filling those positions. These will be reviewed and updated on a periodic basis.
- (d) Employees must be trained on the information security responsibilities and duties associated with their jobs.
- (e) Upon termination of individual employment at CNCS, CNCS will terminate system access, retrieve all IT property, and provide appropriate personnel access to official records maintained by the individual that are stored on the Corporation's systems.
- (f) Upon transfer of personnel or modification of duties, the individual's access permissions will be reviewed and updated.
- (g) CNCS will employ appropriate sanctions for personnel failing to comply with the Corporation's information security policies and procedures.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for the following for the resources they own:
 - (1) Determining who should have access their resources.
 - (2) Determining the level of screening required for access.
 - (3) Ensuring that personnel security policies and procedures are being followed.
- (b) Information Custodians
 - (1) Follow CNCS procedures for adding and removing access for personnel to the resources they manage, including promptly deleting or disabling accounts when users terminate employment.
 - (2) Implementing least privilege and separation of duties for resources they manage.
 - (3) Verifying that employees have appropriate clearance for the resources to which they are being granted access, in accordance with clearance requirements set by information owners.
- (c) Supervisors shall:
 - (1) Adhere to CNCS policies and procedures for adding and removing access for their employees.
 - (2) Ensure their staff undergo the appropriate level of background screening
- (d) Information Users shall:
 - (1) Promptly and accurately complete any background screening paperwork or non-disclosure agreements they are requested to complete.
 - (2) Follow CNCS procedures for obtaining access to information resources.

- (3) Promptly notify the information owner, information custodian, or their own supervisor when they no longer need access to a resource.
- (e) The Office of Procurement Services is responsible for:
 - (1) Working with CNCS personnel to ensure that appropriate personnel security clauses are included in contracts.
- (f) The Office of Human Capital is responsible for:
 - (1) Designating the risk level and the sensitivity level for CNCS positions.
 - (2) Coordinating background investigations
 - (3) Reviewing investigation/clearance documentation provided by contractors for compliance with CNCS requirements.
 - (4) Documenting personnel security procedures.

6. DEFINITIONS:

- (a) Access Privilege – An authorized ability to perform a certain action on a computer, such as read a specific computer file.
- (b) Account – A set of privileges for authorization to system access, which are associated with a user ID.
- (c) Authentication Token – A hardware device, the possession of which can be verified, and which helps to confirm identity as part of the authentication process (e.g., smartcard, SecureID)
- (d) Least Privilege – A concept that means granting users only the minimum level of access they need to perform their official duties.
- (e) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
- (f) Separation of Duties – Refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process or bypass security controls. Where feasible, the responsibilities of programmers, system administrators, database administrators, and system auditors should not overlap.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) Homeland Security Presidential Directive / HSPD-12, August 2004
- (c) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PHYSICAL AND ENVIRONMENTAL SECURITY**ISP-C-07-0905**

1. **SUBJECT:** CNCS will limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; protect the physical plant and support infrastructure for information systems; provide supporting utilities for information systems; protect information systems against environmental hazards; and provide appropriate environmental controls in facilities containing information systems.
2. **SCOPE:** This policy prescribes the procedures, guidelines, and standards that govern the implementation of physical security measures designed to protect CNCS information resources. It does not govern protection of personnel, facilities, and property not directly associated with information technology.
3. **DESCRIPTION:** Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Administrative, physical, and technical safeguards must be applied; and can include the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards.
4. **REQUIREMENTS:**
 - (a) Computer systems, facilities, and media storage areas shall be protected from theft, alteration, damage by fire, dust, water, temperature, humidity, power loss, and unauthorized disruption of operations.
 - (b) Physical access to information resources is to be controlled commensurate with the sensitivity of the resource and the level of risk.
 - (c) CNCS will authorize and control access to the facilities by visitors and will maintain visitor access records.
 - (d) Delivery and removal of information systems equipment will be controlled and appropriate records will be maintained.
 - (e) Areas containing sensitive information resources require special restrictions to limit access to these resources:
 - (1) Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.
 - (2) Personnel assigned to the area must escort personnel without an appropriate background clearance.

- (3) When uncleared personnel are present in these areas, sensitive information must be protected from observation, disclosure, or removal. This includes storing away documents and preventing unauthorized persons from viewing sensitive information on computer monitors.”
- (4) Each person within a sensitive area, regardless of position, shall be subject to challenge by another CNCS employee, facility security personnel, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.
- (5) Areas containing sensitive information must be physically secured.
- (f) Areas containing critical information resources require special protections to safeguard the availability of these resources:
 - (1) Protection must be implemented against fire, flood, humidity, electromagnetic disturbance, and other environmental factors that could damage the resources.
 - (2) Automated systems should monitor for environmental problems and alert specified personnel as appropriate.
- (g) Specific requirements for Data Centers:
 - (1) Comply with all requirements listed above.
 - (2) Provide emergency power shutdown controls. Cover controls to prevent accidental activation.
 - (3) Provide an uninterruptible power supply.
 - (4) Annual testing will be performed on all fire, utility, and environmental alarms and protective systems.
 - (5) A list of people authorized to access the Data Center will be reviewed at least quarterly.
 - (6) The Deputy Chief Information Officer or the Chief Information Security Officer must approve requests to access the computer room.
 - (7) Visitors are to be escorted at all times.
 - (8) All access to the room must be logged.
- (h) Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. It is important to keep backups in a separate location from the originals.
- (i) Other areas where physical access should be restricted are wiring closets and computer storage areas.

5. ROLES & RESPONSIBILITIES:

- (a) Information Users are responsible for:

- (1) Physically protecting the CNCS information resources entrusted into their possession.
 - (2) Reporting any incident or condition contrary to the specified requirements.
- (b) Supervisors are responsible for monitoring their employees' compliance with this policy.
 - (c) Information Owners are responsible for implementing measures to protect their resources against physical and environmental threats, as well as unauthorized physical access.
 - (d) Information Custodians are responsible for assisting information owners with implementing physical and environmental security measures.
 - (c) The Chief Information Security Officer (CISO) is responsible for performing auditing to ensure compliance with these policies and guidelines.
 - (d) The CNCS Facility Security Officer is responsible for ensuring the physical and environmental security of the CNCS facilities.
 - (e) Administrative Services is responsible for:
 - (1) Assisting with implementation and management of facility-related controls such as power systems, fire control, HVAC, etc.
 - (2) Coordination with building management.

6. DEFINITIONS:

- (a) Physical Security - The measures used to provide physical protection of resources against deliberate and accidental threats.
- (b) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

7. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000
- (c) Homeland Security Presidential Directive / HSPD-12, August 2004
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

10. EFFECTIVE DATE: June 1, 2009

11. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

12. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

BACKUP AND RECOVERY**ISP-C-08-0905**

1. **SUBJECT:** Backups of critical information resources must be performed, tested, and appropriately managed.
2. **SCOPE:** This policy applies to all CNCS information resources.
3. **DESCRIPTION:** There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include, but are not limited to, hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. These threats are very common and it is inevitable that some of these events will occasionally occur at CNCS.

It is therefore essential that CNCS maintain backup copies of all critical information and systems so that they can be used to provide the continued availability and viability of these resources when these events occur.

4. REQUIREMENTS:

- (a) All critical CNCS information resources will be backed up in a recoverable fashion.
- (b) Critical information should be backed up daily and these backups stored off-site in a secure, environmentally-controlled location. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.
- (c) System configurations, applications, and licenses, should be backed up whenever changes are made to them and on at least a monthly basis. These should also be stored offsite.
- (d) The backing up of non-critical information is at the discretion of the data owner and system administrator.
- (e) Each system will have a defined backup retention schedule which complies with CNCS' data retention policies.
- (f) CNCS will test the back up and restore procedures at least annually to ensure that data can be effectively restored from the backups.
- (g) CNCS will develop and implement detailed procedures for performing back ups restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.

- (h) Backups will be treated with the same level of criticality and sensitivity as the data and applications stored on them.
- (i) Persons who have access to the backups, or who have access to perform back up or restore functions, must undergo appropriate background screening in accordance with CNCS Personnel Security policy prior to being given such access.
- (j) Backup media (e.g., tapes) must be handled in accordance with CNCS Media Management policy.
- (k) System custodians will back up data stored on their servers. However, information users are responsible for backing up any data stored on workstations and portable storage media (i.e., diskettes, flash drives, CDs, etc).
 - (1) Users may copy their data to servers to be backed up or may perform their own back ups of data not stored on CNCS servers.
 - (2) Backups made by users must be handled in accordance with CNCS Media Management policy.
- (l) CNCS will follow NIST guidance regarding backups.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners will ensure that their resources are backed up in accordance with this policy.
- (b) Information Custodians will assist Information Owners with backing up and restoring their resources.
- (c) The Chief Information Security Officer (CISO) will perform auditing to ensure compliance with this policy.
- (d) Information Users will ensure that any critical information residing on their workstations or portable media are backed up in accordance with this policy.

6. DEFINITIONS:

- (a) Back Up – the action of copying (or mirroring) important data to a second location or onto removable media
- (b) Backup – A copy of data that is made in order to provide redundancy in case the original becomes corrupted or unavailable.
- (c) Restore – The process of copying data from a previously-made backup to the original (or an alternate) system.
- (d) Critical Information – Any information essential to CNCS' activities, the destruction, modification, or unavailability of which would cause serious disruption to the agency's mission.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- (g) NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PATCH MANAGEMENT AND SYSTEM MAINTENANCE

ISP-C-09-0905

1. **SUBJECT:** CNCS will perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. Patches will be deployed to proactively prevent the exploitation of vulnerabilities in CNCS systems.
2. **SCOPE:** This policy covers all servers, workstations, operating systems (OS), network devices, applications, and other information resources for which vendors provide system patches or security updates.
3. **DESCRIPTION:** Maintained patch levels are critical to the security of CNCS systems. Vendors will typically provide OS patches and fixes for security problems, which can be loaded separately from the application. These should be loaded on a timely basis using a controlled process.
4. **REQUIREMENTS:**
 - a) A system maintenance program that includes detailed procedures and standards will be developed and implemented for each CNCS information system.
 - b) CNCS will perform periodic preventative and regular maintenance of systems and components in accordance with vendor recommendations.
 - c) Sources should be monitored for available patches on a continuous basis.
 - a. During regular operation, available patches will be reviewed at least monthly and applied if appropriate.
 - b. In an emergency situation, more urgent application of new security patches may be required.
 - d) Patches will be checked for compatibility with all system components
 - a. Patches will be successfully tested on non-production systems prior to being loaded on production systems.
 - b. The use of standardized configuration baselines will simplify testing and reduce the risk of patching-induced problems.
 - c. The risk and impact of deploying each patch should be assessed prior to implementation of that patch.
 - d. If a decision is made not to deploy a patch (e.g., due to risk or compatibility issues), that decision and the reason for the decision must be documented.

- e) Systems will be backed up prior to system maintenance or installation of new patches.
- f) All system maintenance and patching will be performed in accordance with CNCS Change Control policy and procedures.
- g) In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the correct patch levels before data is reloaded.
- h) New systems must be fully patched before being placed into the production IT environment.
- i) The use of automated tools to expedite the distribution of patches is encouraged. However, measures must be taken to reduce the risk of these tools being used by an attacker to distribute malicious code.
- j) The use of maintenance tools and remote maintenance procedures is to be approved, controlled, and monitored.
- k) Only authorized personnel may perform system maintenance.
 - a. If an outside vendor must perform maintenance, they are to be monitored by authorized personnel.
- l) CNCS will adhere to NIST guidance as set forth in NIST Special Publication 800-40, Creating a Patch & Vulnerability Management Program, and subsequent publications.
- m) See also ISP-P-06, Vulnerability Remediation

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that their information resources are maintained in compliance with CNCS patch management policies and procedures.
- (b) Information Custodians are responsible for:
 - (1) assisting information owners with the development and implementation of patch management policies and procedures for their information resources.
 - (2) implementing patches in accordance with the policies and procedures
- (c) The Chief Information Security Officer (CISO) is responsible for auditing information systems to ensure that they comply with CNCS patch management policies and procedures.

6. DEFINITIONS:

- (a) Network Device – Any physical component which forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

- (b) Network Infrastructure – Network infrastructure includes servers, network devices, and any other back-office equipment.
- (c) Patch – An additional piece of code developed to address a problem in an existing piece of software.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-40, Creating A Patch & Vulnerability Management Program
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (e) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (f) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. **REVIEW SCHEDULE:** This policy will be reviewed and updated annually.

ASSET MANAGEMENT**ISP-C-10-0905**

1. **SUBJECT:** All information assets must be tracked and managed to ensure that they are not lost or misused.
2. **SCOPE:** This policy applies to all CNCS information assets, including but not limited to workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.
3. **DESCRIPTION:** Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the wrath of auditing organizations like GAO and OMB.

Not only would loss of information assets result in a financial impact on CNCS, but it could also result in unauthorized access to data stored on or accessed through these assets, and could have a detrimental effect on the reputation of the agency. Additionally, the tracking and management of information assets is mandated by several federal regulations, such as the Clinger-Cohen Act.

4. REQUIREMENTS:

- (a) CNCS must keep a record of all information assets, including those mentioned in the scope above.
 - (1) Information assets are to be added to the record upon receipt by CNCS and assigned a barcode.
 - (2) For each information asset, CNCS will track at least the following information:
 - The brand, model, and type of asset
 - Serial number and CNCS asset tag number
 - The person to whom the asset is assigned
 - The location of the asset
 - Any maintenance agreements for the asset
 - (3) Upon disposal of an information asset, CNCS will track:
 - date of disposal
 - method of disposal (e.g., transfer, destruction, donation, etc.)

- name of the new owner (if there is one)
- (b) Periodic inventories are to be performed to verify records and account for all information assets.
- (1) Each asset is to be inventoried at least annually.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for:
- (1) Inventorying, tracking, and protecting the CNCS information resources that they own.
- (2) Overseeing development of asset management procedures for their system.
- (b) Information Custodians are responsible for assisting information owners with inventorying, tracking, and protecting CNCS information resources in their care, including documenting asset management procedures.
- (c) Information Users are responsible for exercising due diligence in protecting information resources entrusted to them, and immediately reporting the loss, theft or damage of any CNCS information resource.

6. DEFINITIONS:

- (a) Information Asset – An information resource that has tangible value.
- (b) Information Resource - The equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

(c) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

(d) Federal Managers Financial Integrity Act of 1982 PL 97-255 (H.R. 1526).

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

(a) Original Publication June 2007

(b) Reviewed and updated July 2008

(c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

MEDIA MANAGEMENT**ISP-C-11-0905**

1. **SUBJECT:** Media must be handled, stored, and disposed of properly in order to protect the sensitive data stored upon it. CNCS will protect information media resources, limit access to information on media to authorized users, and sanitize or destroy media before disposal or release for reuse.
2. **SCOPE:** This policy applies to all removable media (such as CDs, tapes, flash drives, etc.) that is used to store CNCS data. It only applies to hard drives when they are not installed inside a computer.
3. **DESCRIPTION:** CNCS has been entrusted with a variety of sensitive data in order to accomplish its mission. This data, which is stored on a variety of media, must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, CNCS will use a variety of security mechanisms that provide protections for media.
4. **REQUIREMENTS:**
 - (a) Media Handling:
 - (1) Users are to take all reasonable steps to protect CNCS storage media in their possession.
 - (2) Appropriate physical and environmental protection controls shall be provided for stored media containing critical data.
 - (3) Handling media that contain sensitive data:
 - Any media containing sensitive data should be marked with sensitivity level. Labeling shall include any special handling instructions
 - Any media containing sensitive data must be secured (such as kept in a locked drawer, cabinet, or safe) when not in use or unattended.
 - The receipt and delivery of media containing sensitive data must be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.
 - Sensitive information shall be secured out of sight when visitors are present.
 - (b) Media Disposal:

- (1) Information Users need to understand that simply deleting data from media does not completely or permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly.
 - (2) Media that contain sensitive data must be sanitized when they no longer need to store sensitive data.
 - (3) Before any CNCS-owned or managed computing equipment is transferred, donated, or otherwise disposed of, storage media associated with the equipment must be sanitized via approved government methods.
 - (4) The method used to sanitize a particular piece of media will correspond to the FIPS 199 level of confidentiality of the information stored on the media.
- (c) The loss of any media containing CNCS information must be reported to the CISO immediately.
- (d) CNCS will adhere to NIST guidance as set forth in Special Publications 800-88, Guidelines for Media Sanitization, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any media they own, and media that contains data or applications that they own, are handled and disposed of in accordance with CNCS policies.
- (b) Information Custodians are responsible for:
- (1) Assisting information owners with the proper handling of their media in accordance with CNCS policies and procedures.
 - (2) Developing documented procedures for media management and disposal.
 - (3) Complying with CNCS policies and procedures for any media entrusted to them.
 - (4) Reporting the loss, damage, or theft of any media entrusted to them that contains CNCS data.
- (c) Information Users are responsible for:
- (1) Protecting CNCS media in their possession
 - (2) Storing CNCS data only on approved media.
 - (3) Backing up data that is stored on media in their physical possession.
 - (4) Reporting the loss, damage, or theft of any media containing CNCS data.
- (d) Supervisors are responsible for ensuring that their employees understand how to properly handle and dispose of media in accordance with CNCS policies and procedures.

6. DEFINITIONS:

- (a) Media – Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
- (b) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
- (c) Sanitization - Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
- (d) Wipe - Deliberately overwriting a piece of media and removing any trace of files or file fragments.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (e) NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- (f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (g) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

- (h) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (i) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (j) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- (k) NIST Special Publication 800-88, Guidelines for Media Sanitization

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SYSTEMS DEVELOPMENT LIFECYCLE (SDLC) SECURITY

ISP-C-12-0905

1. SUBJECT: Security must be integrated into all phases of the System Development Life Cycle (SDLC). CNCS will employ system development life cycle processes that incorporate information security considerations; employ software usage and installation restrictions; allocate sufficient resources to adequately protect organizational information systems; and ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

2. SCOPE: This policy covers all systems at CNCS, whether they are purchased (e.g., COTS, outsourced) or developed internally.

3. DESCRIPTION: Each information system passes through multiple phases during its lifetime (SDLC), as it is planned, developed, deployed, operated, and retired. Specific security-related activities must occur in each phase to assure that the system is secure.

It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later. By considering security early in the information SDLC, CNCS will be able to avoid higher costs later on while also developing a more secure system from the start.

4. REQUIREMENTS:

(a) Security must be considered in all phases of the SDLC and treated as an integral part of any system development or implementation project, including system modifications. In each phase of the SDLC there are specific information security requirements that need to be met.

(b) The following items will be incorporated into CNCS' system development lifecycle process:

(1) Prior to approving the development/acquisition of a system, CNCS will evaluate the risks of the project:

- CNCS will conduct sensitivity assessment (information, potential damage, laws and regulations, threats, environmental concerns, privacy, security characteristics, CNCS policy and guidance). The assessment shall consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (e.g., hazardous location) and public threats to the system or information should also be considered.

- CNCS will perform a preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.
- (2) The acquisition of any system will comply with ISP-C-17 System Acquisition.
 - (3) Security requirements shall be developed at the same time system planners define the other requirements of the system. The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.
 - (4) Application software used at CNCS must be obtained through authorized procurement channels and must comply with all licensing requirements.
 - (5) Each application must be categorized in accordance with CNCS' Security Categorization policy, and provided protection appropriate to its level of sensitivity and criticality.
 - (6) Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.
 - (7) Prior to placing the system into production, the following tasks will be performed:
 - The system will be thoroughly documented.
 - (i) Documentation of sensitive systems must be provided the same degree of protection as that provided for the system.
 - A System Security Plan (SSP) will be developed in accordance with CNCS System Security Plan policy and procedures.
 - Operational practices will be developed, including standard operational procedures and system-specific security policies (e.g., account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.
 - All systems will be thoroughly tested prior to being placed in the CNCS production operating environment.
 - (i) Sensitive data will not be used to test systems until system security has been reasonably assured by testing with non-sensitive data or files.
 - The system's security features will be configured and enabled, and security management procedures will be implemented.
 - The system will be authorized for processing via CNCS' Certification and Accreditation (C&A) process.
 - (8) During ongoing operation and maintenance of the system, CNCS will ensure the following tasks are completed:

- The security activities outlined in the system security plan (e.g., performing backups, holding training classes, managing accounts) will be performed.
 - Any changes made, or maintenance performed, on the system are to comply with CNCS' Change Control and Patch Management policies and processes.
 - Periodic security audits and vulnerability tests will be performed in accordance with CNCS Audit and Vulnerability Testing policies.
 - The SSP will be reviewed and updated in accordance with the System Security Plan policy.
 - The system will be periodically re-Certified and Accredited in accordance with NIST guidance.
 - Systems must comply with all CNCS information security policies and procedures (e.g., change control, patch management, access control, backup and recovery, etc.)
- (9) When disposing of a system, CNCS will ensure that proper measures are taken to protect the data that was stored in the system:
- Information may be moved to another system, archived, discarded or destroyed in accordance with CNCS data retention policies.
 - Any storage media must be disposed of in accordance with CNCS' Media Management policies.
 - The disposition of software needs to comply with its license and other agreements
- (c) CNCS will adhere to NIST guidance as set forth in Special Publications 800-64, Security Considerations in the Information System Development Life Cycle, 800-12, An Introduction to Computer Security: The NIST Handbook, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for:
- (1) Understanding the security requirements for each system life cycle phase.
 - (2) Implementing the life cycle security requirements for their systems.
 - (3) Ensuring that security plans for information systems include a strategy for security risk management. Significant risks should be identified, along with responsibilities and mitigation strategies to reduce the security risks.
 - (4) Documenting the security controls in the System Security Plan.

- (5) Ensuring that security controls are incorporated in the design, development, and testing of contractor-developed software.
 - (6) Accrediting systems in accordance with CNCS C&A policy.
 - (7) Ensuring that security requirements and planning are included in life cycle budgets for information systems and included in project screening forms and business cases that are completed in accordance with the CPIC.
 - (8) Designating someone on their team to act as the system ISSO for each major system they own. This person will be the security liaison for the system.
 - (9) Obtaining a Memorandum of Understanding/Memorandum of Agreement for Interfacing systems and keeping this information readily available.
 - (10) Developing a contingency plan for each system they own in accordance with CNCS contingency planning policies
- (b) Information Custodians are responsible for:
- (1) Assisting Information Owners with the development and implementation of security controls.
 - (2) Ensuring that system security controls are implemented properly and operating as intended.
 - (3) Maintaining the system in accordance with all standard operating procedures and other approved security management processes.
 - (4) Assisting the CISO with testing and auditing of the system.
 - (5) Maintaining a testing and development environment for performing their SDLC activities.
- (c) The Chief Information Security Officer (CISO) is responsible for:
- (1) Providing security guidance to system owners and system developers throughout the system lifecycle.
 - (2) Auditing to ensure that all systems are in compliance with this policy.
 - (3) Performing Certification of systems in accordance with CNCS C&A policy.

6. DEFINITIONS:

- (a) Media – Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes.
- (b) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

- (c) System Development Life Cycle – The system development life cycle (SDLC) starts with the initiation of the system planning process, and continues through system acquisition/development, implementation, operations and maintenance, and ends with disposition of the system.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources."
- (c) Office of Management and Budget Memorandum M-00-07, "Incorporating and Funding Security in Information Systems Investments," February 28, 2000.
- (d) Computer Security Act of 1987, P.L. 100-235 (1988).
- (e) Federal Information Processing Standards (FIPS) Publication 73, Guidelines for Security of Computer Applications, June 1980.
- (f) NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle
- (g) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (h) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (i) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems
- (j) NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook
- (k) NIST Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

CHANGE CONTROL

ISP-C-13-0905

1. **SUBJECT:** Authorized changes must occur to CNCS' network and information systems, and these changes must occur in a timely manner without disruption or compromise to existing system operation. However, CNCS must protect its information systems from unauthorized changes, intrusions or misuse. One way of facilitating this requirement is to formally manage and control hardware and software configuration changes.
2. **SCOPE:** This policy applies to all CNCS information systems.
3. **DESCRIPTION:** Change control involves controlling and managing changes to information systems to ensure integrity and availability. Change control prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other related problems.

Informal operational processes with no means of controlling changes to information systems impede CNCS' ability to determine the status of its current architecture and configuration, respond to security issues, and even to propose changes. Change control planning addresses this deficiency and establishes a consistent, cross-organizational change management process for CNCS information systems. Change control history lays the framework of how CNCS' network is built and is a valuable tool for both emergency response and information architecture planning.

4. **REQUIREMENTS:**

- (a) Changes to each CNCS information system will be systematically planned, approved, tested and documented at a level appropriate with the size, complexity, and sensitivity of the system.
 - (1) Changes will be reviewed and approved by the Change Control Board (CCB), Investment Review Board (IRB) and/or Technical Review Board (TRB) as specified in the CNCS Configuration Management Procedures.
- (b) Change control procedures will be documented for all systems to provide a complete audit trail of decisions and design modifications.
- (c) CNCS will establish and maintain baseline configurations and inventories of its information systems throughout their life cycles and establish and enforce security configuration settings for information technology products employed in organizational information systems.
- (d) For each information system, CNCS will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the

change, the purpose of the change, and any observations made during the course of the change.

- (e) Documentation will adhere to the Document Management Process (DMP) and be stored in the configuration management repository (i.e Subversion)
- (f) Procedures will be implemented to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:
 - (1) Establish who performs maintenance and repair activities.
 - (2) Contain procedures for performance of emergency repair and maintenance.
- (g) Version control that associates system components to the appropriate system version will be followed.
- (h) Impact analyses will be conducted to determine the effect of proposed changes on existing systems and security controls.
- (i) Procedures will be implemented for testing and/or approving system components (operating system, other system, utility, applications) and configuration changes prior to promotion to production.
- (j) Information Users will be notified regarding how they will be impacted by changes.
- (k) Current backups will be available when changes are made.
- (l) All software, operating systems, and patches shall be installed in accordance with U.S. copyright regulations, the license for that software, and applicable CNCS Information Security policies.
- (m) Only authorized personnel may make changes to CNCS information systems.
- (n) CNCS will monitor the configurations and security controls of its systems on an ongoing basis.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that changes to the systems they own are documented and implemented in compliance with the policies and procedures listed in this document.
- (b) Information Custodians are responsible for:
 - (1) Documenting system configurations
 - (2) Participating in the development of procedures for change control.
 - (3) Following change control procedures
 - (4) Evaluating, recommending, and coordinating the implementation of solutions/changes consistent with CNCS technical plans.
 - (5) Maintaining change log documentation

- (c) The Chief Information Officer (CIO) is responsible for defining change management processes for the Corporation's IT environment.
- (d) The Chief Information Security Officer (CISO) is responsible for auditing to ensure that change control policies are followed.
- (e) The Configuration Manager (CM) is responsible for:
 - (1) Developing, documenting and updating configuration management procedures.
 - (2) Auditing to ensure that change control procedures are followed.

6. DEFINITIONS:

- (a) Change Control - Documented procedures used to control the revision of applications, operating systems, and hardware configurations in computing environments.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (d) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (g) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

(h) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

EMERGING THREAT DEFENSE**ISP-C-14-0905**

1. **SUBJECT:** Tools and procedures must be implemented to minimize the impact of computer viruses, spyware, and other emerging threats on CNCS' information resources.
2. **SCOPE:** This policy applies to all CNCS servers and workstations, as well as computers used for remote access to the CNCS network.
3. **DESCRIPTION:** Security risks are constantly evolving. Not only are new viruses, spyware programs, and spam developed daily, but new kinds of threats are constantly emerging. In addition to electronic threats like viruses and spyware, social engineering and other attacks that bypass technical protections are also becoming an increasing issue.

These threats can result in loss of information, reduced system performance, disclosure of sensitive information, identity theft, unauthorized system changes, and a myriad of other risks.

It is critical that CNCS implement proactive measures to protect its information and systems from these emerging threats.

4. REQUIREMENTS:**(a) Viruses**

- (1) Every CNCS server and workstation must run the agency standard, supported antivirus software.
- (2) CNCS will use antivirus software at its email gateway to scan messages and attachments.
- (3) Antivirus software is to be updated automatically as new virus profiles are made available by the vendor.
- (4) Any infected files that cannot be repaired must be quarantined or deleted.
- (5) Any computer used for remote access to the CNCS network (such as a laptop used for telecommuting or a home computer used to do CNCS work) must have antivirus software loaded and updated on a regular basis.
- (6) All portable media (*e.g.* floppy diskettes, CDs) must be scanned for viruses before use on a CNCS computer.

(b) Spyware

- (1) The Corporation will deploy an anti-Spyware solution to protect agency computers against spyware.
 - (2) Anti-spyware software is to be updated automatically as new spyware profiles are made available by the vendor.
- (c) Spam
- (1) The Corporation will implement email filtering tools and procedures to minimize spam as specified in the Electronic Mail Security policy (ISP-S-10).
 - (d) Users may not unload or disable security software for any reason without specific instruction from OIT.
 - (e) Any infected or compromised computers that cannot be immediately cleaned must be removed from the network until they can be verified as malware free.
 - (f) Employees are to be trained on techniques for avoiding viruses, spam, spyware, phishing, and other emerging threats.
 - (g) CNCS will monitor anti-spam, anti-spyware, and anti-virus tools to detect and respond to incidents and trends.
 - (h) Incidents involving emerging threats will be reported and resolved in accordance with CNCS Incident Reporting (ISP-P-03) and Incident Response (ISP-P-04) policies.
 - (i) CNCS will perform periodic testing and remediation of vulnerabilities to emerging threats in accordance with the Corporation's Vulnerability Testing (ISP-P-05) and Vulnerability Remediation (ISP-P-06) policies.
 - (j) Vulnerabilities to emerging threats will be minimized through the timely implementation of system patches and security updates in accordance with the CNCS Patch Management policy (ISP-C-09).
 - (k) CNCS will adhere to NIST guidance on handling emerging threats, including Special Publication 800-83, Guide to Malware Incident Prevention and Handling.
 - (l) Usage restrictions and implementation guidance will be established for mobile code technologies based on the potential to cause harm to CNCS information systems.
 - (1) The Corporation will document, monitor, and implement controls for the use of mobile code within CNCS systems.
 - (2) Appropriate Corporation officials will authorize or deny the use of mobile code.
 - (3) The organization shall implement controls and procedures for mobile code in accordance with NIST SP 800-28.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for deploying malware protection software and procedures on any servers or workstations that they own.

- (b) Information Custodians are responsible for assisting information owners with the implementation of malware protection software and procedures.
- (c) Information Users are responsible for taking appropriate precautions to avoid introducing malware into the CNCS computing environment.
- (d) Supervisors are responsible for assisting their employees with understanding and complying with CNCS malware prevention procedures and guidelines.
- (e) The Chief Information Security Officer (CISO) is responsible for:
 - (1) Auditing the CNCS computer environment for adherence to this policy.
 - (2) Providing awareness training to users to help them avoid propagating malware.

6. DEFINITIONS:

- (a) Antivirus software – software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus may have caused.
- (b) Malware - A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. Examples of malware include spyware and viruses.
- (c) Mobile Code - Software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded within Office documents. Mobile code can also download and execute in the client workstation via email. Mobile code may download via an email attachment (e.g., macro in a Word file) or via an HTML email body (e.g., JavaScript).
- (d) Phishing - Tricking individuals into disclosing sensitive information through deceptive computer-based means.
- (e) Remote Access – Any access to CNCS' corporate network through a network, device, or medium that is not controlled by CNCS (such as the Internet, public phone line, wireless carrier, or other connectivity).
- (f) Spam - Unauthorized and unsolicited electronic mass mailings
- (g) Spyware - Software that is secretly installed on a users computer and that monitors use of the computer in some way without the users' knowledge or consent.
- (h) Virus – A program designed with malicious intent that has the ability to spread to multiple computers or programs.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (c) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers
- (d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (e) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- (f) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- (g) NIST Special Publication SP 800-53, Recommended Security Controls for Federal Information Systems
- (h) Special Publication 800-83, Guide to Malware Incident Prevention and Handling.
- (i) GAO-05-231, Emerging Cybersecurity Issues Threaten Federal Information Systems

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

ENCRYPTION**ISP-C-15-0905**

1. **SUBJECT:** CNCS will use proven, government-approved encryption technologies to protect sensitive information.
2. **SCOPE:** This policy applies to the use of encryption for protecting CNCS information during storage or transmission.
3. **DESCRIPTION:** The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and recognizes the legal authority for the dissemination and use of encryption technologies outside of the United States.
4. **REQUIREMENTS:**
 - (a) The use of encryption to protect sensitive information, both in storage and in transmission, is highly encouraged.
 - (b) Only government-approved encryption techniques and devices may be used.
 - (1) All encryption products must be Federal Information Processing Standard (FIPS) 140-2 or 197 certified.
 - (2) Digital certificates used or issued by CNCS will comply with the Federal Public Key Infrastructure.
 - (c) CNCS will obey all regulations regarding restrictions on export of encryption technologies.
 - (d) When encryption is used, CNCS will have documented and implemented procedures for managing the encryption keys, in order to ensure that these keys are protected from unauthorized disclosure, destruction, or misuse.
 - (1) Where feasible, automated mechanisms will be used to manage the keys.
 - (e) Any use of digital certificates to provide non-repudiation must be approved by the CISO, CIO, or Deputy CIO.
 - (f) CNCS will adhere to NIST guidance as set forth in Special Publications 800-21, Guide for Implementing Cryptography in the Federal Government; 800-57, Recommendation on Key Management; 800-38, Recommendations for Block Cipher Modes of Operation; 800-32, Introduction to Public Key Technology and Federal PKI Infrastructure; 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; 800-15, Minimum Interoperability Specification for PKI Components; and other publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that the use of encryption by, or protection of, systems that they own are compliant with the terms of this policy and all applicable federal standards.
- (b) Information Custodians are responsible for assisting information owners with implementing and managing encryption technologies compliant with this policy.
- (c) The CISO is responsible for providing guidance on the use of encryption technologies and auditing CNCS users and systems for compliance with this policy.

6. DEFINITIONS:

- (a) Digital Certificate - The electronic equivalent of an ID card. A digital certificate, which may contain a users name and other information, is issued by a certification authority (CA), which also keeps track of digital certificates that have been revoked.
- (b) Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.
- (c) Encryption Key - A secret password or bit string used to control the encryption process.
- (d) Non-repudiation - Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.
- (e) Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
- (f) Public Key Cryptography - A coding system in which encryption and decryption are done with public and private encryption keys, allowing users who don't know each other to send secure or verifiable messages.
- (g) Public Key Infrastructure (PKI) - A system for securely exchanging information that includes a method for publishing the public keys used in public key cryptography and for keeping track of keys that are no longer valid.
- (h) Sensitive Information – Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) Federal Information Processing Standard (FIPS) 140-2, Security requirements for Cryptographic Modules.
- (d) Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard.
- (e) NIST Special Publication 800-21, Guide for Implementing Cryptography in the Federal Government.
- (f) NIST Special Publication 800-57, Recommendation on Key Management.
- (g) NIST Special Publication Introduction to Public Key Technology and Federal PKI Infrastructure.
- (h) NIST Special Publication 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication.
- (i) NIST Special Publication 800-15, Minimum Interoperability Specification for PKI Components.
- (j) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- (k) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (l) NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PERIMETER PROTECTION

ISP-C-16-0905

1. **SUBJECT:** Adequate protection must be implemented to protect CNCS information resources from intruders and service disruptions.
2. **SCOPE:** This policy applies to all external entry points into CNCS information systems, including but not limited to Internet connection(s) and communication links to external systems.
3. **DESCRIPTION:** Any connectivity to systems or organizations outside of CNCS provides an opening for unauthorized personnel to access or tamper with CNCS information resources. Such threats range from intruders breaking into CNCS' network to steal or alter data to service disruptions propagated from other systems. CNCS must implement firewalls, intrusion detection systems, and other precautions to prevent, detect, and resolve incidents arising from these threats.
4. **REQUIREMENTS:**
 - (a) CNCS will use firewalls and other security devices to provide filtering and logging of traffic on all external communication links.
 - (1) CNCS will use a Firewall and an Intrusion Detection System (IDS) on all external connections.
 - (2) Traffic into the CNCS network from external systems must be filtered to allow only the minimum access required to meet CNCS business requirements.
 - (3) Firewalls and IDS systems should be configured and administered in accordance with government and industry best practices, including but not limited to:
 - The default filters must specify that all access into the CNCS network be denied unless specifically permitted.
 - Each firewall, IDS, and other perimeter security device must be actively monitored, and periodically audited, for threats to the CNCS network.
 - Firewall and IDS equipment should provide real-time notifications or alerts to administrators upon security events.
 - If the firewall has a failure resulting in its inability to filter traffic in accordance with CNCS rules, it will not allow any traffic to pass until reset by an administrator.

- (i) If the firewall experiences a failure causing a reboot, it will default to a “Deny All” configuration.
 - Firewall services should run on a dedicated system with all other services disabled.
 - Source routing will be disabled on all firewalls and external routers.
 - The firewall will not accept traffic on its external interfaces that appears to be coming from internal network addresses.
 - Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall software must be done by a firewall administrator(s) and requires the approval of the CISO.
 - Patches and updates will be implemented in a timely manner in alignment with CNCS patch management policy.
 - All services and traffic to be authorized across the firewall implementation must be well documented. Documentation will include the business need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements.
 - The firewall will be configured to hide information about the network so that internal host data is not advertised to the outside world.
- (b) Any CNCS systems or services that are to be publicly available on the Internet must adhere to the following rules:
 - (1) These systems must be placed in a protected DMZ.
 - (2) No sensitive data is to be stored on systems located in the DMZ. All sensitive data must be located inside the firewall.
 - (3) Access from the Internet to these systems must not make sensitive information or information systems vulnerable to compromise.
- (c) The details of CNCS’ internal network should not be attainable from outside the firewall.
- (d) Proxy Servers:
 - (1) All outbound connections to the Internet will be performed through a Proxy server. A proxy server provides a number of security enhancements by concentrating services through a specific host to allow monitoring, hiding of internal structure, etc.
 - (2) Because this funneling of services creates an attractive target for a potential intruder, additional measures should be deployed to protect the proxy server.
- (e) Any remote access into the CNCS network (e.g., telecommuting) must utilize two factor authentication and encryption, and adhere to CNCS remote access policies and procedures.

- (f) Any changes to existing equipment or deployment of new equipment on the perimeter must adhere to CNCS change control procedures.
- (g) Information regarding the configuration of firewall and other perimeter protections is considered confidential and is to be treated as Sensitive data.
- (h) All hardware and software deployed on the perimeter must adhere to CNCS system security policies and procedures, including the disabling of all unnecessary services.
- (i) All perimeter equipment must be documented in accordance with CNCS information system documentation procedures.
- (j) All security related events on perimeter equipment, as well as access to CNCSNET via this equipment, must be logged and audited in accordance with CNCS' Audit Trail policies and procedures.
- (k) The responsibility for the security of any equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. COTRs are responsible for third party compliance with this policy.
- (l) Network Trust Relationships:
 - (1) All connections between the CNCS network and external networks (such as those of other agencies) must be approved by the CIO.
 - (2) Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures.
 - (3) An Interconnection Security Agreement will be developed and signed by CNCS and the external system owner specifying security responsibilities and protections that will govern the connection between the networks.
 - (4) All connections to approved external networks will pass through CNCS approved firewalls.
 - (5) Information Owners will validate the need for all such connections on an annual basis.
- (m) CNCS will adhere to NIST guidance as set forth in Special Publications 800-41, Guidelines on Firewalls and Firewall Policy, 800-31, Intrusion Detection Systems NIST Special Publication 800-94, Guide to Intrusion Prevention and Detection Systems; and subsequent publications.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that the resources they own comply with the guidelines specified in this policy, including but not limited to:
 - (1) Obtaining appropriate authorizations and agreements for:
 - Any external connections required by their systems.

- Any systems/services they own that are placed outside a CNCS firewall.
 - External Access through the CNCS perimeter into their systems that are located inside the CNCS network.
- (2) Applying appropriate perimeter protections to any externally accessible resources that they own.
 - (3) Configuring any perimeter resources that they own (including security devices) in accordance with the above-specified guidance.
- (b) Information Custodians are responsible for:
- (1) Assisting Information Owners with the implementation and management of perimeter protections and system configurations to comply with this policy, including developing procedures for monitoring and auditing perimeter security systems.
 - (2) Assisting the CISO with auditing of perimeter protections and system configurations.
 - (3) Immediately reporting any perimeter breaches or potential vulnerabilities to the CISO.
- (c) Information Users are responsible for accessing the Internet and other external systems only through CNCS approved connections and in accordance with CNCS security procedures.
- (d) The Chief Information Security Officer (CISO) is responsible for:
- (1) Auditing CNCS information resources for compliance with this policy.
 - (2) Reviewing and approving access, connectivity, and services provided between the CNCS network and external systems.

6. DEFINITIONS:

- (a) DMZ (De-militarized Zone) - Any un-trusted network connected to, but separated from, the corporate network by a firewall, used for external (Internet/partner, etc.) access from within CNCSNET or to provide services to external parties.
- (b) Encryption – The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.
- (c) Firewall - A program that protects a computer or network from other networks by limiting and monitoring network communication.
- (d) Intrusion - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource through unauthorized access or penetration of an information resource.
- (e) Intrusion Detection System (IDS) – A system that analyzes network traffic to detect anomalies and provide alerts regarding possible intrusions.

- (f) Perimeter – The boundary between CNCS owned/operated information resources and those under the control of another party.
- (g) Perimeter Equipment – Any devices or servers which form part of the perimeter (e.g., perimeter router), are deployed to protect the perimeter (e.g., firewall), or which reside on the perimeter (e.g., DMZ web servers).
- (h) Proxy Server - A system that acts on behalf of another user or process. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
- (i) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.
- (j) Untrusted Network - Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy.
- (d) NIST Special Publication 800-94, Guide to Intrusion Prevention and Detection Systems.
- (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

- (g) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

11. EFFECTIVE DATE: June 1, 2009

11. REVISION HISTORY:

- (a) Original Publication June 2007
- (b) Reviewed and updated July 2008
- (c) Reviewed and updated May 2009

12. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SYSTEM & SERVICES ACQUISITION

ISP-C-17-0905

1. **SUBJECT:** Security considerations and requirements must be included in the acquisition of information systems and services.
2. **SCOPE:** This policy applies to the acquisition of any information system or to any service that will operate, use, or have access to information on behalf of CNCS.
3. **DESCRIPTION:** The increased use of commercial products and services to collect, process, store, and transfer CNCS data presents additional risks to Corporation data. Contractors must be held accountable for meeting federal requirements and CNCS security policies. In order to do this effectively, this must be addressed early in the system acquisition process.
4. **REQUIREMENTS:**
 - (a) The Corporation must include language in all contracts and agreements specifying that the contractor/partner must adhere to Federal Information Security Management Act (FISMA) and Privacy Act requirements. The following statement must be included in all of contracts and agreements for any systems or services which involve collecting or handling information on behalf of the Corporation:

“As a federal agency, the Corporation for National and Community Service (CNCS) is subject to and complies with the security requirements of the Federal Information Security and Management Act (FISMA). The Contractor shall ensure that services and products provided under a contract resulting from this solicitation shall comply with the Corporation’s information security program and privacy program policies, and Contractor Security Requirements available at http://www.nationalservice.gov/home/security_and_privacy_policy/index.asp.”
 - (b) Security requirements and specifications must be included, either explicitly or by reference, in all contracts, and solicitations for contracts, for information systems and information services.
 - (1) The security requirements specified for the contract should be based on an assessment of risk for the contract and the FIPS 199 security category of the system covered by the contract.
 - (2) Requirements should include the following:
 - required security capabilities

- required design and development processes
 - required test and evaluation procedures
 - required documentation
- (3) Documentation requirements should include:
- Documents describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.
 - Administrator and User guides with information on configuring, installing, and operating the information system; and effectively using the system's security features.
- (c) The acquisition of commercial information technology products should be consistent with NIST Special Publication 800-23 which provides guidance on the acquisition and use of tested/evaluated information technology products.
- (d) Security and privacy requirements must be included within all IT investments
- (1) Security must be integrated into and funded over the lifecycle of each system undergoing development, modernization, or enhancement.
 - (2) Steady-state system operations must meet existing security requirements before new funds are spent on system development, modernization or enhancement.
 - (3) As part of the capital planning and investment control process, the organization must provide the resources required to adequately protect the information system.
 - (4) Security requirements for the information system must be included in business case planning.

5. ROLES & RESPONSIBILITIES:

- (a) Procurement Services will:
- (1) Ensure that CNCS security requirements are included in all contracts for information systems and services.
 - (2) Monitor contracts for compliance with requirements.
- (b) System Owners will:
- (1) Include security requirements in all procurement requests and cooperative agreements that they request.
- (c) Contracting Officers Technical Representatives (COTRs) will:
- (1) Provide day-to-day oversight of the contractor's compliance with requirements.

- (2) Act as liaison to the contractor for any audits of the contractor's compliance.
- (d) The Chief Information Security Officer (CISO) will provide guidance on security requirements to be included in contracts.

6. DEFINITIONS:

- (a) Metrics - Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
- (b) Plan of Actions and Milestones (POA&M) - A tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

- 8. POINT OF CONTACT:** CNCS Chief Information Security Officer (CISO)

- 9. ATTACHMENTS:** None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006
- (c) OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, February 28, 2000
- (d) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

- 11. EFFECTIVE DATE:** June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication July 2008
- (b) Reviewed and updated May 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SYSTEM MAINTENANCE

ISP-C-18-0905

1. **SUBJECT:** Systems are maintained in accordance with best practices to ensure their availability, integrity, and confidentiality.
2. **SCOPE:** This policy applies to all information systems operated by or on behalf of CNCS.
3. **DESCRIPTION:** System maintenance shall be employed on all CNCS information systems addressing critical aspects of hardware and software maintenance including scheduling of controlled periodic maintenance; maintenance tools; remote maintenance; maintenance personnel; and timeliness of maintenance.
4. **REQUIREMENTS:**
 - (a) CNCS will schedule, perform, document, and review routine and preventative maintenance, as well as repairs on each system and component in accordance with manufacturer or vendor specifications.
 - (1) Software updates will be applied in accordance with CNCS Patch Management policies.
 - (b) Where feasible, automated mechanisms will be used to schedule and conduct maintenance and to create maintenance records.
 - (c) Maintenance records will be maintained which include the following:
 - (1) Date of maintenance
 - (2) Name of individual performing the maintenance (and escort if applicable)
 - (3) Description of maintenance performed
 - (4) List of equipment removed or replaced
 - (d) Maintenance may only be performed by authorized personnel
 - (1) Maintenance tools will be controlled to ensure use only by authorized personnel.
 - (2) Maintenance personnel must have an appropriate background clearance or be closely supervised by personnel who are cleared and have authorization to perform maintenance activities.
 - (e) The use of remote maintenance and diagnostic tools must be authorized and monitored.
 - (1) Remote maintenance is to be documented in the SSP.

- (2) CNCS will maintain records of all remote maintenance and diagnostic activities.
- (3) Remote maintenance must be performed through a secure encrypted connection in accordance with CNCS Remote Access and Encryption policies.
- (4) When remote maintenance is completed, all sessions and remote connections invoked in the performance of that activity will be terminated.
- (f) Maintenance tools will themselves be properly maintained to ensure their effectiveness.
- (g) Any hardware or software brought in specifically to perform diagnostic/repair activities must be approved and closely monitored
 - (1) Any maintenance tools brought into the facility by external maintenance personnel will be inspected for obvious improper modifications.
 - Antivirus and other appropriate tools will be run to ensure that the tools do not contain malicious code.
 - (2) Any maintenance tools or replaced equipment taken out of the facility will be inspected to ensure they contain no residual Corporation data.
 - Maintenance activities will comply with CNCS media management policies including sanitization.
- (h) CNCS will obtain maintenance support and spare parts for all critical systems and keep these current and available in case of emergency.
- (i) Changes made to systems as part of maintenance activities will be made in accordance with CNCS Change Control policies and procedures.

5. ROLES & RESPONSIBILITIES:

- (a) Information Owners are responsible for ensuring that any systems they own are in compliance with this policy.
- (b) Information Custodians are responsible for developing and following maintenance procedures which comply with the requirements in this policy.

6. DEFINITIONS:

- (a) Maintenance tools – hardware and software used to conduct maintenance on the information system, including diagnostic and test equipment.
- (b) Remote maintenance – Maintenance and diagnostic activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet).

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use

of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Chief Information Security Officer (CISO)

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (b) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (c) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- (d) NIST Special Publication 800-123, Guide to General Server Security
- (e) NIST Special Publication 800-88, Guidelines for Media Sanitization
- (f) NIST Special Publication 800-40, Creating A Patch & Vulnerability Management Program
- (g)

11. EFFECTIVE DATE: June 1, 2009

12. REVISION HISTORY:

- (a) Original Publication June 2009

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.



**Corporation for National & Community Service
Office of Information Technology**

**Information Security
Program Handbook**

May 2009

This Handbook constitutes CNCS' Information Security Program procedures and guidelines, and incorporates CNCS policy for protecting unclassified information resources. All CNCS personnel are responsible for complying with the policies and procedures contained herein.

The CNCS Chief Information Security Officer (CISO) is responsible for updating and maintaining this Handbook.

Security questions may be directed to:

Juliette Sheppard
Chief Information Security Officer
Office of Information Technology
Corporation for National & Community Service
(202) 606-6611

TABLE OF CONTENTS

SECTION 1: Introduction	1-1
1.1 What Is Information Security?	1-2
1.2 What Is the Information Security Program?	1-2
1.3 What Happens If CNCS Information Security Policies Are Violated?	1-3
1.4 What If I Can't Comply With A Policy?	1-4
1.5 Who Is Responsible for Information Security at CNCS?	1-5
1.6 Where Do I Get More Information?	1-7
1.7 Who Can I Contact If I Have Questions?	1-7
SECTION 2: Guide For Information Users	2-1
2.1 Understanding And Accepting Your Information Security Responsibilities	2-2
2.2 Reporting Information Security Incidents	2-4
2.3 Does CNCS Audit The Use Of Information Resources?	2-5
2.4 Acceptable Use of CNCS Resources	2-6
2.5 Access To CNCS Resources	2-9
2.6 Screening and Authorization	2-9
2.7 Passwords & UserIDs	2-9
2.8 Physical Access	2-10
2.9 Remote Access	2-11
2.10 Access to the Internet	2-12
2.11 Mobile Computing	2-12
2.12 Using Wireless Networks	2-13
2.13 Electronic Mail	2-13
2.14 Protecting Against Computer Viruses and other Threats	2-14
2.15 Protecting Media	2-15
2.16 Telephone Security	2-17
SECTION 3: Guide For Supervisors	3-1
3.1 Understanding And Accepting Your Security Responsibilities	3-2
3.2 Maintaining Security Awareness	3-2
3.3 Reporting Security Incidents	3-3
3.4 Employee Security Training Program	3-4
SECTION 4: Guide For Information Owners	4-1
4.1 Understanding And Accepting Your Security Responsibilities	4-2
4.2 Categorizing Resources	4-3
4.3 Assigning An Information Custodian	4-3
4.4 Risk Management	4-4
4.5 Developing System Security Plans	4-4

4.6 Certifying & Accrediting Your Systems	4-5
4.7 Vulnerability Testing	4-6
4.8 Vulnerability Remediation	4-7
4.9 Contingency Planning	4-7
4.10 System Acquisition	4-8
4.11 System Development Lifecycle (SDLC)	4-9
4.12 Application Security	4-11
4.13 System Reports	4-11
4.14 External Systems	4-11
4.15 Security Training & Awareness	4-12
4.16 Incident Reporting	4-12
4.17 Incident Response	4-12
4.18 Authorizing Access Permissions	4-13
4.19 Identifying and Authenticating Users	4-13
4.20 Maintaining Audit Trails	4-16
4.21 Backup & Recovery	4-17
4.22 Media Management	4-18
4.23 Asset Management	4-18
4.24 Managing Changes	4-19
4.25 Patch Management	4-20
4.26 Physical & Environmental Security	4-20
4.27 Protecting Databases	4-21
4.28 Using Encryption	4-22
4.29 Remote Access	4-23
4.30 Server Security	4-24
4.31 Network Security	4-25
4.32 Electronic Mail	4-26
4.33 Mobile Devices	4-26
4.34 Wireless Security	4-27
4.35 Perimeter Protection	4-28
4.36 Emerging Technologies	4-29
4.37 Telephone Security	4-30
4.38 Networked Copiers	4-31
<i>SECTION 5: Guide For Information Custodians</i>	<i>5-1</i>
5.1 Understanding and Accepting Your Security Responsibilities	5-2
5.2 Developing System Security Plans	5-3
5.3 Certifying & Accrediting Systems	5-3
5.4 Contingency Planning	5-4
5.5 Vulnerability Testing	5-4

5.6 Vulnerability Remediation	5-5
5.7 Security Training & Awareness	5-5
5.8 Incident Reporting	5-5
5.9 Incident Response	5-6
5.10 System Development	5-6
5.11 Application Security	5-8
5.12 System Reports	5-8
5.13 Managing Access Permissions	5-9
5.14 Identification & Authentication	5-9
5.15 Maintaining Audit Trails	5-12
5.16 Managing System Changes	5-13
5.17 Backup & Recovery	5-14
5.18 Media Management	5-15
5.19 Patch Management	5-15
5.20 System Maintenance	5-16
5.21 Using Encryption	5-17
5.22 Emerging Threat Defense	5-18
5.23 Physical Security	5-18
5.24 Asset Management	5-19
5.25 Server Security	5-20
5.26 Protecting Databases	5-21
5.27 Network Security	5-22
5.28 Remote Access	5-23
5.29 Web Security	5-23
5.30 Mobile Devices	5-24
5.31 Wireless Security	5-24
5.32 Workstation Security	5-25
5.33 Electronic Mail	5-25
5.34 Perimeter Protection	5-26
5.35 Telephone Security	5-28
5.36 Networked Copiers	5-30
5.37 Emerging Technologies	5-31
<i>Appendix A: Information Security Glossary</i>	<i>1</i>

SECTION 1:

INTRODUCTION



1.1 What Is Information Security?

“Information security” refers to protecting information resources from being misused, either intentionally or accidentally. This includes protecting these resources from being lost, stolen, destroyed, or altered in an unapproved manner, as well as using these resources for illegal, unethical, or other inappropriate purposes.

Information resources include equipment and software that are used to process information, as well as the information itself. Computer equipment, telephones, fax machines, network connectivity (including Internet connections and dial-up accounts), software programs, databases, documents (both electronic and printed), and even personnel, are examples of information resources.

1.1.1 Why Is Information Security Important to CNCS?

CNCS has many critical and sensitive information resources to protect, including computer equipment, software, business data, client information, intellectual property, and confidential personnel records. The safeguarding of all of these information resources is vital to the continued operation and success of CNCS.

As a federal entity, CNCS faces a variety of threats, ranging from terrorist acts to theft to accidental exposure/alteration of data. Inherent vulnerabilities also exist in the computer systems themselves. Each of these threats and vulnerabilities, when targeted at critical assets, can have a serious impact on the ability of CNCS to perform its mission.

1.1.2 Why Should Information Security Be Important To You?

By helping to safeguard CNCS information resources, you are helping to secure the tools needed to perform your duties, as well as protecting the continuation of CNCS’ mission. Additionally, there are federal and local laws and regulations that specify information security responsibilities and rules for everyone who uses information resources at CNCS. Under these laws, you could be held personally accountable, and fined, or even jailed, for security violations or lack of due diligence.

1.2 What Is the Information Security Program?

The CNCS Information Security Program (ISP) is a comprehensive set of initiatives designed to protect critical CNCS information resources so that they can be used to support CNCS’ mission. The ISP is also intended to ensure that CNCS is compliant with all federal regulations and other applicable laws, and to protect CNCS’ reputation.

The program includes policies and procedures that specify how to securely and legally use information resources at CNCS. Also included is a comprehensive set of activities to promote security awareness and educate everyone at CNCS on their information security responsibilities.

1.2.1 What Is Included In The Program And How Is The Program Structured?

The core of the program is a set of information security policies, based on legal requirements, federal government standards, and CNCS management objectives, that specify the “rules” for using and protecting information resources. Each policy discusses a specific security topic or type of information resource. The policies incorporate requirements and guidelines, roles and responsibilities, penalties for violations, the reason for each policy, and other important information pertaining to the particular security topic.



Standards and procedures provide step-by-step details on how to meet the requirements specified in the policies. Essentially, these documents provide the details for meeting the requirements of the policies.

To make it easier for you to understand the information security requirements, and your security responsibilities, we have developed this Handbook. The Handbook serves as your primary reference for understanding and meeting your information security responsibilities.

Additionally, information security training is provided, and required, for all CNCS personnel, to make sure that everyone understands CNCS security policies and maintains awareness of security issues. (More information on the information security training program is provided later in this Handbook)

1.3 What Happens If CNCS Information Security Policies Are Violated?

If anyone is found to be knowingly, willfully, or negligently in violation of any CNCS information security policy or any of the provisions in this Handbook, they will be subject to administrative or disciplinary actions, civil remedies and criminal penalties, including, but not limited to:

- Loss or limitations on use of information resources,
- Disciplinary action, from warning to termination of employment, and/or
- Referral for criminal prosecution.

1.3.1 What Is An Information Security Violation?

An information security violation is any breach of CNCS information security policies, procedures or guidelines, whether or not the confidentiality, integrity, or availability of information is actually compromised. Information security violations may occur knowingly, willfully, or through negligence. Any action or a failure to adhere to CNCS information security policies is considered a security violation.



Examples of information security violations include, but are not limited to:

- Failure to comply with CNCS information security policies and practices, including those outlined in this Handbook.
- Using CNCS information technology resources to violate Federal or state administrative, legislative, judicial or criminal laws or procedures.
- Assisting staff, contractors, or any external entities or individuals in performing any information security offense.

1.3.2 What Determines The Severity Of A Violation?

The significance of an information security violation does not depend only on whether the confidentiality, integrity, and availability of information are actually compromised; it depends on the intentions and attitudes of the individual who commits the violation. Access to CNCS information systems is a privilege that may be changed or revoked at the discretion of management. Ability and willingness to follow the rules for protection of CNCS information systems is a prerequisite for maintaining access to those systems.

1.3.3 How Does CNCS Handle A Violation?



After receiving notification of a possible violation, the CISO may initiate an inquiry to determine whether CNCS information security has been compromised. Based on the findings, the CISO may refer the matter to the Office of the Inspector General for further action.

The specific circumstances of the violation determine what sanctions, remedies or penalties CNCS will pursue.

1.4 What If I Can't Comply With A Policy?

1.4.1 When do I need a waiver

CNCS information security policies have been developed in accordance with federal guidance and will be implemented consistently to ensure effectiveness. However, there are occasional circumstances in which it is not completely feasible or in the best interests of the Corporation to comply with a particular policy provision or to do so within a particular timeframe. In such cases, there is a formal waiver process to evaluate and approve exceptions to the policies. These waivers will be granted in rare situations under specific circumstances and will be based on an analysis of risk.

In general, failure to comply with a policy will result in some sort of disciplinary action. In cases where you or a system that you own cannot comply with a policy or if complying with the policy would not be prudent and in the best interests on the government, you need to obtain a waiver to avoid the consequences of non-compliance. However, waivers are not intended to be used to pardon offenses that have already been committed. Requests are to be submitted as far in advance as possible.

Waivers of policy provisions that are recommended but not strictly required (as specified in the policy language) will be addressed through the Certification and Accreditation risk acceptance process (see ISP-P-10) rather than via a formal policy waiver. Therefore, you should not submit waiver requests for these.

1.4.2 How do I request a waiver?

A waiver request may be submitted to the CISO using the CNCS waiver request form. If the waiver is for a system, the request should be submitted by the system owner.

The waiver request must provide:

- A legitimate justifiable reason for waiving a security requirement.
- The specific scope and circumstances of the waiver (e.g., time period of waiver, specific resources or persons for which the requirement is waived, etc.)
- An understanding of the risks involved
- A recommendation for compensating security control(s) to mitigate the risk resulting from the waiver.

1.4.3

What is the waiver approval process?

The CISO, in consultation with applicable personnel (e.g., the CIO, CFO, General Counsel, etc.) will evaluate and respond to waiver requests. In the specific cases prescribed by federal guidance that require signature of the agency head for a particular waiver situation, the request will be escalated to the CEO.

Waiver requests will be evaluated based on the following criteria:

- Waivers will only be granted if it is within the Corporation's right to do so. Waivers cannot be approved that would violate legal requirements.
- An assessment of whether the reason for the waiver is truly accurate and justified, and whether there are alternatives for meeting the requirement that could be pursued.
- An analysis of the risks and proposed mitigation strategy

1.4.4

Do waivers expire?

Each waiver is approved for a specific period of time. Upon expiration of the granted waiver period, the waiver can be submitted for renewal if it is still needed. If a waiver is not renewed prior to the expiration of the period specified in the waiver, it will cease to be in effect at the end of the period.

If you or your system simply need additional time to implement a policy, your waiver request should include the amount of time you need to achieve compliance.

Waivers granting exceptions to policies (rather than delays) will be good for a period of 1-3 years depending on the nature of the exemption. This will allow for periodic re-evaluation of the need for the waiver.

1.5

Who Is Responsible for Information Security at CNCS?

EVERYONE who uses any information resource at CNCS shares in the responsibility to protect that resource and to use it appropriately. This includes employees, contractors, interns, temporary workers, and even visitors.

1.5.1

What Are The Information Security Roles At CNCS?

Your information security responsibilities are based on your assigned security role. For example, someone who administers a computer system will have different security duties than someone who uses the system to look up or enter information.

The information security roles at CNCS are:

- Information Users are individuals who use or have access to CNCS' information resources, including employees, interns, temporary workers, contractors, vendors, and visitors. When you are using any kind of CNCS information resource, or have access to any CNCS, client, or government data, you are an Information User.
- Supervisors are CNCS employees who have formal supervisory responsibility for employees, contractors, or other information users. This includes managers, COTRs, visitor escorts, and other supervisory personnel. It is crucial that



Supervisors serve as a good example for their employees to follow, as well as helping them to understand and meet their information security responsibilities.

- **Information Owners** are the individuals ultimately responsible for information resources, and are generally Departmental Directors or designated senior managers. The initial owner is the individual who creates, or initiates the creation or storage of, information. For example, the initial owner may be the person who writes a document, creates a database, or purchases a piece of equipment. Once created or installed, the individual’s respective CNCS business unit becomes the Owner, with the Departmental Director of that unit taking official responsibility.
- **Information Custodians** are individuals who develop, implement, maintain, or administer information resources on behalf of Information Owners. For example, OIT staff (including system engineers, database administrators, application developers, etc.) often serve as custodians for systems or data owned by CNCS business units.

**1.5.2
 How Do You Know
 What Role(s) You Are
 Assigned?**

Individuals may serve in multiple roles, depending on the different aspects of their jobs. For example, a Program Director may serve as an Information Owner for a particular resource, as a Supervisor for employees in his/her department, and as an Information User.

The above role descriptions should help you determine your security role(s). It is up to you to find out which roles apply to you, and to understand and perform the responsibilities associated with those roles. If you are unsure which role(s) apply to you, please consult your supervisor or the CISO for further guidance.

**1.5.3
 What Are The
 Responsibilities Of
 Each Security Role?**

The remainder of this Handbook is organized by security role. Each section focuses on the responsibilities of a specific role. You should read the sections for each of your roles and make sure that you fully understand the responsibilities discussed in those sections.

Information Users		SECTION 2: Guide For Information Users
Supervisors		SECTION 3: Guide For Supervisors
Information Owners		SECTION 4: Guide For Information Owners
Information Custodians		SECTION 5: Guide For Information Custodians

**1.5.4
 Are There Specific
 Individuals Who Have
 A Special Role In
 CNCS Security?**

In addition to the general security roles, there are a few individual positions that have specific security responsibilities. These include:

- The **Chief Executive Officer (CEO)** of CNCS is responsible for ensuring that “that the information security policies, procedures, and practices of the executive agency are adequate.”
- The **Chief Information Officer (CIO)** promotes a coordinated, interoperable, secure and shared corporate IT infrastructure.



- The Chief Information Security Officer (CISO) is the individual designated within CNCS to develop and operate the information security program. The CISO is responsible for ensuring that CNCS complies with federal information security requirements and other applicable laws, and that CNCS resources are adequately protected.
- The Privacy Officer is responsible for privacy compliance across an organization, including privacy compliance measures that apply to information security assets and activities.
- Information System Security Officers (ISSOs) are designated by the System Owners. An ISSO's responsibilities include defining security procedures for the specific system, providing information for C&A of the system, participating in incident response, etc. for the system.
- The Director of Personnel Security is responsible for the overall implementation and management of personnel security controls across CNCS, to include integration with specific information security controls.
- The Facility Security Officer is responsible for the overall implementation and management of physical security controls across an organization, to include integration with applicable information security controls.
- The Acquisitions/Contracting function is responsible for ensuring that all agency contracts and procurements are compliant with the agency's information security policy and contain appropriate information security and privacy clauses.
- Office of the Inspector General (OIG) investigates, audits, and takes other action in accordance with the Inspector General Act to detect, prevent, and investigate wrongdoing. In accordance with FISMA, the OIG conducts an annual independent assessment of the CNCS information security program to assess the Corporation's security practices and identify additional security measures needed

1.6 Where Do I Get More Information?

Copies of the CNCS information security policies, as well as a glossary, are provided in the Appendices of this Handbook. Additional information security information will be posted on the CNCS Intranet.

1.7 Who Can I Contact If I Have Questions?

If you have any questions about information security, please contact the CNCS Chief Information Security Officer (CISO), Juliette Sheppard.



SECTION 2:

GUIDE FOR INFORMATION USERS



2.1 Understanding And Accepting Your Information Security Responsibilities

An important aspect of CNCS' Information Security Program (ISP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making everyone aware of their security responsibilities and teaching them correct practices can CNCS reduce the level of security risk to its information systems.

Many components of CNCS' ISP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into CNCS' program. Ensuring that you gain an understanding of your responsibilities is vital to CNCS because without your knowing the necessary security measures (and to how to use them), CNCS' information security will not be effective.

As someone who uses or has access to CNCS' information resources¹, you are referred to as an "Information User." Whether you are a regular employee, an intern, a temporary worker, or a contractor, information security is your personal responsibility, and you serve a critical role in protecting the resources you have been granted to use. As such, you are responsible for familiarizing yourself with, and abiding by, the policies and procedures outlined in this Handbook.

2.1.1 What Are The Responsibilities Of An Information User?

Your responsibilities are outlined throughout this section of the Handbook. However, here is a summary of some of your responsibilities:

- You must review, understand and accept your information security responsibilities.
- You must maintain awareness of information security policies by participating in CNCS' information security training program and by reviewing this Handbook.
- You should discuss with your supervisor or the CISO any information security policies or procedures that you do not understand.
- You must protect CNCS information resources in your possession from theft, loss, damage and unauthorized activities including disclosure, modification, deletion, and misuse; and immediately report any loss, theft or damage to those resources.
- You must obtain, use, or disclose CNCS information only in an authorized fashion and only for authorized purposes.
- You must exercise due diligence to prevent accidental mis-entry, modification, or deletion of data.
- You must act responsibly so as to ensure the ethical use of CNCS information resources in compliance with the Standards of Ethical Conduct for Employees of the Executive Branch and CNCS' Ethics Program.
- You must promptly report any suspected violations of CNCS security policies to the CISO, the Information Owner, or your supervisor.

¹ Information Resources are the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

2.1.2 Reviewing and Understanding CNCS Information Security Policies



2.1.3 Completing CNCS' Information Security Training Program

For more information on Information Security Training, see ISP-04, *Security Training and Awareness*.



2.1.4 Completing The User Security Agreement

This Handbook provides information and instructions for Information Users on:

- Fulfilling your security responsibilities;
- Auditing and privacy considerations;
- Acceptable and unacceptable use of CNCS information resources; and
- Policies and procedures you must follow when using CNCS information systems

You should also take the opportunity to review the detailed Information Systems Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have questions, please ask your supervisor or the CISO for clarification.

The Federal Information Security Management Act (FISMA) requires every federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, OMB Circular A-130 requires that training be completed prior to the granting of access and on a periodic basis.

A Security Training and Awareness program is crucial to the safeguarding of CNCS information resources. Information security policies and standards cannot be effective unless everyone, regardless of level in the organization, is aware of the importance of information security, understands CNCS procedures, and performs required practices.

For these reasons, all employees, including interns, as well as contractors, and other personnel who have internal access to CNCS information resources, must fulfill CNCS' information security training program.

CNCS Information Users (excluding external members, volunteers, and grantees) will complete information security training. This training consists of the following three activities:

1. Information security training is incorporated into the new hire and new contractor orientation processes.
2. All Information Users must complete annual information security refresher training.
3. Information Custodians, Information Owners, and other personnel with responsibilities related to securing systems receive additional security training.

Information security training may be in the form of classroom, one-on-one, computer-based, or other format, as determined by the CISO.

External users (including external members, volunteers, and grantees, will be asked to read and electronically accept posted policies and a rules of behavior statement.

All CNCS employees, interns, contractors, and other personnel, must acknowledge and agree to comply with CNCS' information security policies and procedures in order to have access to CNCS information resources. The "User Rules of Behavior" is to be signed by each employee upon completion of information security orientation training.

See ISP-P-13, *Acceptable Use Of Information Resources*, for a copy of the agreement

2.1.5 Maintaining Security Awareness



One of CNCS' information security program goals is to help Information Users maintain security awareness on an ongoing basis. Information Security is not a one-time event, but a continuous effort and "state of mind." This is achieved by reinforcing appropriate behaviors and mindset on a continuous basis. Effective information security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

CNCS' security awareness program sets the stage by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure. It also reminds users of the procedures that must be followed. Hopefully, awareness will stimulate and motivate all CNCS staff to care about security and remind everyone of important security practices.

The CISO will periodically issue information notices to CNCS employees to remind them of basic security practices (*e.g.*, protecting your passwords). The CISO will also provide brown bag discussions and briefings on special topics (*e.g.*, spam filtering).

It is your responsibility to exercise security awareness at all times when performing your CNCS duties, and to take an active part in protecting CNCS resources.

2.2 Reporting Information Security Incidents

You must immediately report any suspected information security incidents so that CNCS may respond in a timely manner to correctly handle the incident, minimize disruption of critical information services, and minimize loss or theft of sensitive and mission-critical information.

Your cooperation and participation in reporting security incidents is vital to CNCS' maintaining the security of its information resources. It is important that all information users maintain vigilance regarding information security, and immediately report any suspected incidents in order to minimize potential damage to CNCS.

2.2.1 What Is An "Information Security Incident?"



An "information security incident" is any activity or event that has occurred that threatens the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

Examples of information security incidents include (but are not limited to):

- Suspected violations of any CNCS information security policies.
- Loss or theft of laptops, mobile devices (such as PDAs), security tokens, or other items that may provide access to or contain CNCS data.
- Attempts by unauthorized individuals to gain access to CNCS information or systems.
- Accidental disclosure, modification, or destruction of information.

A "critical information security incident" is an incident that will result in a severe impact to CNCS resources if not addressed immediately.

2.2.2 How To Report An Information Security Incident

For more information on Reporting Security Incidents, see ISP-P- 03, *Incident Reporting*.

You must report suspected incidents to the CISO, the OIT Help Desk, the Information Owner, your supervisor, or any OIT director as quickly as possible. You may report incidents either verbally or in writing. It is recommended that you retain proof that you reported the incident.

After you notify the CISO, the Information Owner or your supervisor, you may be required to document relevant information about the suspected incident. You may also be requested to assist the CISO or system administrators with resolution of the incident. Your full cooperation in resolving the incident is required.

2.3 Does CNCS Audit The Use Of Information Resources?

For more information on Auditing, see ISP-C-05, *Audit Trails*.

CNCS regularly audits the use of information resources to ensure accountability for the use of those resources, detect security violations, and to proactively scan for vulnerabilities. All use of CNCS information resources may be monitored by CNCS at any time. You should not have an expectation of privacy or anonymity while using CNCS information resources, including email and Internet access.

As a CNCS Information User, you are governed by CNCS' authorized limited personal use policies. By using CNCS information systems and other office equipment, you imply your consent to disclosing the contents of any files or information maintained or passed-through those information systems or office equipment. As required by law, CNCS may disclose information generated on its information systems to law enforcement or oversight organizations. The information security program in no way removes any privilege or protection afforded CNCS employees under the Privacy Act, the Freedom of Information Act, or any other law or regulation.



In order to enforce information usage policies and security measures, and to be able to investigate security incidents, automated records of access to and alteration of information systems and data are maintained. To accomplish this, a record of activity (or "audit trail") of system and application processes and user activity of systems and applications is maintained. This is used to investigate security incidents, monitor use of CNCS resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. Audit trails also assist in detecting security violations, performance problems, and flaws in applications.

System administrators (on behalf of Information Owners) have the ability to audit network logs (via server, application, router, firewall and other major network device transaction logs), employ monitoring tools, and perform periodic checks for misuse. The CISO is required to conduct periodic reviews of audit logs.

2.3.1 What Is An "Audit Trail?"

In the context of computer systems, an "audit trail" is a record of activities that occur on the system. The audit trail is generally composed of log files that track such things as user login, file access, system modification, resource usage, and other activities. These files can provide information regarding any actual or attempted security violations that may have occurred on the system, and may serve as evidence for disciplinary or criminal action.

2.3.2 **Can I Expect Any Privacy When Using CNCS Information Resources?**



No. You do not have a right, nor should you have an expectation, of privacy while using CNCS information systems. When you use CNCS information systems, it is with the understanding that such use is not private and is not anonymous.

There is no right of privacy on the part of any individual regarding any information transmitted, stored or received via CNCS' information systems. Use or access to the network constitutes consent to CNCS' limited personal use policy, and to the monitoring, storage, retrieval or disclosure of any information transmitted, stored or received via the network for any purpose, including employee discipline, contractual remedies or criminal prosecutions.

Avoid using CNCS information systems for any activities that you wish to keep private.

2.4 **Acceptable Use of CNCS Resources**

For more information on Acceptable Use, see ISP-01, *Acceptable Use of Information Resources*, and CNCS Management Directive 94-04.

CNCS information resources are for use only by authorized persons and only for authorized purposes. Access to computers, systems, networks, and data owned by the government is a privilege that imposes certain responsibilities and obligations and that is subject to governing laws. CNCS' authorized limited personal use policy is intended to promote the efficient, ethical and lawful use of CNCS information resources, yet allow employees the opportunity for limited personal use of those resources.

As a CNCS Information User you must act in a legal, ethical, responsible, and secure manner while using CNCS information systems. Inappropriate use of information resources exposes CNCS to risks including compromise of systems and services, legal issues, financial loss, and damage to reputation.

You are also responsible for exercising good judgement in using CNCS information resources efficiently. You should use your common sense to do what a reasonable person would do to protect CNCS information resources.

The following two sub-sections discuss acceptable and unacceptable use of CNCS information resources.

2.4.1 **What Is Acceptable?**



You may use CNCS-provided information resources only for authorized purposes. Authorized purposes include official use, which is use for CNCS-related business in accordance with your job functions and responsibilities. Authorized purposes also include emergency use, such as sending an emergency email to notify a spouse of illness during working hours. Authorized purposes also include limited personal use of information resources if that use does not result in a loss of employee productivity, does not interfere with official duties or business, and involves "minimal additional expense" to the government.

Authorized limited personal use may incur only "minimal additional expense" to CNCS in areas including but not limited to:

- Communications costs (*e.g.*, telephone charges, telecommunications traffic, etc.).
- Use of consumables in limited amounts (*e.g.*, paper, ink, toner, etc.).
- General wear and tear on equipment.
- Data storage on IT devices (*e.g.*, moderate email message sizes and quantities).

Examples of authorized limited personal use include minimal or non-duty use of phones or

computers to:

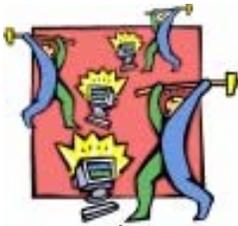
- Check Thrift Savings Plan
- Seek employment
- Deal with employee assistance issues
- Communicate with charity organizations
- Perform academic work/training that does not interfere with completing your job responsibilities.

All use must be in compliance with CNCS information security policies.

CNCS information resources may be used only for authorized purposes, which are discussed in the preceding sub-section. In addition to understanding CNCS' authorized use policy, you should be aware of the following specific activities, which are *strictly prohibited* while using CNCS information resources:

- You may not use CNCS information resources to maintain or support a personal business, including use of those systems to assist relatives, friends, or other persons in such activities. This prohibition includes personal activities that are for commercial purposes, that support "for-profit" activities or are intended to generate income (*e.g.*, electronic day-trading), or that support other outside employment or business activity (*e.g.*, consulting for pay, sales or administration of business transactions, sale of goods or services, or acting as a real estate agent).
- You may not engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity using CNCS resources.
- You may not access or disseminate material that is offensive or harassing in nature, including material that disparages others based on race, religion, ethnicity, gender, sexual orientation, age, disability or political affiliation. You may not access or disseminate sexually explicit or sexually oriented messages, images, or sounds.
- You may not acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data, privacy information, copyrighted or trademarked material or material with other intellectual property rights (beyond fair use), or proprietary data, without authorization.
- You may not disseminate trade secrets or business *sensitive* information, except as permitted by law or regulation, including posting agency info to external newsgroups, bulletin boards or other public forums without authority.
- You may not transmit, store, or process classified data except as authorized.
- You may not conduct any personal activity that could create the perception that the communication was made in your official capacity as a Federal Government employee, unless appropriate CNCS approval has been obtained.
- You may not create, access, or download material related to illegal activities (*e.g.*, gambling, illegal file swapping, software piracy, etc).
- You may not perform any action that would otherwise violate the Standards of

2.4.2 What Is Not Acceptable?



Ethical Conduct for Employees of the Executive Branch.

- You may not conduct any personal use that could generate more than minimal additional expenses to CNCS and/or cause congestion, delay, or disruption of service to any CNCS system or equipment (*e.g.*, downloading large video files). This prohibition includes executing a program that may hamper normal CNCS computing activities.
- You may not send unsolicited email messages (spam) or create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings.
- You may not use CNCS' systems to gain unauthorized access to other systems.
- You may not access information resources, data, equipment, or facilities in violation of any restriction on use. Further, you may not access CNCS systems that are not necessary for the performance of your duties. Nor may you perform functions that are not related to your job responsibilities on authorized systems.
- You may not make unauthorized changes to CNCS computer resources, including installation of unapproved software or interference with security measures (*e.g.*, audit trail logs and antivirus software).
- You may not add components or devices (*e.g.*, PDAs, cameras, etc.) to CNCS desktops without explicit approval from the Deputy CIO.
- You may not connect unauthorized devices (including contractor or personal laptops) to the CNCS computer network without approval from the Deputy CIO.
- You may not copy proprietary software (or software licenses) or CNCS business data for personal or other non-United States government use.
- You may not perform unauthorized security scanning, network monitoring, or data interception that is not part of your regular job duties.
- You may not use another person's userID, with or without his or her permission. Nor may you allow anyone to use your userID.
- You may not reveal system passwords (*e.g.*, network login password, FPPS password, database password, etc.) to anyone who is not specifically authorized to use them. This includes revealing account passwords to others, including family and other household members, when government work is being done at home.
- You may not knowingly, without authorization, introduce a program into the CNCS environment that could hamper normal computer operations.
- You may not intentionally corrupt or damage any information resource.
- You may not remove any CNCS information resource from the CNCS premises without authorization.
- You may not deny, or interfere with, the legitimate use of resources by other CNCS personnel.
- You may not otherwise violate any existing information security law, rule, regulation, CNCS policy or CNCS implementing procedure.



2.5 Access To CNCS Resources

For more information on Access Controls, see ISP-C-01, *Access Controls*.

2.6 Screening and Authorization

For more information, see ISP-C-06, *Personnel Security*.



2.7 Passwords & UserIDs

For more information on Passwords and UserIDs, see ISP-C-03, *Password Management*.



You may only access resources to which you have been authorized, and you may not circumvent the permissions granted to your accounts in order to gain access to unauthorized information resources.

Access to CNCS information resources is limited to those persons who have been appropriately screened and authorized. Any access granted to you to CNCS information resources will be based on the requirements of your duties, and you must have appropriate clearance for the sensitivity level of the resources to which you are granted access.

Therefore, you will be subject to at least a minimal background check (if you have not had a previous investigation and/or do not have any recent, documented positive suitability determination) prior to being granted access to *sensitive* information.

Additionally, if you are a contractor or other non-CNCS employee, you must sign a non-disclosure agreement protecting any *sensitive* data to which you will have access.

CNCS reduces the risk of unauthorized access of its information through the use of UserIDs and passwords. For example, your access to CNCS information resources is limited to the access required for you to perform your duties. You have been granted specific access privileges on each system, and those access privileges are associated with your userID (*i.e.*, logon name). Your password serves as authentication of your identity, and is used to grant or deny access to CNCS information systems. If you choose a poor password, it can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

As an Information User, *you are responsible for any activity initiated by your userID* since you are the only person who should have your logon information. You must protect your user account(s), and not allow anyone else to use your account or use your computer while logged in under your account (except as required for system administration). In order to protect your user credentials, you must adhere to the following rules:

- Do not lend or divulge your password to other persons, including individuals purporting to be system administrators.
- Change your password immediately upon your initial user logon, at least every 90 days, and any time it is suspected that your password may have been compromised.
- Never make your password visible on a screen, in writing (*e.g.*, on sticky notes), or on any other output device unless it is secured in an approved, locked area.
- When you leave your computer unattended, you must either log out or invoke protection of your system (*e.g.*, a password-protected screensaver).

2.7.1 What are the guidelines for choosing an effective password?

*If you need assistance with
selecting an appropriate
password, please contact the
OIT Help Desk*



2.8 Physical Access

For more information on
Physical and Environmental
Security, see ISP-C-07,
*Physical and Environmental
Security*.

- Never send your password via email.
- Avoid using the “remember password” feature on web sites and other applications.
- Choose effective passwords (see the following sub-section).

Adhere to the following guidelines for selecting effective passwords:

- Your password must be at least 8 characters and contain a combination of letters, numbers, and special characters.
- You should not use the same password at CNCS that you use for any non-CNCS computer accounts (*e.g.* an account on an Internet website).
- Do not reuse passwords.
- Don’t choose passwords that contain your userID (*e.g.*, “bob123” is not an appropriate password for user “bob”).
- Your password should not be a dictionary word in any language.
- Your password should not contain any proper noun or the name of any person, pet, child, or fictional character.
- Your password should not contain any employee serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.
- Your password should not contain any simple pattern of letters or numbers, such as “xyz123.”
- Do not simply increment the same password (such as fido1, fido2, etc.)
- You should use a password that is easy to remember (*e.g.*, a phrase, line from a song, or nonsense words) and that you can type quickly

CNCS information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. .

As an Information User, your physical security responsibilities include:

- Admittance to areas containing *sensitive* information resources is limited to individuals who have been authorized access to them. You must escort uncleared personnel through areas containing sensitive information.
- When uncleared personnel are present, you must protect *sensitive* information from observation, disclosure, or removal. This includes storing away documents and positioning all computer monitors to prevent viewing by unauthorized persons.
- Challenge any unrecognized and unescorted person in CNCS’ space to show appropriate id. Notify security immediately of unauthorized persons so that they may escort the person out of CNCS’ space.



2.9 Remote Access

For more information on Remote Access, see ISP-S--08 *Remote Access*.



- Lock your computer screen whenever you walk away from your computer.
- Shred any documents containing sensitive information when no longer needed.

Of course, you must immediately report any incident or condition contrary to CNCS' physical or environmental security.

You use remote access capability any time you access CNCS' network while outside the office (*e.g.*, while traveling or telecommuting). Remote access to CNCS poses an increased risk of intrusion into CNCS information systems by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of the CNCS network also lacks the protections afforded by CNCS' corporate firewall and other security measures. For these reasons, remote access is governed by special security requirements to mitigate the increased security risks that are present in this situation.

OIT has put in place technical measures to ensure that remote access is provided in a secure manner. For example, telecommuters must use multiple methods of authentication to access the CNCS network (*i.e.*, they must use their network passwords in conjunction with tokens). Additionally, information transferred over remote access connections is encrypted to protect it from unauthorized disclosure.

As an Information User you have certain responsibilities when using remote access:

- You must observe all of the same security policies when accessing CNCS information resources remotely that you would at the office.
- Any personal equipment, including personal home computers, used to connect to CNCS' information resources must meet CNCS remote access security requirements, including having an approved antivirus program installed and being configured with the latest software updates.
- You may not store *sensitive* CNCS data on non-CNCS computers.
- You must protect your remote access credentials, devices and connections from disclosure to, or use by, unauthorized persons, including family members.
- You may not change the hardware, software, or security configuration of any CNCS-owned computers, including laptops and other remote access PCs.
- To prevent unauthorized users from accessing *sensitive* CNCS information via open ports, remote access sessions and open terminal windows must never be unattended. You must log out rather than terminate a remote session when finished. You must also wait until you receive a confirmation of your log-out command before you leave the computer you are using.
- You must immediately report any suspected unauthorized use of your remote access account or any damage to or loss of CNCS computer hardware, software, or data that has been entrusted to your care.

2.10 Access to the Internet



Employees will access the Internet only through CNCS-approved Internet access points (e.g. CNCS firewalls). Any form of communication to or from workstations outside the internal (trusted) network that bypasses these protected access points is strictly prohibited without authorization. This includes the use of modems, leased lines to other networks, or wireless connectivity. Access to the Internet from outside of CNCS (e.g., using laptop while traveling) is not governed by this policy. However, such access must be compliant with CNCS Remote Access and Mobile Computing policies.

2.11 Mobile Computing

For more information on Mobile Computing, see ISP-S-07, *Mobile Computing*.



“Mobile devices” are any portable devices that can store or process data. Examples include laptop computers and PDAs (e.g., Blackberry, Palm).

The use of these devices outside the CNCS office environment poses risks to the devices and the information they contain. Mobile devices may also present a hazard to other CNCS resources upon their return to the CNCS office (e.g., by spreading a virus that was obtained outside the office). These devices also have the capability for direct connectivity to the Internet or other networks outside of the CNCS network which lack the protections afforded by CNCS’ corporate firewall and other security measures. That is why you must take additional security measures to reduce the risks presented by mobile computing.

CNCS has put in place technical measures to ensure that mobile devices are assigned to you already have some security in place. For example, all laptops have antivirus software installed. However, you have a major role in protecting the security of these devices.

Your responsibilities as a mobile computing Information User who uses include:

- To ensure that devices are inventoried and tracked, you will be asked to sign out laptops and other mobile computing devices before they are given to you.
- You must back up any data that is stored on the mobile device on a regular basis.
- You must take all reasonable precautions to protect mobile devices from loss, theft, tampering, and damage.
- You must ensure that the device is not used by unauthorized persons or for unauthorized purposes.
- You must immediately report the loss, theft, tampering, unauthorized access, or damage of any CNCS mobile device.
- Only store sensitive data on a mobile device if it is encrypted.



2.12 Using Wireless Networks

For more information on
Wireless Security, see ISP-S-
03, *Wireless Security*.



2.13 Electronic Mail

For more information on
Electronic Mail, see ISP-S-
10, *Electronic Mail*.

You may find that wireless communications and devices are convenient, flexible, and easy to use. Wireless devices transmit data without the use of cables. Examples of wireless communications include radio transmissions, cell phones, PDAs, laptops with wireless network cards, and other devices such as wireless headphones. Infrared devices such as cordless computer keyboards and cordless mouse devices are also included.

In addition to the risks that apply to all networks, wireless connectivity has additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be easily intercepted by anyone nearby who is actively listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this open architecture to access systems, destroy or steal data, and launch attacks that tied up network bandwidth and denied service to authorized users. Additionally, like any mobile devices, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to CNCS networks via the hijacked or stolen device.

Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted over it.

As an Information User, you are required to:

- Obtain approval from OIT before using or deploying any wireless technology to access or transmit CNCS information. This rule applies regardless of whether these devices are owned by CNCS.
- Safeguard wireless devices in your possession and safeguard CNCS information resources being accessed or transmitted via any wireless technology.
- Be aware that wireless interface cards are explicitly prohibited from being used at CNCS facilities.
- Immediately report the loss, theft, tampering, unauthorized access, or damage of any CNCS wireless or handheld device.

Email is an essential tool used by CNCS to conduct its business. However, email is inherently insecure and presents many risks to information security. Email can be read, altered, or deleted by unknown parties without the permission of the sender or recipient. Email can also be used to distribute viruses and other harmful programs that pose a threat to CNCS resources. Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.

As an Information User, you have certain responsibilities in supporting email security:

- You must understand that email can be intercepted or altered without your knowledge (both within and outside of CNCS.)



2.14 Protecting Against Computer Viruses and other Threats

For more information on Anti-Virus Measures, see ISP-C-14, *Emerging Threat Defense*.



- You are prohibited from using any CNCS email systems (or any other email systems accessed from CNCS computers) for prohibited purposes, as outlined in CNCS' *Acceptable Use of Information Resources* policy (ISP-P-13).
- You should not open attachments or click on links in messages from senders you do not know.
- You should report suspicious email messages to the OIT Help Desk.
- To minimize spam and avoid waste of CNCS resources, you should avoid using your CNCS email addresses for personal correspondence on the Internet, especially if this includes giving out your official email address to Internet shopping sites, bulletin boards, and mailing lists (that are not related to your duties.)
- You should have no expectation of privacy while using CNCS' email system.
- You may not direct unauthorized messages to the Corporation All Staff distribution group or other large groups of users.
- You must delete emails once they are no longer needed, in accordance with CNCS Record Management policies. On a periodic basis you must archive from the email server old emails that must be retained. Contact the OIT Help Desk for information and instructions on how to do this.

Security risks are constantly evolving. Not only are new viruses, spyware programs, and spam developed daily, but new kinds of threats are constantly emerging. In addition to electronic threats like viruses and spyware, social engineering and other attacks that bypass technical protections are also becoming an increasing issue. These threats can result in loss of information, reduced system performance, disclosure of *sensitive* information, identity theft, unauthorized system changes, and a myriad of other risks. It is critical that CNCS implement proactive measures to protect its information and systems from these emerging threats.

To minimize risks associated with viruses, spyware, and other threats, CNCS implements standard software and procedures to safeguard CNCS' servers, workstations, and other information resources. The use of security software, such as antivirus, is essential for protecting CNCS resources from the danger posed by malicious programs (malware). These programs check for malware on CNCS' computers and attempt to remove them before they can spread or perform further damage.

As an Information User, you have the following responsibilities:

- You may not unload or disable CNCS security software for any reason.
- Any computer used for remote access to the CNCS network (*e.g.*, a laptop used for telecommuting or a home computer used to do CNCS work) must have approved antivirus software loaded and updated on a regular basis. You should contact the OIT Help Desk for guidance on what antivirus software CNCS has been approved for this purpose.



2.15 Protecting Media

For more information on Backups and Media Management, see ISP-C-08, *Backup and Recovery*, and CNCS ISP-C-11, *Media Management*.



- You must notify the OIT Help Desk immediately if you think your computer may have become infected with a virus or spyware.
- You must take steps to avoid introducing malware into CNCS' computing environment, including:
 - Never open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these messages immediately.
 - Delete spam, chain, and other junk email without forwarding.
 - Never download files from unknown or suspicious sources.
 - *Never install any software on CNCS computers without specific permission from OIT.*
 - You must scan all portable media (e.g. disks, CDs, flash drives) for viruses before using them on a CNCS computer. This should be performed automatically by the antivirus software on your PC. However, it is a good idea to perform an extra manual scan of these media if they have been used outside of CNCS (e.g., if you brought it in from home.) Contact the OIT Help Desk for instructions on how to perform a virus scan.
 - If prompted to install anything from the web, always Cancel.
- Never give out *sensitive* information to anyone without verifying their identity.
- Participate in security training and awareness activities.

You may find the need to store data on "media" other than your CNCS computer or network drive. For example, disks, CDs, flash drives, and backup tapes, are all commonly used types of "storage media". These must be handled, stored, and disposed of properly in order to protect the data placed on them from unauthorized disclosure, damage, and abuse.

You are responsible for adhering to the following when using storage media:

- You may store CNCS data only on approved media. Contact the OIT Help Desk for assistance in identifying the appropriate storage media for your data.
- All storage media brought onto CNCS' premises or used with CNCS information systems must be scanned for viruses prior to use.
- You must take all reasonable steps to protect CNCS storage media in your possession from tampering or accidental damage.
- You are responsible for making your own backups of any data that is stored on media in your physical possession rather than on a CNCS server. Be aware that many threats exist that could cause the loss, corruption, or unavailability of data that is backed up on storage media. It is therefore essential that you maintain backup copies of all critical data that are stored on media so that they can be used to provide the continued availability and viability of these resources if unforeseen events occur. For example, you may copy your data to CNCS' network servers which are backed up daily.

2.15.1

What is the proper way to handle media that contains sensitive data?



2.15.2

What is the proper way to dispose of storage media?



- Special procedures must be applied to the handling and disposal of storage media that are used to store *sensitive* information, as described in the following two subsections.

The following procedures must be followed when storing *sensitive* data on portable media:

- You must mark any media containing *sensitive* data with labeling that includes any special handling instructions.
- You must secure any media containing *sensitive* data when it is not in use or unattended. You should put it in a locked drawer, cabinet, or safe.
- If you send any media containing *sensitive* information through the mail or a courier service, you must double-seal the media, with the outer envelope appropriately marked to reflect the level of sensitivity and the intended recipient.
- The delivery and receipt of media containing *sensitive* data must be monitored and accounted for to ensure that data is not lost and compromised while in transit.
- You may never store national security classified information (*i.e.*, Top Secret, Secret or Confidential information) on portable media unless you are authorized to do so and take security precautions required by law.
- You must immediately report the loss, theft, tampering, unauthorized access, or damage of any storage media that contain critical or *sensitive* CNCS data.
- When disposing of, or reusing, any media containing *sensitive* data, CNCS sanitization procedures must be followed (see next subsection).

Simply deleting data from media does not completely or permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly. Therefore, it is important to properly “sanitize” any media that may contain *sensitive* information once the media and/or the data is no longer needed.

“Sanitization” refers to the process that is used to wipe data from storage media so that data recovery is impossible. The most common types of sanitization are destruction (*e.g.*, burning or smashing), degaussing (*i.e.*, demagnetizing), and overwriting.

CNCS has special software and a standardized process for sanitizing media. If you have media that should be sanitized, please contact the OIT Help Desk for guidance and assistance with this process.

2.16 Telephone Security

For more information on
Telephony Security, see ISP-
S-09, *Telephony Security*.



CNCS telephony resources include telephones, fax machines, and modems. These are vulnerable to a variety of security threats and are subject to the same security requirements and protections as other information resources.

You must adhere to the following rules when using the CNCS phone system or CNCS-issued cellular phones, in order to protect the information communicated:

- You should have no expectation of privacy when using the CNCS phone system or CNCS-issued cellular phones.
- You should understand that CNCS may audit use of these resources, and that it is possible for third parties to tap or redirect phone calls outside of CNCS.
- You should never discuss *sensitive* information over a cell phone because of the ease of intercepting such communications.
- You may never discuss classified information over any phone that has not specifically been approved for such use.
- You should make sure that the person on the other end of the conversation is who they say they are. You must not give out *sensitive* information (including agency credit card information) unless you are sure of the identity of the person who is on the other end of the line.
- You must be cautious when discussing *sensitive* information that the conversation cannot be overheard by unauthorized persons (*e.g.*, visitors to CNCS). You should minimize use of the speakerphone.
- You must obey relevant laws regarding the recording of phone conversations, including informing the other party that you are recording.
- You must follow CNCS' Acceptable Use policy in using phone resources, just as you would with email or other information resources.
- You may not install modems or other telephony equipment without the explicit approval of the appropriate official (*e.g.*, the Deputy CIO for modems and related telephony equipment).

SECTION 3:

GUIDE FOR SUPERVISORS



3.1 Understanding And Accepting Your Security Responsibilities

An important aspect of CNCS' Information Security Program (ISP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making personnel aware of their security responsibilities and teaching them correct practices can CNCS reduce the level of security risk to its information systems.

Many components of CNCS' ISP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into CNCS' program. Ensuring that you gain an understanding of your responsibilities is vital to CNCS because without your knowing the necessary security measures (and to how to use them), CNCS' information security will not be effective.

As someone who supervises CNCS information users, including employees, contractors, interns, and temporary workers, you are referred to as a "Supervisor." As such, you have specific security responsibilities. You are responsible for familiarizing yourself with and performing those responsibilities, as outlined in this Handbook.

3.1.1 What Security Responsibilities Does A Supervisor Have?

The primary information security responsibilities of a "Supervisor" fall into three areas:

- Ensuring that your employees are aware of, and trained on, their InfoSec duties.
- Assisting with ensuring that your employees comply with CNCS information security policies and procedures.
- Reviewing information security reports regarding activities of your staff and taking appropriate action.

The specific duties will be outlined later in this section.

3.1.2 Reviewing and Understanding CNCS Information Security Policies

This section of the Handbook provides information and instructions for Supervisors on fulfilling your security responsibilities

You should also take the opportunity to review the detailed Information Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have questions, please ask the CISO to provide clarification.

3.2 Maintaining Security Awareness



One of CNCS' information security program goals is to help everyone at CNCS maintain security awareness on an ongoing basis. Information Security is not a one-time event, but a continuous effort and "state of mind." This is achieved by reinforcing concerns and appropriate behaviors on a continuous basis. Effective security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

As a Supervisor, it is your responsibility to help maintain your employees' information security awareness, and to take an active part in protecting the CNCS information resources that they use. You should also serve as a good role model for your employees regarding information security awareness.

3.3 Reporting Security Incidents

For more information on Reporting Security Incidents, see ISP-05, *Incident Reporting*.

3.3.1 What Is A “Security Incident?”



3.3.2 How To Report A Security Incident

3.3.3 Incident Response



You must immediately report any suspected information security incidents so that the CNCS incident response team may respond in a timely manner to correctly handle the incident, minimize disruption of critical information services, and minimize loss or theft of *sensitive* and *mission-critical* information.

Your cooperation and participation in reporting security incidents is vital to CNCS’ maintaining the security of its information resources. It is important that all supervisors maintain vigilance regarding information security, and immediately report any suspected incidents in order to minimize potential damage to CNCS.

Additionally, as a supervisor, you may receive reports of incidents directly from your employees. You need to communicate and escalate these incident reports to the CISO.

A “security incident” is any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

Examples of security incidents include (but are not limited to):

- Suspected violations of any CNCS information security policies.
- Loss or theft of laptops, mobile devices (such as PDAs), security tokens, or other items that may provide access to CNCS information resources.
- Attempts by unauthorized individuals to gain access to CNCS information or systems.
- Accidental disclosure, modification, or destruction of information.

You must report suspected incidents to the CISO, the OIT Help Desk, or the Information Owner as quickly as possible. You may report incidents either verbally or in writing. It is recommended that you retain proof that you reported the incident.

You may be required to document relevant information about the suspected incident. You may also be requested to assist the CISO, system administrators, or Human Resources with resolution of the incident. Your full cooperation in resolving the incident is required.

As a Supervisor, you may have to play a role in the incident response process. This could include such activities as:

- Confirming incidents reported by your staff.
- Assisting your staff with providing information to the CISO for incidents that they have reported to you.
- Assisting with investigating incidents involving your staff.
- Helping to determine and implement corrective actions for your employees who have committed security violations.

3.4 Employee Security Training Program

For more information on Information Security Training, see ISP-P-02, *Security Training and Awareness*.



The Federal Information Security Management Act (FISMA) requires every Federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, Office of Management and Budget (OMB) Circular A-130 requires that such training be completed prior to the granting of access and on a periodic refresher basis.

Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of CNCS information resources. Information security policies and standards cannot be effective unless everyone at CNCS, regardless of level in the organization, is aware of the importance of security, understands CNCS security procedures, and performs required practices.

For these reasons, all employees, including individuals hired in the competitive or excepted civil service (*e.g.*, student interns), as well as personal services contractors, industrial contractors, consultants, and experts hired on contract, must fulfill CNCS' information security training program. ISP-P-02, *Security Training and Awareness*, outlines CNCS' training policy.

As a supervisor, you are responsible for:

- Providing the opportunity for your employees to attend security training and review security policies and awareness materials.
- Taking an active role in ensuring that employees complete security training and awareness activities.
- Disciplining employees that do not comply with InfoSec training requirements.
- Helping your employees to understand CNCS information security policies.
- Ensuring that your employees understand their responsibilities.
- Communicating changes in policies and/or procedures to your employees.

SECTION 4:

GUIDE FOR

INFORMATION

OWNERS



4.1 Understanding And Accepting Your Security Responsibilities

An important aspect of CNCS' Information Security Program (ISP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making personnel aware of their security responsibilities and teaching them correct practices can CNCS reduce the level of security risk to its information systems.

Many components of CNCS' ISP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into CNCS' program. Ensuring that you gain an understanding of your responsibilities is vital to CNCS because without your knowing the necessary security measures (and to how to use them), CNCS' information security will not be effective.

As someone who has official responsibility for a CNCS information resource(s), you are referred to as an "Information Owner." As such, you have specific information security responsibilities. You are responsible for familiarizing yourself with and performing those responsibilities, as outlined in this Handbook.

4.1.1 What Security Responsibilities Does An Information Owner Have?

As an information owner, you are ultimately responsible for the information resources for which you have been assigned ownership. You must exercise due diligence to protect the confidentiality, integrity, and availability of those resources. In support of this duty, you have the following general responsibilities (which are detailed in this section of the Handbook):

- You must ensure that your resources are adequately protected, commensurate with their sensitivity and criticality, and the level of risk. This includes the planning and implementation of technical, managerial and operational security controls.
- You must ensure that your resources are in compliance with all CNCS information security policies, procedures and standards, as well as federal laws.
- You may delegate administration and maintenance of the resource to an Information Custodian, but must understand that you are still ultimately responsible for that resource, and thus need to actively monitor that custodianship.
- You must create and maintain thorough documentation of your resource and the security measures employed to protect it.

4.1.2 Reviewing and Understanding CNCS Information Security Policies

This section of the Handbook provides information and instructions for Information Owners on fulfilling your security responsibilities.

You should also take the opportunity to review the detailed Information Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have any questions, please ask the CISO to provide clarification.

4.2 Categorizing Resources

For more information on resource classification, see ISP-P-07, *Security Categorization*.

All CNCS resources must be categorized based on their sensitivity and criticality so that they may be appropriately protected commensurate with their level of categorization. As the assigned owner of a CNCS information resource, you are responsible for working with the CISO to perform this categorization in accordance with NIST guidance.

CNCS information systems will be categorized as one of the following:

1. *Major Applications (MAs)* - An information system that requires special attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. An MA requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
2. *General Support Systems (GSS)* - A GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people, and provides support for a variety of users and applications.
3. *Minor Applications* - An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Based on FIPS Publication 199, each CNCS information resource will be categorized based on level of potential impact to confidentiality, integrity and availability.

Security controls will be applied to CNCS information resources in accordance with the security categorization of each system.

4.3 Assigning An Information Custodian



Although you are the official owner of an information resource, you do not have to personally manage and operate that resource. While the requirements for an information resource (and the usage of the resource) often come from CNCS business units, it is more appropriate that the actual installation, maintenance, and administration of that resource be performed by someone with specialized expertise in performing those tasks. Therefore, you can delegate that role onto another individual or group, such as OIT.

The person who is responsible for managing and maintaining the resource is called an “Information Custodian.” As the resource owner, you are responsible for making an arrangement with someone who will assume this custodian role. (At CNCS, this will generally be the OIT department.) A Service Level Agreement should be developed between the owner and custodian outlining roles, responsibilities, and expectations.

Please note that while the information custodian will assume the day-to-day responsibilities for operating and maintaining the resource, and will assist the owner with planning for and implementing security measures, it is the information owner for the resource who is ultimately responsible for the security of that resource.

4.4 Risk Management

For more information on Risk Management, see ISP-P-08, *Risk Management*.



4.5 Developing System Security Plans

For more information on System Security Plans, see ISP-P-09, *System Security Plans*.



In determining an information security strategy for a system or the organization, CNCS must determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business, while addressing financial and operational concerns.

Risk management (RM) is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel. Effective RM processes support sound *risk-based decision-making*. The CIO and other CNCS executives need to ensure implementation of an effective and comprehensive RM program which encompasses all segments of the enterprise in order to support CNCS' mission.

As an information owner, you are expected to use a risk-based approach to making decisions regarding the acquisition and protection of your information resources. Risk analysis will determine requirements that ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, CNCS information. You are responsible for performing periodic risk assessments of your resources and implementing appropriate safeguards based on these analyses. These analyses and safeguards will be documented in system security plans.

System Security Plans are critical for ensuring an appropriate level of security and risk mitigation for CNCS systems. A security plan lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures.

As an information owner, you are responsible for developing (or ensuring the development of) SSPs for each major system that you own and you must formally approve and accept these plans.

- SSPs must comply with the latest NIST guidance.
- SSPs will document the application of appropriate security controls based on the risk categorization of the system.
- SSPs will include a copy of or reference to security configuration checklists used on the system.
- Each System Security Plan must be reviewed and updated annually or when there is a major change to the system, whichever is earlier.
- SSPs must be marked, handled, and controlled as *sensitive* information.

Minor applications may be an appendix or addressed as part of the System Security Plan for the applicable general support systems or, in some cases, the applicable major application.

4.6 Certifying & Accrediting Your Systems

For more information on C&A, see ISP-P-10, *Certification and Accreditation*.



Certification and Accreditation (C&A) is used to ensure that information systems have adequate security commensurate with the level of risk. To this end, C&A is the formalized process used to assess the risks and security requirements of each system, and to determine whether the system's security needs are being met.

The Federal Information Security Management Act (FISMA) requires CNCS to perform C&A of its information systems. For each system, this process must be completed either every three years or when there is a change that affects the system's security posture.

If you are the owner of a major CNCS information system², then you are responsible for certifying and accrediting your system in accordance with the following requirements:

- You will submit your system for evaluation at least every three years or whenever there is a major change to the security of the system (whichever happens first).
 - All new IT systems will be C&A'd prior to being allowed into operation.
 - All CNCS systems contained in the CNCS System Inventory will be examined at least annually to determine if there have been a major change
 - You must notify the CISO when there is a significant change to the security of any major information system that you own.
- Certification will test and evaluate technical and non-technical IT security features and other safeguards used by the system. Certification shall not only address software and hardware security safeguards, but also procedures, physical protections, and personnel security measures. Security controls will be tested and evaluated during the Certification process to evaluate the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This will be performed in accordance with NIST guidance as specified in Special Publication 800-53A.
- Accreditation will be used for obtaining official management authorization for the operation of a system and will be in the form of a formal declaration that the system is approved to operate in a particular security mode using a prescribed set of safeguards.
 - The Accreditation determination shall be based on findings, facts, and support documents produced during the Certification process, as well as other management considerations.
 - An Accreditation statement, which affixes security responsibility with the accrediting authority (DAA), will be used to certify that proper attention has been afforded to the security of the IT resource. The statement shall address the residual risks associated with the system.
 - You will review the C&A statements before they are signed by the DAA.

² A major information system is one that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.



- The assembled C&A Package will include the following:
 - Appointment Letters for the DAA, System Owner, and ISSO
 - System Categorization in accordance with the CNCS Security Categorization policy (ISP-P-07).
 - Signed Accreditation Letter
 - Risk Assessment in accordance with the CNCS Risk Management policy.
 - System Security Plan
 - System Contingency Plan
 - Security Assessment Report
 - Interconnection Security Agreements (ISA) if necessary
 - E-Authentication Risk Assessment
 - Privacy Impact Assessment in accordance with CNCS Privacy policy
 - System Rules of Behavior
 - A System POA&M containing any residual items that need to be resolved.
 - A completed C&A document checklist with appropriate signatures.
- You will adhere to NIST Certification and Accreditation guidance.
- You will work with the CIO to determine a suitable DAA for your system.

4.7 Vulnerability Testing

For more information on vulnerability testing, see ISP-P-05, *Vulnerability Testing*



Security testing is an important means of detecting weaknesses and determining risk. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand information security attacks.

Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires CNCS to perform vulnerability testing on a periodic basis. A systematic, comprehensive, ongoing, security testing program assists CNCS with determining its information security priorities and making prudent investments to enhance the security posture of its resources.

The CISO will develop a program to perform periodic, standardized vulnerability testing of all CNCS systems. Attempts will be made to minimize disruption of business operations.

As the owner of a CNCS information system, it is your responsibility to:

- Cooperate with, and provide assistance as requested to, the CISO and other designated personnel for performing testing on your systems.
- Provide information required to perform testing
- Support and participate in development of testing “rules of engagement”.
- Resolve vulnerabilities discovered by testing, as reported in the test results.
- Document steps taken to resolve vulnerabilities and report these to the CISO.

4.8 Vulnerability Remediation

For more information on vulnerability testing, see ISP-P-06, *Vulnerability Remediation*

For more information on POA&Ms, see ISP-P-01, *Information Security Governance and Reporting*.

4.9 Contingency Planning

For more information on Contingency Planning, see ISP-P-11, *Contingency Planning*.

Vulnerabilities may be detected or reported through a variety of sources, including periodic vulnerability testing; vendor alerts; US-CERT, NIST, or other reputable organization alerts; and IG or audit findings.

As a system owner, you are responsible for ensuring that all vulnerabilities are remediated for your system within a timely manner. You will work with your System Custodian(s) to assess reported vulnerabilities to determine level of impact on CNCS systems and develop a mitigation strategy.

- Corrective actions will be documented and scheduled in accordance with Patch Management and Change Control procedures.
- Once corrective actions have been taken, they will be validated to ensure the vulnerability has been adequately mitigated.
- Completion of vulnerability resolution will be reported back to the CISO.

A Plan of Actions & Milestones (POA&M) will be maintained for each major system to track specific weaknesses or vulnerabilities resulting from Inspector General audits, reviews, or scanning activity related to such work as risk assessments, certification testing, or penetration testing. You are responsible for providing updates on your system POA&M to the CISO on at least a quarterly basis to support FISMA reporting to OMB.

You will treat information about CNCS vulnerabilities as *sensitive* information and protect the confidentiality of this information.

CNCS' information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of CNCS' risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside CNCS' control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus, effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

As an information owner, you are responsible for the development of a Contingency Plan or Disaster Recovery Plan for each major information system that you own and ensuring that appropriate personnel are trained on the plan. These plans will be based on a business impact analysis, and will identify measures to reduce the effects of system disruptions and increase system availability. Recovery strategies and procedures will be developed to ensure that systems may be recovered quickly and effectively following a disruption. Testing will occur annually or when a significant change occurs. Contingency plans will be reviewed regularly and updated as needed to remain current.

4.10 System Acquisition

The increased use of commercial products and services to collect, process, store, and transfer CNCS data presents additional risks to Corporation data. Contractors must be held accountable for meeting federal requirements and CNCS security policies. In order to do this effectively, this must be addressed early in the system acquisition process.

You must include language in all your contracts and agreements specifying that the contractor/partner must adhere to Federal Information Security Management Act (FISMA) and Privacy Act requirements. The following statement must be included in all of contracts and agreements for any systems or services which involve collecting or handling information on behalf of the Corporation:

“As a federal agency, the Corporation for National and Community Service (CNCS) is subject to and complies with the security requirements of the Federal Information Security and Management Act (FISMA). The Contractor shall ensure that services and products provided under a contract resulting from this solicitation shall comply with the Corporation’s information security program and privacy program policies, and Contractor Security Requirements available at http://www.nationalservice.gov/home/security_and_privacy_policy/index.asp.”

Security requirements and specifications must be included, either explicitly or by reference, in all contracts, and solicitations for contracts, for information systems and information services. The security requirements specified for the contract should be based on an assessment of risk for the contract and the FIPS 199 security category of the system covered by the contract. Requirements should include the following:

- required security capabilities
- required design and development processes
- required test and evaluation procedures
- required documentation

Documentation required of the contractor should include:

- Documents describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.
- Administrator and User guides with information on configuring, installing, and operating the information system; and effectively using the system’s security features.

The acquisition of commercial information technology products should be consistent with NIST Special Publication 800-23 which provides guidance on the acquisition and use of tested/evaluated information technology products.

Security and privacy requirements must be included within all of your IT investments

- Security must be integrated into and funded over the lifecycle of each system undergoing development, modernization, or enhancement.
- Steady-state system operations must meet existing security requirements before new funds are spent on system development, modernization or enhancement.
- As part of the capital planning and investment control process, you must ensure that

4.11 System Development Lifecycle (SDLC)

For more information on system development security requirements, see ISP-C-12, *System Development*.



the resources required to adequately protect the information system are provided.

- Security requirements for the information system must be included in business case planning.

Each information system passes through multiple phases during its lifetime as it is planned, developed, deployed, operated, and retired. In order to develop a secure system in a cost effective manner, security must be considered in all phases of the SDLC. Security must be treated as an integral part of any system development or implementation project, including system modifications. It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later. By considering security early in the system life cycle, CNCS will be able to avoid higher costs later on while also developing a more secure system from the start.

You are responsible not only for ensuring that the required tasks are completed during the development/acquisition cycle for the systems that you own, but you must actively participate in all phases to ensure that the system is secure and meets your requirements. This applies regardless of whether the system is developed by CNCS or purchased from/developed by a 3rd party.

- Prior to approving the development/acquisition of a system, CNCS will evaluate the risks of the project:
 - You will conduct a sensitivity assessment (information, potential damage, laws and regulations, threats, privacy, security characteristics, CNCS policy and guidance). The assessment shall consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (e.g., hazardous location) and public threats to the system or information should also be considered.
 - You will perform a preliminary Risk Assessment and incorporate the results into the decision process regarding the development/acquisition of the system.
- Security requirements shall be developed at the same time system planners define the other requirements of the system. The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.
- Application software used at CNCS must be obtained through authorized procurement channels and must comply with all licensing requirements.
- Each application must be categorized in accordance with CNCS' Security Categorization policy, and provided protection appropriate to its level of sensitivity and criticality.
- Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.
- Prior to placing the system into production, you will ensure that the following tasks

are performed:

- The system will be thoroughly documented. Documentation of *sensitive* systems must be provided the same degree of protection as that provided for the system.
- A System Security Plan (SSP) will be developed in accordance with CNCS System Security Plan policy and procedures.
- Operational practices will be developed, including standard operational procedures and system-specific security policies (e.g., account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.
- All systems will be thoroughly tested prior to being placed in the CNCS production operating environment. *Sensitive* data will not be used to test systems until system security has been reasonably assured by testing with *non-sensitive* data or files.
- The system's security features will be configured and enabled, and security management procedures will be implemented.
- The system will be authorized for processing via CNCS' Certification and Accreditation (C&A) process.
- During ongoing operation and maintenance of the system, CNCS will ensure the following tasks are completed:
 - The security activities outlined in the system security plan (e.g., performing backups, holding training classes, managing accounts) will be performed.
 - Any changes made, or maintenance performed, on the system are to comply with CNCS' Change Control and Patch Management policies and processes.
 - Annual testing of security controls will be performed.
 - The SSP will be periodically reviewed and updated in accordance with the System Security Plan policy.
 - The system will be periodically re-C&A in accordance with NIST guidance.
 - Systems must comply with CNCS information security policies and procedures (e.g., change control, patch management, access control, etc.)
- When disposing of a system, CNCS will ensure that proper measures are taken to protect the data that was stored in the system:
 - Information may be moved to another system, archived, discarded or destroyed in accordance with CNCS data retention policies.
 - Any storage media must be disposed of in accordance with CNCS' Media Management policies.
 - The disposition of software needs to comply with its license agreements.

Additionally, you will designate someone on your team to act as the system ISSO and security liaison for the system.

4.12 Application Security

Applications must identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries. The structure and content of error messages will be carefully considered as part of the design of any application. Error messages generated by the system will provide timely and useful information, without divulging potentially harmful information to unauthorized persons (i.e. information that could be used to exploit the system). Sensitive information (e.g., account numbers, SSNs, passwords, etc.) will not be shown in any error messages or error logs.

Applications must prevent unauthorized and unintended information transfer via shared resources by controlling object reuse (information remnance). No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

User interface services (e.g., web services) shall be physically or logically partitioned from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

4.13 System Reports

Any report containing sensitive data must be marked with an appropriate header or footer, such as "Sensitive Information – For Official Use Only"

4.14 External Systems

For more information on perimeter protection, see ISP-S-12, *External System*.

FISMA and OMB guidance requires agencies to ensure the security of all external systems that contain CNCS information, or which operate, use, or have access to federal information on behalf of CNCS. These systems must meet federal security requirements. This includes contractor systems and systems operated by other agencies that provide services to CNCS (such as NFC payroll system). However, it does not apply to systems or services that do not contain federal information or do not operate on behalf of CNCS.

A CNCS employee will be assigned as the CNCS Information Owner for each external system used by or for the Corporation. The owner of an external system is responsible for coordinating with the external system operator to ensure compliance with the following:

- You will sign a Memorandum of Understanding (MOU) with the operator of each external system and provide a copy of the MOU to the CNCS CISO. The MOU will require the external party to secure the system in compliance with federal requirements, including:
 - Development and maintenance of a System Security Plan in compliance with NIST guidelines
 - Completion of a Certification & Accreditation or a SAS70.
 - Having a viable contingency plan that is tested annually

- Performing a Privacy Impact Assessment
- Background screening of personnel who will have access to the system
- Notification of the CNCS information owner and/or Chief Information Security Officer (CISO) of any security incidents involving the system.
- You will provide system inventory information on the system to the CNCS CISO.
- Contact info for relevant contacts will be provided in the MOU.
- MOUs will be reviewed by the CISO prior to CNCS sign off.

If you own a CNCS system that interfaces with an external system, you will develop an Interconnection Security Agreement (ISA) between your system and the external system.

4.15 Security Training & Awareness

For more information on security training, see ISP-P-02, *Security Training and Awareness*.

As the owner of an information resource, it is your responsibility to ensure that users of your system are trained on and aware of the specific security policies and procedures that apply to your system. These policies and procedures should be documented and published for your users, and training provided if necessary.

Additionally, you will be required to complete special Information Owner security training as prescribed by the CISO.

4.16 Incident Reporting

For more information on incident reporting, see ISP-P-03, *Incident Reporting*.

You must immediately report any suspected information security incidents so that CNCS may respond in a timely manner to minimize disruption of critical information services and minimize loss or theft of *sensitive* and mission-critical information.

As an information owner, you may receive reports from users or the information custodian regarding security incidents involving your resources. You may also personally discover such incidents. In either case, you are obligated to report these incidents to the CISO using CNCS' incident reporting process.

4.17 Incident Response

For more information on incident response, see ISP-P-04, *Incident Response*.

CNCS must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

The Federal Information Security Management Act (FISMA), and OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems* require all organizations to have an incident response capability and to share information concerning common vulnerabilities and threats.

As an information owner, it is your responsibility to cooperate and support CNCS' incident response procedures. Such cooperation will make it possible for CNCS to respond quickly and effectively to situations that might compromise the agency's information resources.



4.18 Authorizing Access Permissions

For more information, see
ISP-C-01, *Access Control* and
CNCS ISP-C-06, *Personnel
Security*.

For information on
background investigations,
contact the CNCS Personnel
Security Officer.

4.19 Identifying and Authenticating Users

For More Information, see
ISP-C-02, *Identification and
Authentication*.

Specifically, your responsibilities include:

- Ensuring that incident response procedures are in place for your systems
- Immediately reporting incidents to the CISO
- Cooperating with, and providing assistance as requested to personnel investigating an incident.
- Implementing additional measures, as needed, to prevent further incidents.
- Providing follow up to ensure that incidents have been resolved.

Excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability. Therefore, access to CNCS information resources is limited to those who need those resources to perform their duties. Access to specific resources is only to be granted to authorized personnel who have a legitimate need to use them, and will be limited to those privileges required for their duties.

You are responsible for determining who will have access to your resource, and the level of access granted. In making this determination, you are to adhere to the following policies:

- Ensure that your resources are protected against unauthorized access by implementing appropriate access control measures.
- Access is only to be granted to personnel who have a legitimate business need.
- Grant users only the minimum access permissions required for their duties.
- Users must have appropriate clearance for the sensitivity level of the resources to which they are given access. Prior to granting someone access to *sensitive* information resources, you must verify that they have undergone the appropriate background investigation and that it has resulted in a suitable outcome.
- Use a documented process for granting, modifying, and revoking permissions.
- Before granting contractors or other non-CNCS personnel access to any *sensitive* data, you must make sure that they have signed a nondisclosure agreement.
- Periodically review access permissions and make adjustments as appropriate.

In order to ensure that unauthorized persons do not have access to *sensitive* CNCS resources, it is necessary to first establish the identity of the user who is attempting access. Access controls can then be used to control access based on the established user identity.

The specific method(s) of authentication used for each system must be appropriate to the sensitivity of the system. Multiple authentication methods (*e.g.*, use of both a password and a token) may be required for high-sensitivity resources or high-risk situations.

You must ensure that access to your system is protected by ensuring that authentication credentials are selected, assigned, stored, and administered appropriately..

4.19.1

What are the policies regarding account management?



You must ensure that credentials are appropriately assigned, used, and managed on the resources that you own, and that authentication policies are enforced. When feasible, automated techniques should be used for enforcement.

Detailed procedures must be documented for the creation, removal, and modification of user accounts and authentication credentials for each system. These procedures will also address automatic termination of temporary and emergency accounts; disabling of inactive accounts; automated mechanism(s) to audit account creations, modification, disabling, and termination actions;

User accounts must adhere to the following guidelines:

- Allow only one user per account; User IDs are never to be shared.
- Never install a guest account. Remove any guest accounts that are created by default unless absolutely required and approved by the system owner and the CISO.
- No accounts will be named with easily guessed generic names (such as “anonymous”, “guest”, “admin”, “ftp”, “telnet”, “www”, “host”, “user”, “test”, “bin”, “nobody”, etc.) unless absolutely technically required by the system.
- Default accounts that are present upon initial installation of the system should be removed or renamed unless technically required by the system to keep the name.
- Accounts should be deactivated immediately upon termination of user.
- Unused accounts will be deactivated on at least a monthly basis.
- Accounts for contractors and other temporary staff will be configured to expire on the final date of their contract/employment.

Administrator accounts must adhere to the following guidelines:

- The names of the administrator accounts should be renamed, if possible, to make it more difficult for attackers to guess the names of these accounts.
- Each person who has a legitimate need to use Administrator privileges should have their own administrative account that they will use to perform administrative functions. Usage of the main administrator account for each system should be limited to emergencies, and is to be limited to specific designated OIT staff. This will protect the main administrator account and also provide an audit trail of administrative activities.
- All accounts with administrator privileges must have strong passwords or other alternative strong authentication methods.

Account credential information (e.g., User IDs, passwords) that are stored on devices (such as enable passwords in router configuration files) must be encrypted.

To preclude brute force attacks, an intruder lockout feature must be implemented on each system to temporarily suspend the account after several invalid logon attempts.

4.19.2

What are the policies regarding password management?

For More Information, see ISP-C-03, *Password Management*.



4.19.3

What are the policies regarding managing access tokens?

For More Information, see ISP-C-04, *Access Tokens*

If passwords are used for authentication, it is critical that they be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

In systems that use passwords as their authentication method, every account (including newly issued accounts) will have a password.

If SNMP is used, the community strings should follow the same rules as passwords.

Passwords must be changed:

- Immediately upon initial user logon.
- At least every 90 days (systems may set a shorter expiration period for their users) except for external users who meet the requirements specified in ISP-C03.
- If it is suspected that the password has been compromised.
- For admin accounts, immediately upon the departure of personnel with access.

The following guidelines apply to password storage and visibility:

- Passwords will not be visible on a screen, hardcopy or other output device.
- Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.
- Passwords will not be sent via unsecured email.
- Passwords will not be stored in written form (*e.g.* sticky notes).

The assignment of passwords for specific CNCS systems should adhere to the following:

- Each system should have its own password selection standard that adheres to the password guidelines while being commensurate with the level of security required by the level of sensitivity of the system.
- The system will be configured to enforce the password selection criteria specified in the system criteria.
- Passwords must be at least 8 characters and contain a combination of letters, numbers, and special characters.
- Passwords cannot be reused for at least 24 changes.
- Never set any password equal to the null string (*i.e.*, a blank password), which is equivalent to no password at all.

Tokens will be used only in conjunction with another authentication factor, such as a password or PIN.

You must implement defined procedures for distributing, tracking, and reclaiming access tokens which comply with the following:

- Tokens will only be given to personnel upon verification of their identity to ensure that tokens are not given to unauthorized persons.



4.20 Maintaining Audit Trails

For more information on audit trails, see ISP-C-05, *Audit Trails*.



- The custodian will maintain an inventory of tokens and their assignments.
- If tokens are lost, stolen, or not returned upon staff termination, they will be immediately disabled.

Systems will require that the token PIN be changed upon first use and on a periodic basis.

An audit trail of token usage will be enabled and periodically reviewed.

Tokens will be issued only for exclusive use by a single individual. Users may not share their tokens or allow anyone else to use them or the access they provide.

In order to enforce policies and to be able to investigate security incidents, automated logs of access to and alteration of systems and data must be maintained. A record of activity (or “audit trail”) of system and application processes and user activity of systems and applications must be maintained. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and system flaws.

As an Information Owner, you must ensure that your systems comply with audit trail policy:

- For each server, you must enable and maintain logs for the following transactions (where possible given the constraints of the logging capabilities of the operating system and application software):
 - Server startup and shutdown
 - Manual loading and unloading of services
 - Installation and removal of software
 - User logon and logoff
 - System administration activities
- For each major application, enable and maintain logs for the following transactions:
 - Modifications to the application
 - User sign on and sign off
 - System administration activities
- For each for each router, firewall, or other major network device that you manage, you must enable and maintain logs for the following transactions (where possible given the constraints of the logging capabilities of the device):
 - Device startup and shutdown
 - Administrator logon and logoff
 - Configuration changes
 - Account creation, modification, or deletion
 - Modifications of privileges and access controls
- For each logged transaction, you must record the type of event, date, time, and the

4.21 Backup & Recovery

For more information on media management, see ISP-C-08, *Backup and Recovery*.



name of the account performing the transaction.

- Do not store *sensitive* information, such as passwords and system data, in the logs.
- Cooperate with and provide assistance (as requested) to the CISO and other designated personnel, who will perform periodic audits of the log files to look for potential security issues or to research an incident.
- Control access to the audit logs to prevent tampering.
- Keep all audit trail files for at least one year and store them in a secure location.
- Develop documented procedures for audit trail monitoring.

There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include such events as hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. These threats are very common and it is inevitable that some of these events will occasionally occur at CNCS.

It is therefore essential that CNCS maintain backup copies of all critical data and systems so that they can be used to ensure the continued availability and viability of these resources when these unfortunate events occur. The action of copying (or mirroring) important data to a second location or onto removable media is calling “backing up.”

As the owner of a CNCS resource, it is your responsibility to make sure that your resource is successfully backed up in accordance with CNCS policies. This means working with your Information Custodian to ensure that the following requirements are met:

- You must back up all critical CNCS information resources that you own.
- Critical data and system configurations must be backed up on at least a daily basis.
- Applications and licenses will be backed up whenever there are changes to them.
- You should back up critical information daily and store these backups off-site in a secure, environmentally-controlled location. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.
- You will define and implement a backup retention schedule for your resources which complies with CNCS’ data retention policies.
- You will develop and implement detailed procedures for performing backups restoring data, testing backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.
- You will periodically (at least annually) test your back up and restore procedures to ensure that data can be effectively restored from the backups.
- You will be treat backups with the same level of criticality and sensitivity as the data and applications stored on them.
- Persons who have access to the backups, or who have access to perform backup or restore functions, must undergo appropriate background screening in accordance with CNCS Personnel Security policy prior to being given such access.
- You will handle backup tapes in accordance with CNCS Media Management policy.

4.22 Media Management

For more information on media management, see ISP-C-11, *Media Management*.



CNCS has been entrusted with a variety of *sensitive* data in order to accomplish its mission. This data, which is stored on a variety of media (*e.g.*, hard drives, CDs, tapes), must be protected from unauthorized disclosure, damage, and abuse. To protect the information, CNCS uses a variety of security mechanisms that provide protections for media.

As an Information Owner, you are responsible for the proper handling and disposal of your media in accordance with CNCS policies and procedures. This includes:

- Provide appropriate physical and environmental protections for stored media.
- Mark any media containing *sensitive* data with its classification level. Labeling shall include any special handling instructions.
- Media containing *sensitive* data must be secured (*e.g.*, in locked drawer, cabinet or safe) when not in use or unattended. Media containing *sensitive* data transported through the mail or by courier service shall be double-sealed. The second envelope shall be appropriately marked with the sensitivity classification of the data.
- Monitor the receipt and delivery of media containing *sensitive* data, and account for media to ensure that data is not lost and potentially compromised while in transit.
- Sanitize (*i.e.*, securely delete) media that contain *sensitive* data before disposal, in accordance with CNCS media sanitization procedures.
- Report the loss, damage, or theft of any media entrusted to you.

4.23 Asset Management

For more information on asset management, see ISP-C-10, *Asset Management*.



Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the unwanted attention of auditing organizations like GAO and OMB.

Not only would loss of information assets result in a financial impact on CNCS, but it could also result in unauthorized access to data stored on, or accessed by, these assets, and could have a detrimental effect on the image and reputation of the agency. Additionally, several federal laws and regulations, such as the Clinger-Cohen Act, mandate the tracking and management of information assets.

As an information owner, you are responsible for inventorying, tracking, and protecting the assets that you own. This includes ensuring that the following tasks are performed:

- Keep a record of all assets that you own, including, but not limited to, workstations, servers, network devices, printers, PDAs, phones, software, and licenses.
- You are to record and barcode your information assets upon receipt at CNCS.
- For each information asset, you must track the following information:
 - The brand, model, and type of asset
 - Serial number and CNCS asset tag number
 - The location and person to whom the asset is assigned
- You are required to perform periodic inventories to verify your records and account for all information assets. Each asset is to be inventoried at least annually.

4.24 Managing Changes

For more information on change management, see ISP-C-13, *Change Control*.



Changes to CNCS' information systems must be controlled and managed to ensure integrity of the system and its data. Change control prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure, and other problems.

As an Information Owner, you are responsible for ensuring that changes made to your resources are documented and implemented in compliance with CNCS policy:

- Changes will be systematically planned, approved, tested and documented at a level appropriate with the size, complexity, and sensitivity of the system.
- Changes will be reviewed and approved by the Change Control Board (CCB) or Investment Review Board (IRB) and Technical Review Board (TRB) as specified in the CNCS Configuration Management Plan.
- CNCS will develop baseline information that includes a current list of all components (hardware, software, and their documentation), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths, and switch settings of machine components.
- For each of your systems, CNCS will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change, and any observations made during the course of the change.
- Procedures will be implemented to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:
 - Establish who performs maintenance and repair activities.
 - Contain procedures for performance of emergency repair and maintenance.
 - Contain the management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.
- Impact analyses will be conducted to determine the effect of proposed changes on existing systems and security controls.
- Standardized procedures will be implemented for thoroughly testing and approving system components (operating system, other system, utility, applications) and configuration changes prior to transition from development to production.
- Information Users will be notified regarding how they will be impacted by changes.
- Current backups will be available when changes are made.
- All software, operating systems, and patches shall be installed in accordance with U.S. copyright regulations, the license for that software, and CNCS policies.
- Only authorized personnel may make changes to CNCS information systems.
- Change control procedures will be documented for all systems to provide a complete audit trail of decisions and design modifications.
- Change control documentation (especially change logs) will be available even if the network is down and will not contain passwords for affected components.

4.25 Patch Management

For More Information, see
ISP-C-09, *Patch
Management & System
Maintenance*.



Maintained patch levels are critical to the security of CNCS systems. Vendors will typically provide OS patches and fixes for security problems, which can be loaded separately from the application. These should be loaded on a regular basis using a coordinated process.

As the owner of any CNCS information resource, it is your responsibility to make sure that timely maintenance is performed on information systems that you own, including deployment of patches to proactively prevent the exploitation of vulnerabilities. Specifically, you must adhere to the following requirements:

- Define detailed patch management procedures for each system you manage
- Monitor sources for available patches on a continuous basis. During regular operation, available patches will be reviewed monthly and applied if appropriate. In an emergency, more urgent application of new security patches may be required.
- Patches will be checked for compatibility with all system components prior to being applied.
 - Patches will be successfully tested on non-production systems prior to being loaded on production systems.
 - The use of standardized configuration baselines will simplify testing and reduce the risk of patching-induced problems.
 - The risk and impact of deploying each patch should be assessed prior to implementation of that patch.
 - If a decision is made not to deploy a patch (e.g., due to risk or compatibility issues), that decision and the reason for the decision must be documented.
- All patching will be performed in accordance with CNCS Change Control policy and procedures.
- In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the correct patch levels before data is reloaded.
- New systems must be fully patched before being placed onto the production network.
- The use of automated tools to expedite the distribution of patches is encouraged. However, measures must be taken to reduce the risk of these tools being used by an attacker to distribute malicious code.

4.26 Physical & Environmental Security

Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.

As the owner of an information resource, you must ensure that your resource is located in an area which meets the following standards:

For more information on physical security, see ISP-C-07, *Physical and Environmental Security*.



4.27 Protecting Databases

For more information on database security, see ISP-S-06, *Database Security*

- Physical access is to be controlled according to the sensitivity of the resource.
- Areas containing *sensitive* resources require special restrictions to limit access:
 - Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.
 - Personnel without an appropriate security clearance must be escorted.
 - Areas containing *sensitive* information must be physically secured in accordance with CNCS facility security policies and CNCS Directive 94-14.
- Areas containing critical information resources require special protections to safeguard the availability of these resources:
 - Protection must be implemented against fire, flood, humidity, electromagnetic disturbance, and other environmental factors that could damage the resources.
- Automated systems should monitor for environmental problems and alert specified personnel as appropriate.
- Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. Keep backups in a separate location from originals.

If you are the owner of a Data Center, you must comply with the following requirements:

- Meet all requirements listed above.
- Provide emergency power shutdown controls.
- Provide an uninterruptible power supply.
- Escort vendors and visitors at all times.
- Track all physical access to the room.
- Perform annual testing on fire, utility, and environmental alarms and systems.
- Make sure that access permissions to the Data Center have been authorized and logged.

CNCS has been entrusted with a variety of *sensitive* data to accomplish its goals. The success of agency programs depends on the availability, integrity and confidentiality of this data. To protect this information, CNCS must implement data security measures, such as validation and verification controls. These controls are used to prevent accidental or malicious data alteration or destruction, and to assure that data meets quality expectations.

As an Information Owner, you are responsible for:

- Ensuring the confidentiality, integrity, and availability of the data that you own.
- Authorizing and limiting access to the data that you own.
- Reporting data security incidents to the CISO.



Additionally, you must ensure that data repositories comply with the following:

- Data will be secured commensurate with its level of sensitivity and criticality.
- Databases, and applications that interface with databases, will be configured in accordance with security best practices:
 - Integrity verification tools, such as consistency and reasonableness checks, will be used to look for evidence of data tampering, errors and omissions.
 - Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure that software and data have not been modified.
 - If users are allowed to make updates to a database via a web page, these updates must be validated to ensure that they are warranted and safe.
 - Table access controls will be applied to databases containing *sensitive* data. Access to specific data within the database will be limited to only those personnel who need access, and will be limited to only those functions (*e.g.*, read, modify) required for the person to perform his or her duties.
 - Database servers must only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).
 - For *sensitive* data, audit trails must be created and maintained within the database to track transactions and provide accountability.
 - Selectively encrypting data within the database in order to protect *sensitive* information is highly encouraged.
- Programs or utilities that may be used to maintain and/or modify *sensitive* databases or software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully tested, selected, and controlled.
- Never put databases containing non-public information on the same physical machine as a public web server.
- Data repositories (and database servers) that store public information cannot be used to also store non-public (*e.g.*, private, proprietary, *sensitive*) information.
- Database servers and database software must adhere to all CNCS information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

4.28 Using Encryption

For more information on the encryption, see ISP-C-15, *Encryption*.

Encryption is an important tool that can be used to protect the confidentiality and integrity of information. It is CNCS' policy that proven, government-approved encryption technologies be used to protect *sensitive* information which is transferred or stored outside of the CNCS computing environment (*i.e.* on traveling laptops or for transmission over the Internet). This use must adhere to the following policies:

- The use of encryption to protect *sensitive* data, both in storage and in transmission, is encouraged.
- Only government-approved encryption techniques and devices may be used.



4.29 Remote Access

For more information on remote access, see ISP-S-08, *Remote Access*



- All encryption products must be Federal Information Processing Standard (FIPS) 140-2 or 197 certified.
- Digital certificates used or issued by CNCS will comply with the Federal Public Key Infrastructure.
- CNCS will obey all regulations regarding restrictions on export of encryption technologies.
- You will have documented and implemented procedures for managing encryption keys, in order to ensure that these keys are protected from unauthorized disclosure, destruction, or misuse.
- Any encryption solution used must have a process for the CISO to perform administrative recovery of lost keys.
- Any use of digital certificates to provide non-repudiation must be approved by the CISO, CIO, or Deputy CIO.

Remote access to CNCS provides many benefits. It allows personnel traveling on business to connect to CNCS information resources and provides the capability for telecommuting. However, remote access to CNCS via dial-up or other connectivity poses a risk of intrusion into CNCS by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of CNCS also lacks the protections afforded by CNCS' corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.

As the owner of a CNCS remote access system (other than those systems intended for public access), you are responsible for ensuring that the following requirements are met for your resource:

- Any remote access into the CNCS computing environment must be approved by the CIO.
- All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).
- All *sensitive* data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.
- Session time-outs will be used to disconnect idle sessions after an inactivity period.
- All security policies used in the CNCS office must also be observed when using or connecting to CNCS resources while outside the CNCS office environment.
- Authorizing personnel to perform remote access and determining what system applications and functions may be accessed remotely.

4.30 Server Security

For more information on servers, see ISP-S-01, *Server Security*.



It takes only one incorrectly configured system to allow an intruder into CNCS' network. Therefore, no server should ever be placed on the production network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.

If you are the Owner of any CNCS server, then you are responsible for complying with the following server security requirements:

- Standard base security configurations will be developed for and applied to each type of server.
- The level of security applied to each server will be commensurate with the level of criticality and sensitivity of the data and services that it provides.
- Where possible, security configurations will be enforced through automated policies (such as Windows Group Policies).
- Server images will be scanned to ensure they have been securely configured before they are placed into production.
- System patches and security updates must be applied in a timely fashion in accordance with the CNCS Patch Management policy.
- Any unnecessary services will be disabled (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).
- Access to all CNCS servers must adhere to the CNCS Access Control and Identification and Authentication policies.
- Auditing and logging must be enabled in accordance with CNCS auditing policies and procedures.
- All servers must run approved antivirus software configured in accordance with CNCS antivirus policies and procedures.
- Each server must be inventoried and tracked in accordance with CNCS asset management policies and procedures.
- Each server's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a server must be performed in accordance with CNCS change management policies and procedures.
- Servers will be located in access-controlled and environmentally protected facilities, in accordance with CNCS physical and environmental security policies and procedures.

4.31 Network Security

For more information on network security, see ISP-S-02, *Network Security*.



It takes only one incorrectly configured system to allow an intruder into CNCS' network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.

If you are the owner of a network device or a system containing network devices, then you are responsible for adhering to the following requirements:

- Standard baseline security configurations will be developed for each type of network component (*i.e.* routers, switches, etc.) and applied to all such components.
- The level of security applied to each network component should be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.
- Patches and security updates must be applied in a timely fashion in accordance with CNCS patch management procedures.
- Any unnecessary services will be disabled.
- Access to all CNCS network devices must adhere to the CNCS Access Control and Identification and Authentication policies.
- Remote administration of network devices can only be performed using encrypted and authenticated connections.
- Logging must be enabled in accordance with CNCS auditing policies and procedures.
- Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network or device.
- Each device must be inventoried and tracked in accordance with CNCS asset management policies and procedures.
- Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a device must be performed in accordance with CNCS change management policies and procedures.
- Physical access to Network devices will be controlled in accordance with CNCS physical and environmental security policies.
- Domain Name Service
 - CNCS will comply with federal DNSSEC requirements, including SP800-81.
 - Name/address resolution systems will provide data origin and integrity information along with the authoritative information they return.
 - Systems providing name/address resolution service for the organization will be fault tolerant and will implement role (e.g., internal vs. external) separation.

4.32 Electronic Mail

For more information on electronic mail security, see ISP-S-10, *Electronic Mail*.



Electronic mail is an essential tool used by CNCS to conduct its business. However, email is inherently insecure and presents many risks to CNCS information security. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to CNCS resources. Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.

If you are the owner of a resource (including a device or application) that provides or uses electronic mail services, you must abide by the following rules:

- All electronic mail services provided on CNCS must be approved by the CIO. This includes the use of SMTP or other protocols or services by an application/system.
- All incoming electronic mail must be scanned and filtered for viruses, disallowed content (including certain types of attachments), and other malicious content.
- *Sensitive* information may not be sent over any public network (e.g., the Internet) unless it is encrypted.
- Electronic mail systems must adhere to and support CNCS record retention policies. This includes periodic archival and deletion of messages.

4.33 Mobile Devices

For more information on mobile device security, see ISP-S-07, *Mobile Computing*.



The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow CNCS personnel to be more productive. However, the use of these devices outside of the CNCS office poses risks to those devices and the information they contain. These devices may also present a hazard to other CNCS resources upon their return to the CNCS office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of CNCS which lack the protections afforded by CNCS' corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.

Owners of mobile devices are responsible for complying with the following requirements:

- Laptops and other mobile computing devices must be inventoried and tracked.
- Any mobile device (e.g., a laptop or PDA) which stores or transmits *sensitive* data, or which can be used to connect to other *sensitive* CNCS systems, should require users to authenticate (i.e., logon) in order to gain access.
- All data on mobile computers/devices which carry agency data must be encrypted unless the data is determined to be non-sensitive, in writing, by the CEO or an individual he/she may designate in writing.
- Mobile devices must abide by ISP-S-08 Remote Access when connecting to CNCS systems from outside CNCS' offices.
- The loss, theft, or destruction of any mobile device must be immediately reported.

4.34 Wireless Security

For more information on wireless, see ISP-S-03, *Wireless Security*.



In addition to the risks that apply to all networks, wireless connectivity has additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tied up network bandwidth and denied service to authorized users. Additionally, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to CNCS networks via the hijacked device. Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

As the owner of any wireless resource, you have the following InfoSec responsibilities:

- The use of any wireless connectivity or device for accessing or transmitting CNCS information must be approved by the CIO, regardless of whether these devices are owned by CNCS.
- You must use CNCS Risk Management procedures to ensure that risks have been analyzed and appropriately mitigated prior to, and during, use of any wireless technology resources that you own.
- All CNCS wireless devices must be labeled and inventoried.
- Access to CNCS and other systems and networks must be immediately terminated for any lost or stolen devices.
- Access to any CNCS systems or networks using wireless devices or wireless networks must be authenticated.
- Security risks and controls should be evaluated more frequently for wireless technologies than for other networks and systems.
- Ongoing, randomly timed security audits should be used to monitor and track wireless and handheld devices.
- Patches and security enhancements must be applied to wireless networks in accordance with CNCS system security policy.
- Robust cryptography (at least 128bit) must be used whenever *sensitive* data is stored or transmitted on a wireless device.
- The SSID for each device should be configured such that it does not reveal any identifying information about CNCS.
- Inherent security features such as authentication and encryption methods that are available in wireless technologies should be tested and used.
- You must communicate the specific policies and procedures for securely using your wireless resources to the users of those resources.

4.35 Perimeter Protection

4.35.1 What Must CNCS Do To Protect The Agency's Computing Perimeter?

For more information on perimeter protection, see ISP-C-16, *Perimeter Protection*.

4.35.2 What Are The Responsibilities Of Someone Who Owns A Resource That Resides Or Provides Services At The Perimeter?



Any connectivity to systems or networks outside of CNCS provides an opening for unauthorized personnel to access or tamper with CNCS information resources. Such threats range from intruders breaking into CNCS' network to steal or alter data to service disruptions propagated from other systems. CNCS must implement firewalls and other precautions to prevent, detect, and resolve incidents arising from these threats.

There are certain security protections that must be implemented at the enterprise level to protect CNCS' information resources. If you are the information owner for CNCS' general enterprise computing environment (*i.e.*, CNCS network), then you are responsible for implementing and managing appropriate perimeter protections as prescribed by CNCS ISP-C-16, *Perimeter Protection*. These requirements include, but are not limited to:

- Use of firewall and intrusion detection systems configured to security best practices.
- Creation of a DMZ for placement of web-facing systems and services to protect the internal CNCS network.
- Use of a proxy server for all outbound connections to the Internet.
- Formalization of Network Trust Relationships between CNCS and external networks (such as those of other agencies) to which CNCS is connected.

If you are the owner of any resource that resides on, or provides services at, the perimeter of the CNCS network (*e.g.*, Internet web servers), you are responsible for ensuring that your resources comply with the following requirements:

- These systems must be placed in a protected DMZ.
- No *sensitive* data is to be stored on systems located in the DMZ. All *sensitive* data must be located within the internal network. Waivers may be granted as needed.
- Access from the Internet to these systems must not make *sensitive* information or information systems vulnerable to compromise (*i.e.*, these systems cannot be used to compromise other internal systems).
- All perimeter equipment must be documented in accordance with CNCS information system documentation procedures.
- All hardware and software deployed on the perimeter must adhere to CNCS system security policies and procedures, including the disabling of all unnecessary services.
- Any changes to existing equipment or deployment of new equipment on the perimeter must adhere to CNCS change control procedures.
- Security events on perimeter equipment, as well as access to CNCS via this equipment, must be logged and audited.
- The responsibility for the security of any equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures must be documented. COTRs are responsible for third party compliance with this policy.

4.35.3

What Are The Requirements For Connectivity To Other Networks Or External Systems (Such As At Other Agencies)?

If your system needs connectivity to another system or external network (other than the Internet), then the connection must comply with the following criteria:

- All connections between CNCS and external networks (such as those of other agencies) must be approved by the CIO.
- Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures.
- An Interconnection Security Agreement (ISA) will be developed and signed by CNCS and the external system owner specifying security responsibilities and protections that will govern the connection between the networks.
- All connections to external networks will pass through CNCS approved firewalls.
- Information Owners will validate the need for all such connections annually.

4.36

Emerging Technologies

For more information on perimeter protection, see ISP-S-13, *Emerging Technology*



Prior to implementing any emerging technology into the CNCS production information technology environment, a risk analysis will be performed to ensure that the technology does not introduce undue risk to the Corporation's information and systems.

In conjunction with the CISO, you will assess the technology to determine:

- Whether any other federal government entity is using it, and if so, with what level of success, and what security issues they have encountered
- Whether the technology is really ready for production use. For example, if new bugs, vulnerabilities, and patching are being introduced at a fast rate, adoption of the technology should be delayed
- Whether there is sufficient benefit to the use of this technology over more established technologies to warrant the additional risks.
- Whether CNCS can acceptably manage and mitigate the risks to its information and operations due to the proposed technology.

The proposed technology will first be tested and evaluated in a non-production environment before being recommended for production use.

Use of the technology will be documented and evaluated as part of the CNCS system development lifecycle procedures, including:

- Development/Update of a System Security Plan
- Development/Update of a system Risk Assessment
- Completion of Certification and Accreditation

You will stay abreast of vulnerabilities reported for the new technology and take steps to address them in a timely fashion, in accordance with the CNCS Vulnerability Remediation and Patch Management policies.

4.37 Telephone Security

For more information on telephony, see ISP-S-09, *Telephony Security*.



Telephone services are intended to support the objectives and operations of CNCS, and are critical to fulfilling CNCS' mission. However, these telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.

As an owner of a telephony resource, or of a system that uses telephony resources, you are responsible for deploying, managing, and protecting the telephony resources in compliance with CNCS information security policies, including the following:

The agency VoIP and other critical telephony components must be protected:

- This equipment should be stored in a secure, environmentally controlled location in accordance with CNCS physical security policy.
- Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, etc.
- Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk, and criticality/sensitivity of those resources.

Modems or other telephony equipment and may not be installed without the explicit approval of the Deputy CIO.

Analog Phone Lines - As a rule, the following applies to requests for fax and analog lines. Waivers to the policy will be granted on a case-by-case basis.

- Fax machines must be placed in centralized administrative areas designated for departmental use, and away from other computer equipment.
- The fax line is used solely for the fax machine that it has been assigned to.
- When not in use, analog lines are to be physically disconnected from the computer.

Computer-to-Analog Line Connections

- Requests for computers or other intelligent devices to be connected with analog lines from within CNCS will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the agency. Waivers to the policy will be granted on a case-by-case basis. See ISP-S-09 for details.
- Lines must be terminated as soon as they are no longer in use.
- Computers cannot be connected to both an analog line and CNCS network.

Voice over IP (VoIP)

- When feasible Voice and Data should be logically separated onto different subnets.
- A mechanism to allow VOIP traffic through firewalls is required.
- Use IPSec or Secure Shell (SSH) for remote management access.
- Physical controls are especially important in a VOIP environment and should be deployed accordingly.
- Additional power backup systems may be required to ensure continued operation during power outages.



4.38 Networked Copiers

- The security features that are included in VOIP systems are to be enabled, used, and routinely tested.
- The use of “softphone” systems, which implement VOIP using an ordinary PC with a headset and special software, should be tightly limited.
- If mobile units are to be integrated with the VOIP system, use products with WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

"The networked copier that all companies have in the hallway or backroom is no longer the 'old school' device most IT managers still assume it to be. On the contrary, it's quickly evolved into a sophisticated computing platform that can grant access into the heart of the network. Copiers have been reborn as document distribution centers, enabling users to scan paper and send images via email or to, for example, document management, financial, or human resources systems. Integration with business applications allows for efficient distribution, editing, and storage of what was traditionally paper-based information. However, most networked copiers have not been secured in the same rigorous way as other end points, such as mobile devices and office workstations. In many companies, network-attached copiers could be used to distribute unauthorized documents or even distribute documents using identities that impersonate company executives."

"The most common threats to digital copiers and printers stem from intruders stealing the hard drives containing confidential data, or reprinting documents directly from the machine after the earlier print command was canceled... Today's multifunctional copiers and printers store documents in memory... They might not just retain the last job, but the last 20 to 30."

When selecting new copiers, the risks and vulnerabilities inherent in each model should be considered as part of the selection criteria. Things to look for include:

- Resistant to viruses and Denial of Service attacks
- Less vulnerable operating systems.
- SSL and other encryption options.
- Ability to automatically securely delete documents from memory
- Robust access control features.
- Build in firewall capabilities
- Common Criteria certification
- Consider buying any additional security kit offered by the vendor.

Make sure your copiers are configured in accordance with the policies described in section 5.36.

CNCS security and privacy policies apply to copiers as they would to any other system/device on the network.

SECTION 5:

GUIDE FOR INFORMATION CUSTODIANS



5.1 Understanding and Accepting Your Security Responsibilities

An important aspect of CNCS' Information Security Program (ISP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making personnel aware of their security responsibilities and teaching them correct practices can CNCS reduce the level of security risk to its information systems.

Many components of CNCS' ISP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into CNCS' program. Ensuring that you gain an understanding of your responsibilities is vital to CNCS because without your knowing the necessary security measures (and to how to use them), CNCS' information security will not be effective.

As someone who has been assigned duties related to the development, implementation, maintenance, or administration of a CNCS information resource, you are an "Information Custodian." As such, you have specific information security responsibilities. You are responsible for familiarizing yourself with and performing these responsibilities as outlined in this Handbook.

5.1.1 Signing The Elevated Privileges/ Information Custodian Agreement

For more information on the Information Custodian Agreement, see ISP-P-13, *Acceptable Use of Information Resources*.

In order to perform their duties, information custodians are usually assigned additional access privileges on the resources for which they have been assigned custodianship. These privileges come with additional responsibilities for safeguarding your access credentials and using them appropriately. Misuse of your elevated privileges, or failure to protect them from disclosure, can seriously impact the security of CNCS information resources.

In order to be granted administrative privileges, you must sign an agreement acknowledging that you understand the additional responsibilities and agree to use the privileges only for the purposes for which they have been granted. A signed copy of the agreement (see ISP-P-13 in the appendices) must be provided to the CISO.

5.1.2 What Security Responsibilities Does An Information Custodian Have?

As an information custodian, you have direct impact on the security of CNCS resources because you are the one who implements and operates the security controls that have been prescribed for the resources that you manage. Your responsibilities include the following duties, which are described later in this section:

- Assisting the information owner with planning safeguards to protect the resource and to ensure compliance with all CNCS information security policies.
- Implementing and operating the safeguards for the resource.
- Assisting with auditing resources under your management and investigating security incidents which affect those resources, as requested.
- Immediately reporting incidents that occur on your resources.
- Maintaining thorough, up-to-date documentation on your resources.
- Adhering to all CNCS information security standards and procedures for administration and maintenance of the resource (e.g., change control, backups, etc.)
- Assist with recovery of resource functionality and integrity in the event of disaster.
- Developing documented procedures for the custodian tasks you perform.

5.1.3 Reviewing And Understanding CNCS Information Security Policies

This section of the Handbook provides information and instructions for Information Custodians on fulfilling your information security responsibilities

You should also take the opportunity to review the detailed Information Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have any questions, please ask your supervisor or the CISO to provide clarification.

5.2 Developing System Security Plans

For more information on System Security Plans, see ISP-P-09, *System Security Plans*.



System Security Plans are critical for ensuring an appropriate level of security and risk mitigation for CNCS systems. A security plan lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures.

As an information custodian, you will be called upon to assist the owner of each major system that you manage with developing an SSP. As part of this process, you will fully document the configuration of the system, and help the owner to determine appropriate security measures to protect the system.

- SSPs must comply with the latest NIST guidance.
- SSPs will document the application of appropriate security controls based on the risk categorization of the system.
- SSPs will include a copy of or reference to security configuration checklists used on the system.
- Each System Security Plan must be reviewed and updated annually or when there is a major change to the system, whichever is earlier.
- SSPs must be marked, handled, and controlled as *sensitive* information.

5.3 Certifying & Accrediting Systems

For more information on C&A, see ISP-P-10, *Certification and Accreditation*.

Certification and Accreditation (C&A) is used to ensure that information systems have adequate security commensurate with the level of risk. To this end, C&A is the formalized process used to assess the risks and security requirements of each system, and to determine whether the system's security needs are being met.

The Federal Information Security Management Act (FISMA) requires CNCS to perform C&A of its information systems. For each system, this process must be completed either every three years or when there is a change that affects the system's security posture.

If you are the custodian of a major CNCS information system, then you will assist the owner of the system with certifying and accrediting that system. You may also be called upon by the CISO to assist with security testing of the system during the C&A process.

5.4 Contingency Planning

For more information on Contingency Planning, see ISP-P-11, *Contingency Planning*.



CNCS' information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, managerial, or operational solutions as part of CNCS' risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside CNCS' control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus, effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

If you are the custodian of a major CNCS information system, then you are responsible for the assisting the owner of that system with the development of a Contingency Plan or Disaster Recovery Plan. These plans will be based on a business impact analysis, and will identify measures to reduce the effects of system disruptions and increase system availability. You will help develop recovery strategies and procedures to ensure that systems may be recovered quickly and effectively following a disruption, and will participate in testing of the plans annually or when a significant change occurs. Additionally, you will assist with reviewing the plans regularly and updating them as needed to remain current.

5.5 Vulnerability Testing

For more information on vulnerability testing, see ISP-P-05, *Vulnerability Testing*.



Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand security attacks.

Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires CNCS to perform security testing on a periodic basis. A systematic, comprehensive, ongoing, and priority-driven security testing program will assist CNCS with determining its security priorities and making prudent investments to enhance the security posture of its information resources.

The CISO will develop a program to perform periodic, standardized vulnerability testing of all CNCS systems. Attempts will be made to minimize disruption of business operations.

As the custodian of a CNCS information resource, it is your responsibility to:

- Cooperate with, and provide assistance as requested to, the CISO and other designated personnel for performing testing on your systems.
- Resolve vulnerabilities discovered by testing, as reported in the test results.
- Document steps taken to resolve vulnerabilities and report these to the CISO.

5.6 Vulnerability Remediation

For more information on vulnerability testing, see ISP-P-06, *Vulnerability Remediation*



For more information on POA&Ms, see ISP-P-01, *Information Security Governance and Reporting*.

5.7 Security Training & Awareness

For more information on security training, see ISP-P-02, *Security Training & Awareness*.

5.8 Incident Reporting

For more information on incident reporting, see ISP-P-03, *Incident Reporting*.

Vulnerabilities may be detected or reported through a variety of sources, including periodic vulnerability testing; vendor alerts; US-CERT, NIST, or other reputable organization alerts; and IG or audit findings.

As a system custodian, you are responsible for remediating vulnerabilities reported for your system within a timely manner. You will work with your System Owner to assess reported vulnerabilities to determine level of impact on CNCS systems and develop a mitigation strategy.

- Corrective actions will be documented and scheduled in accordance with Patch Management and Change Control procedures.
- Once corrective actions have been taken, they will be validated to ensure the vulnerability has been adequately mitigated.
- Completion of vulnerability resolution will be reported back to the CISO.
- You will subscribe to vulnerability alerts and maintain awareness of vulnerability information for your systems.

A Plan of Actions & Milestones (POA&M) will be maintained for each major system to track specific weaknesses or vulnerabilities resulting from Inspector General audits, reviews, or scanning activity related to such work as risk assessments, certification testing, or penetration testing. You are responsible for helping your system owner to updates the system POA&M on at least a quarterly basis to support FISMA reporting to OMB.

You will treat information about CNCS vulnerabilities as *sensitive* information and protect the confidentiality of this information.

As the custodian of an information resource, it is your responsibility to train users, and make them aware of, the specific security policies and procedures of your system. These policies and procedures should be documented and published, and training provided if necessary.

You will also complete Information Custodian security training as prescribed by the CISO.

Additionally, you will subscribe to and participate in professional associations, news lists, peer groups, specialized forums and other activities to stay up to date with the latest security practices, techniques, and technologies applicable to your area of responsibility.

You must immediately report any suspected information security incidents so that CNCS may respond in a timely manner to minimize disruption of critical information services, as well as to minimize the loss or theft of *sensitive* and mission-critical information.

As an information custodian, you may receive reports from users or the information owner regarding security incidents involving your resources. You may also personally discover such incidents. In either case, you are obligated to report these incidents to the CISO using CNCS' incident reporting process, and to inform the information owner.

5.9 Incident Response

For more information on incident response, see ISP-P-04, *Incident Response*.



The agency must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

Additionally, the Federal Information Security Management Act (FISMA), and OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*, require organizations to have an incident response capability and to share information concerning common vulnerabilities and threats.

As an information custodian, it is your responsibility to cooperate with and support CNCS' incident response procedures. Such cooperation will make it possible for CNCS to respond quickly and effectively to situations that might compromise the agency's information resources.

Specifically, your responsibilities include:

- Implementing incident response procedures for the systems you manage.
- Immediately reporting incidents to the CISO.
- Documenting incidents and the resolution steps that were taken.
- Cooperating with, and providing assistance as requested to, the CISO, OIG, or other designated personnel investigating an incident.
- Informing the information owner regarding incidents.
- Implementing additional measures, as needed, to prevent further incidents.
- Providing follow up to ensure that incidents have been resolved.

5.10 System Development

For more information on system development security requirements, see ISP-C-12, *System Development Lifecycle Security*.



Security must be treated as an integral part of any system development or implementation project, including system modifications. It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later on. By considering information security early in the system life cycle, CNCS will be able to avoid higher costs later on while also developing a more secure system from the start.

You are responsible for helping the system owner with performing required tasks throughout the system lifecycle:

- Prior to approving the development/acquisition of a system, CNCS will evaluate the risks of the project:
 - CNCS will conduct sensitivity assessment (information, potential damage, laws, threats, environmental concerns, privacy, security characteristics, CNCS policy and guidance). The assessment will consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (e.g., hazardous location) and public threats to the system or information should also be considered.
 - CNCS will perform a preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.

- Security requirements shall be developed at the same time system planners define the other requirements of the system. The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.
- Application software used at CNCS must be obtained through authorized procurement channels and must comply with all licensing requirements.
- Each application must be categorized in accordance with CNCS' Security Categorization policy, and provided protection appropriate to its level of sensitivity and criticality.
- Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.
- Prior to placing the system into production, the following tasks will be performed:
 - The system will be thoroughly documented. Documentation of *sensitive* systems must be provided the same degree of protection as that provided for the system.
 - A System Security Plan (SSP) will be developed in accordance with CNCS System Security Plan policy and procedures.
 - Operational practices will be developed, including standard operational procedures and system-specific security policies (e.g., account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.
 - All systems will be thoroughly tested prior to being placed in the CNCS production operating environment.
 - *Sensitive* data will not be used to test systems until system security has been reasonably assured by testing with non-*sensitive* data or files.
 - The system's security features will be configured and enabled, and security management procedures will be implemented.
 - The system will be authorized for processing via CNCS' Certification and Accreditation (C&A) process.
- During ongoing operation and maintenance of the system, CNCS will ensure the following tasks are completed:
 - The security activities outlined in the system security plan (e.g., performing backups, holding training classes, managing accounts) will be performed.
 - Any changes made, or maintenance performed, on the system are to comply with CNCS' Change Control and Patch Management policies and processes.
 - Periodic security audits and vulnerability tests will be performed in accordance with CNCS Audit and Vulnerability Testing policies.
 - The SSP will be periodically reviewed and updated in accordance with the System Security Plan policy.

- The system will be periodically re-Certified and Accredited in accordance with NIST guidance.
- Systems must comply with all CNCS information security policies and procedures (e.g., change control, patch management, access control, backup and recovery, etc.)
- When disposing of a system, CNCS will ensure that proper measures are taken to protect the data that was stored in the system:
 - Information may be moved to another system, archived, discarded or destroyed in accordance with CNCS data retention policies.
 - Any storage media must be disposed of in accordance with CNCS' Media Management policies.
 - The disposition of software needs to comply with its license agreements.

Additionally, you will maintain a testing and development environment for performing your SDLC activities.

5.11 Application Security

Applications must identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries. The structure and content of error messages will be carefully considered as part of the design of any application. Error messages generated by the system will provide timely and useful information, without divulging potentially harmful information to unauthorized persons (i.e. information that could be used to exploit the system). Sensitive information (e.g., account numbers, SSNs, passwords, etc.) will not be shown in any error messages or error logs.

Applications must prevent unauthorized and unintended information transfer via shared resources by controlling object reuse (information remnance). No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) shall be available to any current user (or current process) who obtains access to a shared system resource that has been released back to the information system. There shall be no residual information from the shared resource.

User interface services (e.g., web services) shall be physically or logically partitioned from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

5.12 System Reports

Any report containing sensitive data must be marked with an appropriate header or footer, such as "Sensitive Information – For Official Use Only"

5.13 Managing Access Permissions

For more information on assigning access permissions, see ISP-C-01, *Access Control*.



Access to CNCS information resources is only to be granted to authorized personnel who have a legitimate need to use them, and access privileges for each resource will be limited to only those required to perform their duties. Excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability for negligence in protecting them.

As an information custodian, you are responsible for administering access permissions for the resources you manage, based on direction from the information owner. You are to work with the owner to develop and implement a process for managing access which complies with the following policies:

- Ensure that your resources are protected against unauthorized access by implementing appropriate access control measures.
- Use a documented process for granting, modifying, and revoking permissions.
- Grant access only to personnel who have a legitimate business need.
- Grant each user only the minimum access permissions required for their duties.
- Prior to granting someone access to *sensitive* information, verify that they have passed the appropriate background investigation.
- Before granting contractors or other non-CNCS personnel access to any *sensitive* data, make sure that they have been authorized by their COTR for this access.
- Periodically review access permissions and make adjustments as appropriate.
- Implement session timeout features

Detailed procedures must be documented for the creation, removal, and modification of user accounts and authentication credentials for each system. These procedures will also address automatic termination of temporary and emergency accounts; disabling of inactive accounts; automated mechanism(s) to audit account creations, modification, disabling, and termination actions;

5.14 Identification & Authentication

For More Information, see ISP-C-02, *Identification and Authentication*.



In order to ensure that unauthorized persons do not have access to *sensitive* CNCS information resources, it is necessary to first establish the identity of the user who is attempting to access the resource. Access can then be granted based on established identity.

The specific method(s) of authentication used for each resource shall be appropriate to its level of sensitivity (*i.e.*, more *sensitive* systems require stronger authentication). Multiple methods (*e.g.*, use of both a password and a token) may be required in high-risk situations.

Information custodians are responsible for:

- Assisting owners with determining and implementing appropriate authentication measures for their resources.
- Ensuring that passwords are appropriately assigned, used, and managed on the resources you manage, and that password and authentication policies are enforced. When feasible, automated techniques should be used to ensure strong passwords.
- Instructing users on the specific password and logon policies of the resource.

5.14.1
What are the policies regarding account management?



- Implementing measures to restrict access to authentication data.
- Obtaining authorization from the system owner prior to granting credentials.
- Reporting password or account compromises to the CISO and information owner.

User accounts must adhere to the following guidelines:

- Allow only one user per account; User IDs are never to be shared.
- Never install a guest account. Remove any guest accounts that are created by default by the system unless absolutely required and approved by the system owner and the CISO.
- No accounts will be named with easily guessed generic names (such as “anonymous”, “guest”, “admin”, “ftp”, “telnet”, “www”, “host”, “user”, “test”, “bin”, “nobody”, etc.) unless absolutely technically required by the system.
- Default accounts that are present upon initial installation of the system should be removed or renamed unless technically required by the system to keep the name.
- Accounts should be deactivated immediately upon termination of user.
- Unused accounts will be deactivated on at least a monthly basis.
- Accounts for contractors and other temporary staff will be configured to expire on the final date of their contract/employment, or 1 year from activation, whichever is earlier.

Administrator accounts must adhere to the following guidelines:

- The names of the administrator accounts should be renamed, if possible, to make it more difficult for attackers to guess the names of these accounts.
- Each person who has a legitimate need to use Administrator privileges should have their own administrative account that they will use to perform administrative functions. Usage of the main administrator account for each system should be limited to emergencies, and is to be limited to specific designated OIT staff. This will protect the main administrator account and also provide an audit trail of administrative activities.
- All accounts with administrator privileges must have strong passwords or other alternative strong authentication methods.

Account credential information (e.g., User IDs, passwords) that are stored on devices (such as enable passwords in router configuration files) must be encrypted.

To preclude brute force attacks, an intruder lockout feature must be implemented on each system to temporarily suspend the account after several invalid logon attempts.

5.14.2
What are the policies regarding password management?

If passwords are used for authentication, it is critical that they be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

For More Information, see
ISP-C-03, *Password
Management*.



In systems that use passwords as their authentication method, every account (including newly issued accounts) will have a password.

If SNMP is used, the community strings should follow the same rules as for passwords.

Passwords must be changed:

- Immediately upon initial user logon.
- At least every 90 days (systems may set a shorter expiration period for their users)
- If it is suspected that the password has been compromised.
- For admin accounts, immediately upon the departure of personnel with access.

The following guidelines apply to password storage and visibility:

- Passwords will not be visible on a screen, hardcopy or other output device.
- Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.
- Passwords will not be sent via unsecured email.
- Passwords will not be stored in written form (*e.g.* sticky notes).

The assignment of passwords for specific CNCS systems should adhere to the following:

- Each system should have its own password selection standard that adheres to the password guidelines while being commensurate with the level of security required by the level of sensitivity of the system.
- The system will be configured to enforce the password selection criteria specified in the system criteria.
- Passwords must be at least 8 characters and contain a combination of letters, numbers, and special characters.
- Passwords cannot be reused for at least 24 changes.
- Never set any password equal to the null string (*i.e.*, a blank password), which is equivalent to no password at all.

Tokens will be used only in conjunction with another authentication factor, such as a password or PIN.

You must implement defined procedures for distributing, tracking, and reclaiming access tokens which comply with the following:

- Tokens will only be given to personnel upon verification of their identity to ensure that tokens are not given to unauthorized persons.
- The custodian will maintain an inventory of tokens and their assignments.
- If tokens are lost, stolen, or not returned upon staff termination, they will be immediately disabled.

5.14.3

What are the policies regarding managing access tokens?

For More Information, see
ISP-C-04, *Access Tokens*



5.15 Maintaining Audit Trails

For more information on audit trails, see ISP-C-05, *Audit Trails*.



Systems will require that the token PIN be changed upon first use and on a periodic basis.

An audit trail of token usage will be enabled and periodically reviewed.

Tokens will be issued only for exclusive use by a single individual. Users may not share their tokens or allow anyone else to use them or the access they provide.

In order to enforce information security policies, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or “audit trail”) of system and application processes and user activity of systems and applications must be kept.

As an information custodian, you are responsible for configuring and maintaining audit trails on the resources that you manage, in accordance with the following requirements:

- For each server, you must enable and maintain logs for the following transactions (where possible given the constraints of the logging capabilities of the operating system and application software):
 - Server startup and shutdown
 - Manual loading and unloading of services
 - Installation and removal of software
 - User logon and logoff
 - System administration activities
- For each major application, enable and maintain logs for the following transactions:
 - Modifications to the application
 - User sign on and sign off
 - System administration activities
- For each for each router, firewall, or other major network device that you manage, you must enable and maintain logs for the following transactions (where possible given the constraints of the logging capabilities of the device):
 - Device startup and shutdown
 - Administrator logon and logoff
 - Configuration changes
 - Account creation, modification, or deletion
 - Modifications of privileges and access controls
- For each logged transaction, you must record the type of event, date, time, and the name of the account performing the transaction.
- Do not store *sensitive* information, such as passwords and system data, in the logs.
- Cooperate with and provide assistance (as requested) to the CISO and other

5.16 Managing System Changes

For more information on change management, see ISP-C-13, *Change Control*.



designated personnel, who will perform periodic audits of the log files to look for potential security issues or to research an incident.

- Control access to the audit logs to prevent tampering.
- Keep all audit trail files for at least one year and store them in a secure location.
- Develop documented procedures for audit trail monitoring.

Changes to CNCS' information systems must be controlled and managed to ensure integrity of the system and its data. Change control prevents unexpected changes from inadvertently causing denial of service, unauthorized disclosure of information, and other problems.

As an Information Custodian, you are responsible for implementing and documenting changes to your systems in compliance with CNCS policies and procedures:

- You will systematically plan, obtain approval, test and document changes to each system.
- You will develop baseline information that includes a current list of all components (hardware, software, and their documentation), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths, and switch settings, for your systems.
- For each of your information systems, you will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change, and any observations made during the course of the change.
- You will implement procedures to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:
 - Establish who performs maintenance and repair activities.
 - Provide for emergency repair and maintenance contingencies.
 - Procedures for verifying system and data integrity once change is complete.
- You will maintain version control that associates system components to the appropriate system version.
- You will conduct impact analyses to determine the effect of proposed changes on existing systems and security controls.
- You will implement procedures for testing and/or approving system components (operating system, other system, utility, applications) and configuration changes prior to promotion to production.
- You will adequately notify users regarding how they will be impacted by changes.
- You will have current backups available when changes are made.
- You will install all software, operating systems, and patches in accordance with U.S. copyright regulations, the license for that software, and applicable CNCS Information Security policies.

5.17 Backup & Recovery

For more information on media management, see ISP-C-08, *Backup and Recovery*.



- You will only make changes to CNCS information systems for which you are authorized to do so.
- You will document the change control procedures for your systems.
- You will keep change control documentation (especially change logs) available even if the network is down.
- You will provide documentation to the document manager to include in the repository.

There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. It is therefore essential that CNCS maintain backup copies of all critical data and systems so that they can be used to provide the continued availability and viability of these resources when these events occur.

As the custodian of a CNCS resource it is your responsibility to effectively back up your resources in accordance with CNCS policies, which include:

- You must back up all critical CNCS information resources that you manage.
- Back up critical data and system configurations on at least a daily basis. Back up applications and licenses whenever there are changes to them. The backing up of non-critical information is at the discretion of the data owner and system administrator. System configurations, applications, and licenses, should be backed up whenever changes are made to them and on at least a monthly basis. These should also be stored offsite.
- Send backups to an approved, environmentally-controlled, off-site storage location. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.
- Define and implement a backup retention schedule for your resources which complies with CNCS' data retention policies.
- Develop and implement detailed procedures for performing backups, restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.
- Periodically (at least annually) test your back up and restore procedures to ensure that data can be effectively restored from the backups.
- Handle backups with the same criticality and sensitivity as the data and applications stored on them, and in accordance with CNCS Media Management policy.
- Persons who have access to the backups, or who have access to perform back up or restore functions, must undergo appropriate background screening in accordance with CNCS Personnel Security policy prior to being given such access.

5.18 Media Management

For more information on media management, see ISP-C-11, *Media Management*.



CNCS has been entrusted with a variety of *sensitive* data in order to accomplish its mission. This data, which is stored on a variety of media (*e.g.*, hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes), must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, CNCS uses a variety of security protections for media.

Information custodians are responsible for the proper handling of media that has been entrusted to them, in accordance with CNCS policies and procedures. This includes:

- Providing appropriate physical and environmental protections for stored media.
- Marking any media containing *sensitive* data with its classification level. Labeling shall include any special handling instructions.
- Securing any media containing *sensitive* data (*e.g.*, storing it in a locked drawer, cabinet, or safe) when not in use or unattended. Any media containing *sensitive* information transported through the mail or courier/messenger service shall be double-sealed. The second envelope shall be appropriately marked with the sensitivity classification of the data.
- Monitoring the receipt and delivery of media containing *sensitive* data, and ensuring that data is not lost and potentially compromised while in transit.
- Sanitizing media that contains *sensitive* data before disposal, in accordance with CNCS media sanitization procedures.

Reporting the loss, damage, or theft of any media that has been entrusted to you.

5.19 Patch Management

For More Information, see ISP-C-09, *Patch Management & System Maintenance*.

Maintained patch levels are critical to the security of CNCS systems. Vendors will typically provide OS patches and fixes for security problems, which can be loaded separately from the application. These should be loaded on a regular basis using a coordinated process.

As the custodian of any CNCS information resource, it is your responsible to deploy patches to proactively prevent the exploitation of vulnerabilities. Specifically, you must adhere to the following requirements:

- Define detailed patch management procedures for each system you manage
- Monitor sources for available patches on a continuous basis. During regular operation, available patches will be reviewed monthly and applied if appropriate. In an emergency situation, more urgent application of new security patches may be required.
- Patches will be checked for compatibility with all system components prior to being applied.
 - Patches will be successfully tested on non-production systems prior to being loaded on production systems.
 - The use of standardized configuration baselines will simplify testing and reduce the risk of patching-induced problems.
 - The risk and impact of deploying each patch should be assessed prior to



5.20 System Maintenance

implementation of that patch.

- If a decision is made not to deploy a patch (e.g., due to risk or compatibility issues), that decision and the reason for the decision must be documented.
- All syst patching will be performed in accordance with CNCS Change Control policy and procedures.
- In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the correct patch levels before data is reloaded.
- New systems must be fully patched before being placed into the production IT environment.
- The use of automated tools to expedite the distribution of patches is encouraged. However, measures must be taken to reduce the risk of these tools being used by an attacker to distribute malicious code.

CNCS must be maintained in accordance with the following requirements:

- CNCS will schedule, perform, document, and review routine and preventative maintenance, as well as repairs on each system and component in accordance with manufacturer or vendor specifications.
- Software updates will be applied in accordance with CNCS Patch Management policies.
 - Where feasible, automated mechanisms will be used to schedule and conduct maintenance and to create maintenance records.
- Maintenance records will be maintained which include the following:
 - Date of maintenance
 - Name of individual performing the maintenance (and escort if applicable)
 - Description of maintenance performed
 - List of equipment removed or replaced
- Maintenance may only be performed by authorized personnel
 - Maintenance tools will be controlled to ensure use only by authorized personnel.
 - Maintenance personnel must have an appropriate background clearance or be closely supervised by personnel who are cleared and have authorization to perform maintenance activities.
- The use of remote maintenance and diagnostic tools must be authorized and monitored.
 - Remote maintenance is to be documented in the SSP.
 - CNCS will maintain records of all remote maintenance and diagnostic activities.
 - Remote maintenance must be performed through a secure encrypted connection in accordance with CNCS Remote Access and Encryption

policies.

- When remote maintenance is completed, all sessions and remote connections invoked in the performance of that activity will be terminated.
- Maintenance tools will themselves be properly maintained to ensure their effectiveness.
- Any hardware or software brought in specifically to perform diagnostic/repair activities must be approved and closely monitored
 - Any maintenance tools brought into the facility by external maintenance personnel will be inspected for obvious improper modifications.
 - Antivirus and other appropriate tools will be run to ensure that the tools do not contain malicious code.
 - Any maintenance tools or replaced equipment taken out of the facility will be inspected to ensure they contain no residual Corporation data.
 - Maintenance activities will comply with CNCS media management policies including sanitization.
- CNCS will obtain maintenance support and spare parts for all critical systems and keep these current and available in case of emergency.
- Changes made to systems as part of maintenance activities will be made in accordance with CNCS Change Control policies and procedures.

5.21 Using Encryption

For more information on encryption, see ISP-C-15, *Encryption*.



Encryption is an important tool that can be used to protect the confidentiality and integrity of information. CNCS' policy is that proven, government-approved encryption technologies be used to protect *sensitive* information which is transferred or stored outside of the CNCS computing environment (*e.g.*, on traveling laptops or for transmission over the Internet). This use must adhere to the following policies:

- The use of encryption to protect *sensitive* data, both in storage and in transmission, is encouraged.
- Only government-approved encryption techniques and devices may be used.
 - All encryption products must be Federal Information Processing Standard (FIPS) 140-2 or 197 certified.
 - Digital certificates used or issued by CNCS must comply with the Federal Public Key Infrastructure.
- Obey all regulations regarding restrictions on export of encryption technologies.
- Procedures must be documented for managing encryption keys, in order to ensure that these keys are protected from unauthorized disclosure, destruction, or misuse.
- A process must exist that allows the CISO to administratively recover lost keys.
- Any use of digital certificates to provide non-repudiation must be approved by the CISO, CIO, or Deputy CIO.

5.22 Emerging Threat Defense

For more information on the virus protection, see ISP-C-14, *Emerging Threat Defense*.



5.23 Physical Security

For more information on physical security, see ISP-C-07, *Physical and Environmental Security*.

Security risks are constantly evolving. Not only are new viruses, spyware programs, and spam developed daily, but new kinds of threats are constantly emerging. In addition to electronic threats like viruses and spyware, social engineering and other attacks that bypass technical protections are also becoming an increasing issue. These threats can result in loss of information, reduced system performance, disclosure of *sensitive* information, identity theft, unauthorized system changes, and a myriad of other risks. It is critical that CNCS implement proactive measures to protect its information and systems from these emerging threats. Tools and procedures must be implemented to minimize the impact of computer viruses, spyware, and other emerging threats on CNCS' information resources.

You must make sure that all systems and resources you manage are configured and compliant with the Corporation's approved antivirus, anti-spyware, anti-spam and other malware protection tools and procedures.

If you are the custodian of any CNCS server, workstation, laptop, or email gateway, you are responsible for:

- Installing and managing standard, supported security software on that resource
- Ensuring that the software is updated automatically as new definitions are made available by the vendor.
- Configuring the system to quarantine or delete infected files that cannot be repaired, and to scan all portable media before it is used on the computer.
- Removing any infected information resource that cannot be cleaned by the security software from the CNCS network.
- If lab testing conflicts with the security software, run a scan to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the software. When the software is disabled, do not run any applications that could transfer malware, *e.g.*, email or file sharing.
- Restricting the use of mobile code susceptible to malicious exploitation.

Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.

As the custodian of an information resource, you must implement and operate physical and environmental protections for your resource which meet the following standards:

- Physical access is to be controlled according to the sensitivity of the resource.
- Areas containing *sensitive* resources require special restrictions to limit access:
 - Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.
 - Personnel without an appropriate security clearance must be escorted.



- Areas containing *sensitive* information must be physically secured in accordance with CNCS facility security policies and CNCS Policy. 94-14.
- Critical resources require special protections to safeguard their availability:
 - Protection must be implemented against fire, flood, humidity, electromagnetic disturbance, and other environmental factors that could damage the resources.
 - Automated systems should monitor for environmental problems and alert specified personnel as appropriate.
- Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. It is important to keep backups in a separate location from the originals, not only for damage considerations, but also to guard against thefts.

If you are the custodian of a Data Center, you must:

- Meet all requirements listed above.
- Provide emergency power shutdown controls.
- Provide an uninterruptible power supply.
- Escort vendors and visitors at all times.
- Track all physical access to the room.
- Perform annual testing on fire, utility, and environmental alarms and systems.
- Make sure that access permissions to the Data Center are authorized and logged.
- Review data center access lists monthly



5.24 Asset Management

For more information on asset management, see ISP-C-10, *Asset Management*.

Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the wrath of auditing organizations like GAO and OMB.

Not only would loss of information assets result in a financial impact on CNCS, but it could also result in unauthorized access to data stored on or accessed through these assets, and could have a detrimental effect on the reputation of the agency. Additionally, several federal laws and regulations mandate the tracking and management of information assets.

You are responsible for assisting information owners with inventorying, tracking, and protecting the information assets which they own. This includes performing the following:

- Keeping a record of all information assets under their custodianship, including, but not limited to, workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.
- Assets are to be added to the record upon receipt and assigned a barcode.
- For each information asset, track at least the following information:
 - The brand, model, and type of asset
 - Serial number and CNCS asset tag number



5.25 Server Security

For more information on server security, see ISP-S-01, *Server Security*.



- The person to whom the asset is assigned
- The location of the asset
- Any maintenance agreements for the asset
- Upon disposal of an information asset, track the date of disposal, the method of disposal (*e.g.*, transfer, destruction, donation, etc.), and the name of the new owner.
- Perform periodic inventories to verify records and account for all information assets. Each asset is to be inventoried at least annually.

It takes only one incorrectly configured system to allow an intruder into CNCS' network. Therefore, no server should ever be placed on the production network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.

If you are the custodian of any CNCS server, then you are responsible for complying with the following server security requirements:

- Standard security configurations will be applied to each type of server.
- Where possible, security configurations will be enforced through automated policies
- Server images will be scanned to ensure they have been securely configured before they are placed into production.
- System patches and security updates must be applied in a timely fashion in accordance with the CNCS Patch Management policy.
- Any unnecessary services will be disabled (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).
- Access to all CNCS servers must adhere to the CNCS Access Control and Identification and Authentication policies.
- Auditing and logging must be enabled in accordance with CNCS auditing policies and procedures.
- All servers must run approved antivirus software configured in accordance with CNCS antivirus policies and procedures.
- Each server must be inventoried and tracked in accordance with CNCS asset management policies and procedures.
- Each server's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a server must be performed in accordance with CNCS change management policies and procedures.
- Servers will be located in access-controlled and environmentally protected facilities, in accordance with CNCS physical and environmental security policies and procedures.

5.26 Protecting Databases

For more information on database security, see ISP-S-06, *Database Security*.



CNCS has been entrusted with a variety of *sensitive* data to accomplish its goals. The success of agency programs depends on the availability, integrity and confidentiality of this information. In order to protect the data, CNCS must implement data security measures, such as data validation and verification controls. These controls are used to protect data from accidental or malicious alteration or destruction, to provide assurance that the information meets the expectations about its quality, and to ensure that it has not been altered.

As an Information Custodian, you are responsible for:

- Assisting Information Owners with maintaining the confidentiality, integrity, and availability of their data.
- Assisting Information Owners with implementing database security controls.
- Immediately reporting database security breaches to the data owner and the CISO.

Additionally, you must ensure that data repositories that you manage are compliant with the following security requirements:

- Data will be secured commensurate with its level of sensitivity and criticality.
- Databases, and applications that interface with databases, will be configured in accordance with security best practices:
 - Integrity verification programs, such as consistency checks, shall be used to look for evidence of data tampering, errors, and omissions.
 - Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure that software and data have not been modified.
 - If users are allowed to make updates to a database via a web page, these updates must be validated to ensure that they are warranted and safe.
 - For databases containing *sensitive* information, table access controls will be applied. Access to specific information within the database will be limited to only those personnel who need access to that information, and access will be limited to only those functions (*e.g.*, read, write, modify, etc.) required for the person to perform his or her duties.
 - Database servers must be configured to only allow connections from authorized, trusted sources (such as web servers to which they supply data).
 - For *sensitive* data, audit trails must be created and maintained within the database to track transactions and provide accountability.
 - You are encouraged to selectively encrypt data within the database in order to protect *sensitive* information.
- Programs or utilities that may be used to maintain and/or modify *sensitive* databases and other software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully controlled.
- Databases containing non-public information should never be on the same physical machine as a web server.
- Data repositories (and database servers) that store public information cannot be used

5.27 Network Security

For more information on network security, see ISP-S-02, *Network Security*.



to also store non-public (*e.g.*, private, proprietary, sensitive) information.

- Database servers and database software must adhere to all CNCS information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

It takes only one incorrectly configured system to allow an intruder into CNCS' network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.

If you are the custodian of a network device, then you are responsible for assisting the owner of the resource with implementing and managing security for that resource, and adhering to the following requirements:

- Standard baseline security configurations will be developed for each type of network component (*i.e.* routers, switches, etc.) and applied to all such components.
- The level of security applied to each network component should be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.
- Any unnecessary services will be disabled.
- Access to all CNCS network devices must adhere to the CNCS Access Control and Identification and Authentication policies.
- Remote administration of network devices can only be performed using encrypted and authenticated connections.
- Logging must be enabled in accordance with CNCS auditing policies and procedures.
- Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network or device.
- Each device must be inventoried and tracked in accordance with CNCS asset management policies and procedures.
- Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a device must be performed in accordance with CNCS change management policies and procedures.
- Physical access to Network devices will be controlled in accordance with CNCS physical and environmental security policies.
- Domain Name Service
 - CNCS will comply with federal DNSSec requirements, including SP800-81.
 - Name/address resolution systems will provide data origin and integrity information along with the authoritative information they return.
 - Systems providing name/address resolution service for the organization will be fault tolerant and will implement role (*e.g.*, internal vs. external) separation.

5.28 Remote Access

For more information on remote access, see ISP-S-08, *Remote Access*.



Remote access into CNCS systems provides many benefits. It allows personnel traveling on business to connect to CNCS information resources and provides the capability for telecommuting. However, remote access to CNCS via dial-up or other connectivity poses a risk of intrusion into CNCS by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of CNCS also lacks the protections afforded by CNCS' corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.

As the custodian of a resource which provides remote access into CNCS systems (other than those intended for public access), you are responsible for assisting the resource owner with the following requirements:

- All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).
- All *sensitive* data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.
- Session time-outs will be used to disconnect idle sessions after an inactivity period.
- All security policies for use in the CNCS office environment must also be observed when using or connecting to CNCS resources while outside the CNCS office.

5.29 Web Security

For more information on network security, see ISP-S-05, *Web Security*.

If you are the custodian for any workstations, you must adhere to the following policies regarding the configuration and management of those workstations:

- Standard base security configurations will be developed for and applied to each web server platform used by CNCS.
- You will apply additional appropriate security measures to web systems that require higher levels of security due to the data/services that they provide.
- Where possible, enforce security configurations through automated policies.
- You will apply system patches and security updates in a timely fashion in accordance with the CNCS Patch Management policy.
- You will configure audit trails in accordance with CNCS auditing policies.
- Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the system.
- Changes made to the web systems must be performed in accordance with CNCS change management policies and procedures.
- You will protect the integrity and availability of info made available to the public

5.30 Mobile Devices

For more information on mobile devices, see ISP-S-07, *Mobile Computing*.



The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow CNCS personnel to be more productive. However, the use of these devices outside of the CNCS office poses risks to those devices and the information they contain. These devices may also present a hazard to other CNCS resources upon their return to the CNCS office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of CNCS which lack the protections afforded by CNCS' corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.

If you are the custodian of any mobile devices, then you are responsible for assisting the owner of these resources with complying with the following requirements:

- Laptops and other mobile computing devices must be inventoried and tracked.
- Laptops must have antivirus software installed and enabled.
- Access to mobile devices which store or transmit *sensitive* data, or which can be used to connect to other *sensitive* CNCS systems, must be authenticated.
- If the device is used to store *sensitive* data, then encryption or other appropriate measures must be deployed to protect this data.
- The loss, theft, or destruction of any mobile device must be immediately reported.

5.31 Wireless Security

For more information on wireless networking, see ISP-S-03, *Wireless Security*.



In addition to the risks that apply to all networks, wireless connectivity is exposed to additional vulnerabilities. Wireless transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tied up network bandwidth and denied service to authorized users. Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

As the custodian of any wireless connectivity resource, you have the following responsibilities regarding wireless security:

- Assisting the owner of the resource with planning, implementing, and managing security controls to safeguard the wireless resource and the data transmitted over it.
- Safeguarding wireless information resources with which you have been entrusted.
- Adhering to CNCS policies for the administration of wireless devices, including:
 - Labeling all wireless devices prior to deployment.
 - Maintaining an inventory of all wireless devices.
- Disabling access or service for wireless devices that have been lost or stolen.
- Obtaining permission from the CIO before using or installing any wireless network cards, routers, or access points on the CNCS network.

5.32 Workstation Security



If you are the custodian for any workstations, you must adhere to the following policies regarding the configuration and management of those workstations:

- Standard base security configurations will be developed for and applied to each workstation operating system version (e.g., Windows XP, Windows 2000) used by CNCS. These baselines will conform to NIST and FDCC guidance or other appropriate federal standards if not available from NIST.
- You will apply additional appropriate security measures for workstations that require higher levels of security due to the sensitivity of the data and services that they access/provide (e.g., badging workstation).
- Where possible, you will enforce security configurations through automated policies (such as Windows Group Policies).
- You will verify workstation configurations to ensure they have been securely configured before they are placed into production.
- You will apply system patches and security updates in a timely fashion in accordance with the CNCS Patch Management policy.
- You will configure audit trails in accordance with CNCS auditing policies.
- All workstations must run approved antivirus software configured in accordance with CNCS antivirus policies and procedures.
- You will inventory and track each workstation in accordance with CNCS asset management policies and procedures.
- Changes made to the workstation baselines must be performed in accordance with CNCS change management policies and procedures.
- Restrict remote activation of collaborative computing devices, such as webcams

5.33 Electronic Mail

For more information on electronic mail, see ISP-S-10, *Electronic Mail*.



Electronic mail is an essential tool used by CNCS to conduct its business. However, email is inherently insecure and presents many risks to CNCS information. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to CNCS resources. Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.

If you administer electronic mail services, you must abide by the following policies:

- All email services provided on the CNCS network must be approved by the CIO.
- All incoming email must be scanned and filtered for viruses, disallowed content (including certain types of attachments), and other potentially malicious content.
- *Sensitive* information may not be sent over any public network (e.g., the Internet) unless it is encrypted.
- Electronic mail systems must adhere to and support CNCS record retention policies. This includes periodic archival and deletion of messages.

5.34 Perimeter Protection

For more information on perimeter protection, see ISP-C-16, *Perimeter Protection*.



Any connectivity to systems or organizations outside of CNCS provides an opening for unauthorized personnel to access or tamper with CNCS information resources. Such threats range from intruders breaking into CNCS' network to steal or alter data to service disruptions propagated from other systems. CNCS must implement firewalls, intrusion detection systems, and other precautions to prevent, detect, and resolve incidents arising from these threats.

As an information custodian, you are responsible for assisting information owners with deploying and managing perimeter resources and associated security measures, and complying with CNCS perimeter protection policies:

- Use firewalls and an Intrusion Detection System (IDS) to provide filtering, monitoring, and logging of traffic on all external communication links.
- Firewalls and IDS systems should be configured and administered in accordance with government and industry best practices, including but not limited to:
 - The default filters must specify that all access into the CNCS network be denied unless specifically permitted.
 - Each firewall, IDS, and other perimeter security device must be actively monitored, and periodically audited, for threats to the CNCS network.
 - Firewall and IDS equipment should provide real-time notifications or alerts to administrators upon security events.
 - If the firewall has a failure resulting in its inability to filter traffic in accordance with CNCS rules, it will not allow any traffic to pass until reset by an administrator.
 - If the firewall experiences a failure causing a reboot, it will default to a “Deny All” configuration.
 - Firewall services should run on a dedicated system with all other services disabled.
 - Source routing will be disabled on all firewalls and external routers.
 - The firewall will not accept traffic on its external interfaces that appears to be coming from internal network addresses.
 - The firewall implementation (system software, configuration data, database files, etc.) must be backed up in accordance with CNCS backup policy.
 - Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall software must be done by a firewall administrator(s) and requires the approval of the CISO.
 - Patches and updates will be implemented in a timely manner in alignment with CNCS patch management policy.
 - All services and traffic to be authorized across the firewall implementation must be well documented. Documentation will include the business need, protocol used, inbound and/or outbound, port assignments, known



vulnerabilities, and risk mitigation statements.

- The firewall will be configured to hide information about the network so that internal host data is not advertised to the outside world.
- Routing by the firewall will be disabled so that IP packets from one network are not directly routed from one network to the other.
- Any CNCS systems or services that are to be publicly available on the Internet must adhere to the following rules:
 - These systems must be placed in a protected DMZ.
 - No *sensitive* data is to be stored on systems located in the DMZ. All *sensitive* data must be located inside the firewall.
 - Access from the Internet to these systems must not make *sensitive* information or information systems vulnerable to compromise.
- Details of CNCS' internal network will not be attainable from outside the firewall.
- Proxy Servers:
 - All outbound connections to the Internet will be performed through a Proxy server. A proxy server provides a number of security enhancements by concentrating services through a specific host to allow monitoring, hiding of internal structure, etc.
 - Because this funneling of services creates an attractive target for a potential intruder, additional measures should be deployed to protect the proxy server.
- Any remote access into the CNCS network (e.g., telecommuting) must utilize 2 factor authentication and encryption, and adhere to CNCS remote access policies and procedures.
- Any changes to existing equipment or deployment of new equipment on the perimeter must adhere to CNCS change control procedures.
- Information regarding the configuration of firewall and other perimeter protections is considered confidential and is to be treated as *Sensitive* data.
- All hardware and software deployed on the perimeter must adhere to CNCS system security policies and procedures, including the disabling of all unnecessary services.
- All perimeter equipment must be documented in accordance with CNCS information system documentation procedures.
- All security related events on perimeter equipment, as well as access to CNCS via this equipment, must be logged and audited in accordance with CNCS' Audit Trail policies and procedures.
- The responsibility for the security of any equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. COTRs are responsible for third party compliance with this policy.
- Network Trust Relationships:

5.35 Telephone Security

For more information on telephony, see ISP-S-09, *Telephony Security*.

- All connections between the CNCS network and external networks (such as those of other agencies) must be approved by the CIO.
- Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures.
- An Interconnection Security Agreement will be developed and signed by CNCS and the external system owner specifying security responsibilities and protections that will govern the connection between the networks.
- All external connections will pass through CNCS-approved firewalls.

Telephone services are intended to support the objectives and operations of CNCS, and are critical to fulfilling CNCS' mission. These telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.

As a custodian of a telephony resource, you are responsible for assisting information owners with deploying, managing, and protecting their telephony resources in compliance with CNCS information security policies.

The agency VoIP and other critical telephony components must be protected:

- This equipment should be stored in a secure, environmentally controlled location in accordance with CNCS physical security policy.
- Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, Auditing, Patch Management, Server Security, Network Security, etc.
- Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk, and criticality/sensitivity of those resources.

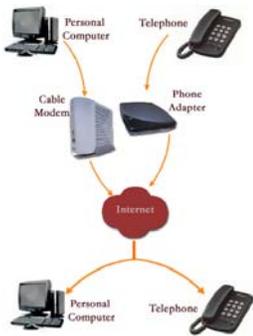
Modems or other telephony equipment and may not be installed without the explicit approval of the Deputy Chief Information Officer.

Analog Phone Lines - As a rule, the following applies to requests for fax and analog lines. Waivers to the policy will be granted on a case-by-case basis.

- Fax machines must be placed in centralized administrative areas designated for departmental use, and away from other computer equipment.
- The fax line is used solely for the fax machine that it has been assigned to.
- When not in use, analog lines are to be physically disconnected from the computer.

Computer-to-Analog Line Connections

- The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within CNCS will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the agency, and active penetrations have been launched against such lines by hackers. Waivers to the policy will be granted on a case-by-case basis. See ISP-S-09 for details on requesting a waiver.



- Lines must be terminated as soon as they are no longer in use.
- Computers are not to be connected to both an analog line and the CNCS network simultaneously.

Voice over IP (VoIP)

- When feasible Voice and Data should be logically separated onto different subnets.
 - Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VOIP firewall protection
 - At the voice gateway, which interfaces with the PSTN, H.323, SIP, or other VOIP protocols should be disallowed from the data network.
 - Use strong authentication and access control on the voice gateway system, as with any other critical network component.
- A mechanism to allow VOIP traffic through firewalls is required.
 - Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call.
 - VOIP-ready firewalls and other appropriate protection mechanisms should be employed.
- Use IPSec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
 - If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPSec tunneling. See the CNCS Encryption policy (ISP-C-15) for requirements.
- Physical controls are especially important in a VOIP environment and should be deployed accordingly.
- Additional power backup systems may be required to ensure continued operation during power outages.
- The security features that are included in VOIP systems are to be enabled, used, and routinely tested.
- The use of “softphone” systems, which implement VOIP using an ordinary PC with a headset and special software, should be tightly limited.
- If mobile units are to be integrated with the VOIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

5.36 Networked Copiers

"The networked copier that all companies have in the hallway or backroom is no longer the 'old school' device most IT managers still assume it to be. On the contrary, it's quickly evolved into a sophisticated computing platform that can grant access into the heart of the network. Copiers have been reborn as document distribution centers, enabling users to scan paper and send images via email or to, for example, document management, financial, or human resources systems. Integration with business applications allows for efficient distribution, editing, and storage of what was traditionally paper-based information. However, most networked copiers have not been secured in the same rigorous way as other end points, such as mobile devices and office workstations. In many companies, network-attached copiers could be used to distribute unauthorized documents or even distribute documents using identities that impersonate company executives."³

"The most common threats to digital copiers and printers stem from intruders stealing the hard drives containing confidential data, or reprinting documents directly from the machine after the earlier print command was canceled... Today's multifunctional copiers and printers store documents in memory... They might not just retain the last job, but the last 20 to 30."⁴

If you administer a networked copier, you need to follow these policies:

- Configure the copier to require authentication in order to access the administrator or core configuration functions on the copier. It is recommended that copiers also be configured to require network passwords for all functions to prevent unauthorized persons from accessing them. Configure the copier to log out the user after a brief period of inactivity. Employ intruder lockout features.
- Where possible, configure the copier to encrypt any scanned documents before transmitting them across the network.
- Configure the copier to securely delete temporary files rather than keeping them in memory. This will protect sensitive documents that have been copied or scanned. This should include automatic clearing of hard drives, RAM, and flash memory.
- Configure an audit trail on the copier to track all user activity including copying, printing, scanning, etc.
- Allow documents to be sent from the copier only to CNCS email addresses and internal applications (i.e. don't allow send from copier directly to outside CNCS).
- Prevent access to/from the copier from outside the firewall except through CNCS VPN.
- Copier operating system vulnerabilities should be tracked and addressed, including the periodic implementation of patches, like any other device on the network.
- Copiers must not be simultaneously connected to both the network and a phone line (for faxing) as this could provide a hacker with access into the network from the

³ "Seven Deadly Sins of Copier Security", Bill DeStefanis, AIIM E-DOC Magazine, February 9, 2007

⁴ IT Administrators May Be Overlooking Copier/Printer Security Risks, [Marcia Savage](#), ChannelWeb, August 2001

phone line.

- Security features that are provided with the copier should be activated to the greatest extent possible. If the copier has internal firewall features, filtering should be configured to prevent unauthorized use both incoming and outgoing. If the copier has a hard drive encryption feature, use it.
- Securely dispose of the copier when it is no longer needed.

When selecting new copiers, the risks and vulnerabilities inherent in each model should be considered as part of the selection criteria. Things to look for include:

- Resistant to viruses and Denial of Service attacks
- Less vulnerable operating systems.
- SSL and other encryption options.
- Ability to automatically securely delete documents from memory
- Robust access control features.
- Build in firewall capabilities
- Common Criteria certification
- Consider buying any additional security kit offered by the vendor.

CNCS security and privacy policies apply to copiers as they would to any other system/device on the network.

5.37 Emerging Technologies

For more information on perimeter protection, see ISP-S-13, *Emerging Technology*.

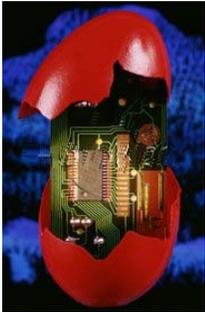
Prior to implementing any emerging technology into the CNCS production information technology environment, a risk analysis will be performed to ensure that the technology does not introduce undue risk to the Corporation's information and systems.

In conjunction with the CISO, you will assess the technology to determine:

- Whether any other federal government entity is using it, and if so, with what level of success, and what security issues they have encountered
- Whether the technology is really ready for production use. For example, if new bugs, vulnerabilities, and patching are being introduced at a fast rate, adoption of the technology should be delayed
- Whether there is sufficient benefit to the use of this technology over more established technologies to warrant the additional risks.
- Whether CNCS can acceptably manage and mitigate the risks to its information and operations due to the proposed technology.

The proposed technology will first be tested and evaluated in a non-production environment before being recommended for production use.

Use of the technology will be documented and evaluated as part of the CNCS system development lifecycle procedures, including:



- Development/Update of a System Security Plan
- Development/Update of a system Risk Assessment
- Completion of Certification and Accreditation

You will stay abreast of vulnerabilities reported for the new technology and take steps to address them in a timely fashion, in accordance with the CNCS Vulnerability Remediation and Patch Management policies.

APPENDIX A: INFORMATION SECURITY GLOSSARY

<i>Access</i>	The right to enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of specific information resources.
<i>Access Control</i>	The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.
<i>Access Control List</i>	List that contains a set of access control entries that define an object\'s permission settings and enables administrators to explicitly control access to resources.
<i>Access Privilege (Privilege)</i>	A specific activity that a user has been granted access to perform on an information resource (e.g. view or modify)
<i>Account</i>	A set of privileges for authorization to system access, which are associated with a userid.
<i>Accountability</i>	The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.
<i>Accreditation</i>	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
<i>Administrative Access</i>	Enhanced privilege level that allows the user to perform administration of the system.
<i>Alert</i>	A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.
<i>Analog</i>	A method of transmitting information in a continuous fashion via energy waves.
<i>Antivirus Software</i>	A program that monitors a computer or network to identify
<i>Application</i>	A self-contained software program designed to perform a defined set of tasks for a user, such as word processing, communications, or database management.
<i>Archival Data</i>	Information no longer in use, but which must be retained, and is stored separately to free space on a drive.
<i>Assurance</i>	A measure of confidence that the security features and architecture of a system accurately mediate and enforce the security policy.
<i>Attack</i>	An attempt to bypass security controls on a computer.
<i>Audit Trail</i>	A record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
<i>Authentication</i>	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
<i>Authentication Token</i>	A hardware device, the possession of which can be verified, and which helps to confirm identity as part of the authentication process (e.g., smartcard, SecureID)
<i>Authorization</i>	The formal granting of access to an individual to perform certain activities.
<i>Authorized Telework</i>	Approved work performed by an employee away from his or her duty station that requires connectivity to CNCS information resources.
<i>Authorizing Official (AO)</i>	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
<i>Availability</i>	Ensuring timely and reliable access to and use of an information resource
<i>Awareness</i>	A state of focused attention on security that allows individuals to recognize IT security concerns and respond accordingly.
<i>Back Up</i>	The action of copying (or mirroring) important data to a second location or onto removable media
<i>Backup</i>	A copy of data that is made in order to provide redundancy in case the original becomes corrupted or unavailable.

<i>Biometrics</i>	The identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice or handwriting.
<i>Blacklist</i>	A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity.
<i>Breach</i>	The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular system such that information assets or system components are unduly exposed.
<i>Brute Force Attack</i>	Attack where the attacker attempts to “guess” a password or other secret by trying all possible values.
<i>Bug</i>	An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction.
<i>Building Service Contractors</i>	Includes, but is not limited to, custodians, mechanics, electricians, plumbers, and guards.
<i>Business Identifiable Information (BII)</i>	information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."
<i>Certification</i>	A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
<i>Chain of Custody</i>	Verifies that information was not altered in the copying process and has not been altered during any analysis.
<i>Change Control/ Management</i>	Documented procedures used to control the revision of applications, operating systems, and hardware configurations in computing environments.
<i>Client</i>	Software that resides on the user's computer and communicates with a server(s).
<i>Compromise</i>	An intrusion into a computer system where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
<i>Computer Security</i>	The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).
<i>Confidential Information</i>	A classification for information whose disclosure may damage CNCS, the federal government, our customers, or other parties.
<i>Confidentiality</i>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
<i>Contingency Plan</i>	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
<i>Continuity Of Operations Plan (COOP)</i>	A predetermined set of instructions or procedures that describe how an organization’s essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.
<i>Contract</i>	Any U.S. Government contract or agreement issued or made by or on behalf of CNCS
<i>Contractor</i>	Any non-Federal employees working on any U.S. Government contract
<i>Cookie</i>	Small file on your computer in which a web site may write data.
<i>Copyrighted software</i>	Software for use only in accordance with licensing agreements.
<i>Countermeasures</i>	Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system. Synonymous with security controls and safeguards.
<i>Countermeasures</i>	Protections that are aimed at specific threats and vulnerabilities or involve more active techniques.
<i>Critical Incident</i>	An incident that will result in a severe impact to CNCS resources if not addressed quickly.
<i>Critical Information</i>	Any information essential to CNCS’ activities, the destruction, modification, or unavailability of which

	would cause serious disruption to the agency's mission.
<i>Critical Infrastructure</i>	A foundation of services that citizens and businesses rely on for their health, safety and well-being. Telecommunications, transportation, energy and banking services are part of the critical infrastructure, which is often privately owned but which citizens expect the government to protect.
<i>Cryptography</i>	A coding method in which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format by someone with a secret key) using an algorithm. Cryptography is used to send or store information securely.
<i>Cyberspace</i>	Describes the world of connected computers and the society that gathers around them. Commonly known as the INTERNET.
<i>Data</i>	A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.
<i>Database</i>	An organized collection of logically related information stored together in one or more computerized files.
<i>Decryption</i>	The mathematical process by which an encrypted message is rendered readable or usable (reverses the encryption process).
<i>Degaussing</i>	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.
<i>Denial-of-Service Attack (DoS)</i>	An attack in which a network, server, or even a telephone system is purposely overloaded with phony requests so that it cannot respond properly to valid ones. Prevents normal use of computer or network by valid users where the attacker can cause abnormal termination of the applications, flood the network with traffic, or block traffic.
<i>Designated Approving Authority (DAA)</i>	The senior management official or executive with the authority to approve the operation of an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
<i>Dial-in</i>	The capability to allow one system to access information or receive a message from another system over non-dedicated public phone lines.
<i>Digital</i>	Data that has been created, transmitted, or stored as a string of signals coded as "1" (on) or "0" (off). Data in digital form (text, numbers, graphics, voice, video, etc.) can be stored and processed by computers and communicated at high speed over electronic networks with complete accuracy and reliability.
<i>Digital Certificate</i>	The electronic equivalent of an ID card, which works in conjunction with public key encryption to sign digital signatures. A digital certificate, which may contain a users name and other information, is issued by a certification authority (CA), which also keeps track of digital certificates that have been revoked.
<i>Digital Signature</i>	A sequence of bits which accompanies a message that is generated via encryption; such a bit sequence shows that a message (a) was sent by an identified person, and (b) is free from modification or tampering.
<i>Disaster</i>	A condition in which an information resource is unavailable, as a result of a natural or manmade occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.
<i>Disaster Recovery Plan (DRP)</i>	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
<i>Disclosure</i>	Unauthorized access to confidential or sensitive information.
<i>Disposal</i>	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
<i>Disruption</i>	An unplanned event that causes the system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
<i>Distributed Denial-of-Service Attack (DDoS)</i>	A denial-of-service attack in which the attackers load their malignant code onto a host of other machines (often through Trojan horses). Distributed attacks can cause much more damage than an attack originating

from a single machine, as the defending company needs to block dozens or even hundreds of IP addresses. Compromised hosts used to attack other Internet sites, altering system binaries, and exposing sensitive information to external parties.

<i>DMZ (de-militarized zone)</i>	Any un-trusted network connected to, but separated from, the corporate network by a firewall, used for external (Internet/partner, etc.) access from within <Company Name>, or to provide information to external parties.
<i>Dongle</i>	A small device that plugs into a computer port that contains types of information similar to information on a smart card. Also called a hardware key.
<i>Dual Homing</i>	Having concurrent connectivity to more than one network from a computer or network device.
<i>Dynamic password</i>	A password which changes each time a user logs-into a computer system (typically accomplished via smart cards).
<i>E-commerce</i>	Transactions where money is exchanged for valuable goods and services with either the money and/or the goods and services transported over computer networks.
<i>Electronic Evidence</i>	Information and data of investigative value that is stored on or transmitted by an electronic device. Such evidence is acquired when data or physical items are collected and stored for examination purposes.
<i>Emerging Technology</i>	A new technology not yet fully exploited by businesses
<i>Employee Non-work Time</i>	Times when the employee is not otherwise expected to be addressing official business.
<i>Encryption</i>	The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access, especially during transmission
<i>Encryption key</i>	A secret password or bit string used to control the encryption process.
<i>End User</i>	An individual who employs computers to support CNCS activities, who is acting as the source or destination of information flowing through a computer system.
<i>Exposure</i>	The condition of vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.
<i>False Negative</i>	Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.
<i>False Positive</i>	Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.
<i>Fault Tolerance</i>	The ability of a system or component to continue normal operation despite the presence of hardware or software faults.
<i>Federal Information System</i>	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
<i>Field</i>	A single piece of information stored in a database.
<i>Firewall</i>	A program that protects a computer or network from other networks by limiting and monitoring network communication.
<i>General Support Systems (GSS)</i>	An interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and applications.
<i>Government Office Equipment</i>	Includes but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones to include cellular, facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and E-mail
<i>Hacker</i>	A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around.
<i>Hardening</i>	The process of disabling unnecessary services, installing all the latest patches, installing security software

	(e.g., antivirus software), tuning the operating system, and documenting the system.
<i>Host</i>	A computer or IT device (e.g., router, switch, gateway, firewall). Host is synonymous with the less formal definition of system.
<i>Identification</i>	The process of determining who a user claims to be; usually performed by presenting a user ID (i.e., “jsmith”).
<i>Impersonation</i>	Pretending to be authorized to enter a secure location.
<i>Industrial Espionage</i>	The act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies).
<i>Information Asset</i>	An information resource that has tangible value.
<i>Information Assurance</i>	Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
<i>Information Custodians</i>	Individuals (e.g., IT staff) who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner’s requirements for processing, telecommunications, protection controls, and output distribution for the resource.
<i>Information in Identifiable Form (IIF)</i>	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
<i>Information Owner</i>	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
<i>Information Resources</i>	The equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.
<i>Information Security (InfoSec)</i>	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
<i>Information system</i>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
<i>Information Technology</i>	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.
<i>Information Type</i>	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
<i>Information Users</i>	Individuals who use or have access to CNCS’ information resources, including employees, vendors, and visitors.
<i>Integrity</i>	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
<i>Interconnection Security Agreement (ISA)</i>	An agreement established between owners/operators of connected IT systems that documents the requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.
<i>Intruder</i>	An unauthorized user or unauthorized program, generally considered to have malicious intent, on a computer or computer network.
<i>Intrusion</i>	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource through unauthorized access or penetration of an information resource.
<i>Intrusion Detection</i>	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.
<i>Intrusion Detection System</i>	A system that analyzes network traffic to detect anomalies and provide alerts regarding possible intrusions.

<i>IP address</i>	A 32-bit binary address used to identify a host's network ID.
<i>ISDN</i>	A type of communication line which can carry voice, digital network services and video.
<i>Isolated computer</i>	A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.
<i>Key</i>	A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt.
<i>Keystroke Monitoring</i>	A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.
<i>Lab Network</i>	Any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to CNCS nor affect the production network.
<i>LDAP (Lightweight Directory Access Protocol)</i>	A standardized way to connect with a directory which might hold passwords, addresses, public encryption keys, and other exchange-facilitating data.
<i>Least Privilege</i>	Granting users only the minimum privileges required to provide the level of access needed to perform their official duties.
<i>Legacy System</i>	Older software and hardware systems still in use and generally proprietary.
<i>LISTSERV</i>	Commercial mailing list. Although LISTSERV refers to a specific mailing list server, the term is sometimes used incorrectly to refer to any mailing list server.
<i>Local Area Network (LAN)</i>	A communications system that connects information resources within a building or group of buildings within a few square kilometers, including workstations, front-end processors, controllers, switches, and gateways.
<i>Log files</i>	Files that show the status of the system and are accessed via Event Viewer, which lists the severity and a brief description of the logged event.
<i>Major Application (MA)</i>	An information system that requires special attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. An MA requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
<i>Major change</i>	Any change to the hardware, software, or firmware components of an information system that may have an impact on the protection capabilities of that system and the enforcement of the system security policy.
<i>Malicious Code</i>	Any software or firmware that is intentionally included in a system for an unauthorized purpose. Examples include viruses like Trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and to modify audit logs to hide unauthorized activity Information given to you when you log into or otherwise access a system.
<i>Malware</i>	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
<i>Management Controls</i>	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
<i>Media</i>	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
<i>Memory Cards</i>	Removable electronic storage devices, which do not lose the information when power is removed from the card.
<i>Memory Scavenging</i>	Searching through data storage to collect residue thereby acquiring data. Data may be stored on records, blocks, pages, segments, files, directories, words, bytes, fields, or peripheral devices, such as printers or

video displays.

<i>Metadata</i>	Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. There are at least three types of metadata: semantic data, which gives the meaning of the "raw" data; formatting data which describes the appearance of the data on-screen or on-page; and intellectual property data which describes data ownership conditions.
<i>Metrics</i>	Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
<i>Minor Application</i>	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.
<i>Mobile Computing Device</i>	A laptop, PDA, or other portable device that can store or process data.
<i>Modem</i>	A device that enables a computer to transmit data over telephone lines by converting data between the computer's digital format and the phone line's analog format.
<i>National Security System</i>	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
<i>Need-to-know</i>	The necessity for access to, knowledge of, or possession of sensitive information to carry out duties. The possessor of the information, not the prospective recipient, is responsible for determining whether a person's official duties require possession or access to sensitive or controlled information and whether the person is cleared to receive it.
<i>Network</i>	Two or more machines interconnected for communications.
<i>Network Device</i>	Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.
<i>Network Infrastructure</i>	Network infrastructure includes servers, network devices, and any other back-office equipment.
<i>Network Security</i>	Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.
<i>Node</i>	In a network, a node can be a computer or some other device such as a printer. Every node has a unique network address.
<i>Non-Repudiation</i>	Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.
<i>Operating System</i>	The master control program that runs a computer.
<i>Operational Controls</i>	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
<i>Organization</i>	A federal agency or, as appropriate, any of its operational elements.
<i>Password</i>	Any secret string of characters which serves as authentication of a person's identity, and which may be used to grant or deny access.
<i>Patch</i>	An additional piece of code developed to address a problem in an existing piece of software.
<i>Penetration</i>	The successful unauthorized access to an information resource by bypassing the security mechanisms of a

	network or system.
<i>Penetration Testing</i>	The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators work under the same constraints applied to ordinary users.
<i>Perimeter</i>	The boundary between CNCS owned/operated information resources and those under the control of another party.
<i>Perimeter Based Security</i>	The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and intrusion detection systems.
<i>Perimeter Equipment</i>	Any devices or servers which form part of the perimeter (e.g., perimeter router), are deployed to protect the perimeter (e.g., firewall), or which reside on the perimeter (e.g., DMZ web servers).
<i>Personal Firewall</i>	Software installed on a computer or device which helps protect that system against unauthorized access.
<i>Personal use</i>	Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.
<i>Personnel Security</i>	The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.
<i>Phishing</i>	Tricking individuals into disclosing sensitive information through deceptive computer-based means.
<i>Physical Security</i>	The measures used to provide physical protection of resources against deliberate and accidental threats.
<i>Piggybacking</i>	1. Unauthorized access to information by using a terminal that is already logged on with an authorized ID; 2. Entering secure premises by following an authorized person through the security perimeter.
<i>Plaintext</i>	Unencrypted data.
<i>Plan of Actions and Milestones (POA&M)</i>	A tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.
<i>Platform</i>	Underlying hardware or software for a system.
<i>Policies</i>	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
<i>Privacy Impact Assessment (PIA)</i>	An analysis of how information is handled: 1) to ensure handling conforms to applicable regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
<i>Private Branch Exchange (PBX)</i>	A private telephone switchboard that provides on-premises dial service and may provide connections to public communications networks.
<i>Private Key Cryptography</i>	An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.
<i>Privilege</i>	A specific activity that a user has been granted access to perform on a resource (e.g. view or modify)
<i>Plan of Actions & Milestones (POA&M)</i>	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
<i>Proprietary Encryption</i>	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
<i>Protocol</i>	Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data.
<i>Proxy Server</i>	A system that acts on behalf of another user or process. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
<i>Public Key</i>	A system for securely exchanging information that includes a method for publishing the public keys used in

<i>Infrastructure (PKI)</i>	public key cryptography and for keeping track of keys that are no longer valid.
<i>Record</i>	Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph
<i>Records</i>	All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them.
<i>Remanence</i>	Residual information remaining on data storage media after clearing.
<i>Remediation</i>	The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.
<i>Remote Access</i>	Any access to CNCS' corporate network through a network, device, or medium that is not controlled by CNCS (such as the Internet, public phone line, wireless carrier, or other connectivity).
<i>Residual Data</i>	Information that appears to be gone, but is still recoverable from the computer system and includes "deleted" files still extant on a disk surface and data existing in other system hardware such as buffer memories of printers and fax machines.
<i>Restore</i>	The process of copying data from a previously-made backup to the original (or an alternate) system.
<i>Risk</i>	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
<i>Risk Assessment</i>	The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk.
<i>Risk Management</i>	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the n system.
<i>Router</i>	A device that interconnects networks and directs and filters traffic between them.
<i>Safeguards</i>	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
<i>Sanitize</i>	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
<i>Security Architecture</i>	A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.
<i>Security Baseline</i>	The set of minimum security controls defined for a type of information system.
<i>Security Controls</i>	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
<i>Security Incident</i>	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

<i>Security Requirements</i>	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, regulations, or procedures, or organizational mission/business needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
<i>Security Violation</i>	An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.
<i>Sensitive Information</i>	Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
<i>Separation Of Duties</i>	Concept which provides the necessary checks and balances to mitigate against fraud, errors, and omissions by ensuring that no individual or function has control of the entire process
<i>Server</i>	Computer that provides a service or application that users access through a network connection.
<i>Signature</i>	A pattern that corresponds to a known threat.
<i>Smart Card</i>	A device that is similar in size to a credit card but that has the capability to store data and perform processing of information.
<i>Spam</i>	Unauthorized and unsolicited electronic mass mailings.
<i>Split Tunneling</i>	Simultaneous direct access to a non-CNCS network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into CNCS' corporate network via a VPN tunnel.
<i>Spoofing</i>	The creation of IP packets with counterfeit IP source addresses.
<i>Spyware</i>	Software that is secretly installed on a users computer and that monitors use of the computer in some way without the users' knowledge or consent.
<i>Standard</i>	A procedure or control mechanism that is required to be used in specific situations.
<i>Strong Authentication</i>	An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.
<i>Switch</i>	A physical component that connects multiple computers and devices to a network
<i>System Administrator</i>	An individual who has special privileges to maintain the operation of a computer application or system.
<i>System control data</i>	Data files such as programs, password files, security tables, authorization tables, etc., which if not adequately protected, could permit unauthorized access to information resources
<i>System Development Life Cycle</i>	The system development life cycle (SDLC) starts with the initiation of the system planning process, and continues through system acquisition/development, implementation, operations and maintenance, and ends with disposition of the system.
<i>System of Records</i>	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual
<i>System Permissions</i>	The technical configuration that provides an individual the ability to perform certain actions on information resources.
<i>System Security Plan</i>	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
<i>System Testing & Evaluation</i>	Review and validation of security controls to ensure that they are implemented as specified and are effectively providing the desired level of security.
<i>Technical Controls</i>	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
<i>Telephony</i>	The technology associated with the electronic transmission of voice, fax, or other information between

	distant parties using systems historically associated with the telephone.
<i>Threat</i>	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
<i>Threat Assessment</i>	Process of formally evaluating the nature and degree of threat to an information system.
<i>Token</i>	Something that the user physically possesses which is used to authenticate the user's identity. Examples include access cards, secureIDs, and dongles.
<i>Trojan Horse</i>	A malicious program that disguises itself as a beneficial or entertaining program but that actually damages a computer or installs code that can counteract security measures (perhaps by collecting passwords) or perform other tasks (such as launching a distributed denial of service attack).
<i>Unauthorized Access</i>	The use of an information resource without permission
<i>Un-Trusted Network</i>	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.
<i>UserID</i>	Character string that uniquely identifies a computer user or computer process.
<i>Validation</i>	The checking of data for correctness and/or for compliance with applicable standards, rules, and conventions.
<i>Verification</i>	The process of ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.
<i>Virtual Private Network (VPN)</i>	A method for establishing a secure virtual channel ("tunnel") through an unsecured network (such as the Internet) through the use of encryption.
<i>Virus</i>	A program designed with malicious intent that has the ability to spread to multiple computers or programs.
<i>Vulnerability</i>	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
<i>Vulnerability Testing/Assessment</i>	Systematic examination of a network or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
<i>Web Server</i>	A computer that provides World Wide Web (WWW) services. It includes the hardware, operating system, Web server software, and the Web site content.
<i>Web System</i>	A web server or web-based service or application that runs on a web server
<i>White List</i>	A list of discrete entities, such as hosts or applications, that are known to be benign.
<i>Wide Area Network (WAN)</i>	A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks
<i>Wipe</i>	Deliberately overwriting a piece of media and removing any trace of files or file fragments.
<i>Wireless Technology</i>	Any type of connectivity that transmits data without the use of physical cabling. Wireless systems include radio transmissions, satellite links, cell phones, and devices such as wireless headphones. Infrared (IR) devices such as remote controls, cordless computer keyboards, and cordless mouse devices are also included.
<i>Workstation</i>	Includes desktop computers, laptops, and other computers used to access CNCS systems.
<i>Worm</i>	Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads, perhaps causing denial of service.