

Corporation for National and Community Service

Policies and Procedures

Policy Number: 376

Effective Date: February 26, 2016

Subject: Cybersecurity Policy

Purpose: This policy is designed to protect CNCS information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

Who is Covered: This policy applies to all CNCS employees, including federal full-time, part-time, and temporary employees, contractors, interns, volunteers, or any other individual who operates or has access to CNCS information or information systems.

Policies Replaced: CNCS Policy Number 376, *Information Assurance Program*; dated 11/2012

Originating Office: OIT

Summary of Revisions: This policy is revised to update the organization name to Cybersecurity (from Information Assurance) and update contents to reflect and support current laws, Executive Orders, memoranda, requirements, and guidance.

Approved By:



Asim Mishra
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 800-833-3722 (TDD). You may also send an email to ashelp@cns.gov.

Table of Contents

1.0 CYBERSECURITY PROGRAM	1
1.1. Objective	1
1.2. Scope.....	1
1.3. Noncompliance	1
2.0 ROLES AND RESPONSIBILITIES	2
2.1. Chief Executive Officer (CEO)	2
2.2. Chief Information Officer (CIO)	2
2.3. Chief Information Security Officer (CISO).....	3
2.4. Authorizing Official (AO)	4
2.5. Information System Owner (ISO).....	4
2.6. Information System Security Manager (ISSM)	5
2.7. Information System Security Officer (ISSO)	5
3.0 INFORMATION SYSTEM SECURITY	7
3.1. Scope.....	7
3.2. Control Noncompliance	7
3.3. Information Security Controls	7
3.3.1. Program Management (PM).....	7
3.3.2. Access Control (AC)	7
3.3.2.1 Acceptable Use.....	7
3.3.3. Awareness and Training (AT).....	8
3.3.4. Audit and Accountability (AU).....	9
3.3.5. Certification, Accreditation, and Security Assessments (CA)	9
3.3.6. Configuration Management (CM).....	9
3.3.7. Contingency Planning (CP).....	9
3.3.8. Identification and Authentication (IA)	10
3.3.9. Incident Response (IR).....	10
3.3.10. Maintenance (MA)	10
3.3.11. Media Protection (MP).....	10
3.3.12. Physical and Environmental Protection (PE).....	10
3.3.13. Planning (PL)	11

3.3.14. Personnel Screening for Information and Information System Access (PS) 11

3.3.15. Risk Assessment (RA)..... 11

3.3.16. System and Services Acquisition (SA) 11

3.3.17. System and Communications Protection (SC) 12

3.3.18. System and Information Integrity (SI) 12

APPENDIX A: Applicable Laws and References A-1

APPENDIX B: Acronyms and Abbreviations..... B-1

1.0 CYBERSECURITY PROGRAM

The Corporation for National and Community Service (CNCS) is responsible for implementing and administering an information security program. This program must protect CNCS information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction. CNCS's procedures for securing federal information must be consistent with federal security and privacy laws and policies (see APPENDIX A: [Appendix A: Applicable Laws and References](#)). To meet these requirements, CNCS has established a Cybersecurity Program to secure information systems and protect privacy information. This policy documents and describes the cybersecurity program. It is reviewed and updated annually, or as needed.

1.1. Objective

The objective of this policy is to establish a Cybersecurity Program that:

- Protects privacy and business sensitive information.
- Implements best security practices based on a risk and cost/benefit approach.
- Provides training and awareness for users, employees with elevated privileges, and those with information assurance roles.

1.2. Scope

This policy applies to:

1. CNCS information systems that collect, store, process, disseminate, transmit, or dispose of information, including information or those information systems managed by contract personnel for CNCS, and non-CNCS owned information systems that access CNCS information or information systems;
2. Any information system funded by CNCS, all information systems connected to CNCS information systems, and prototype information systems connected to any CNCS operational information systems; and
3. Agency employees, contract personnel, and other users of CNCS information and information systems under written agreement between the user or contract personnel and CNCS.

1.3. Noncompliance

Any user exceeding assigned privileges could be subject to loss or limitations on use of information resources, as well as disciplinary and/or legal action, up to termination of employment and referral for criminal prosecution.

2.0 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities of key participants involved in the Cybersecurity Program. Some of the following positions may be held by the same individual if there is not an oversight function, and some may be held by more than one individual if there is a clear delineation of responsibility.

2.1. Chief Executive Officer (CEO)

The CEO is responsible for ensuring that the Cybersecurity Policy is developed and implemented in accordance with regulatory and business requirements. The CEO plays a crucial role in allocating resources and fostering commitment to the Cybersecurity Program. In support of the Cybersecurity Program, the CEO ensures that the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) positions are filled with qualified individuals.

2.2. Chief Information Officer (CIO)

The CIO¹ is responsible for the execution of CNCS's overall Information Technology (IT) program and delegates authority to the CISO for the management of the Cybersecurity Program. The CIO is the focal point for IT management and governance of IT portfolios and is responsible for:

- Managing the agency's cybersecurity risks. Coordinating with senior management to report annually to the head of the federal agency on the overall effectiveness of CNCS's Cybersecurity Program, including progress of remedial actions.
- Keeping the Corporation's senior executives abreast of the agency's cyber capabilities, and informing them in the event of any attacks.
- Identifying the IT infrastructure and data that is critical to the agency's mission, and securing the agency's resources – including infrastructure, data, and personnel – against known and emerging cyber threats in the most timely and cost-effective manner.
- Establishing and supporting the resource and budget requirements to meet the intent of this Policy.
- Establishing identity, credentials and access management. Ensuring that information systems are covered by approved system security plans (SSPs) and are authorized to operate.
- Ensuring that all requirements for annual Federal Information Security Modernization Act 2014 (FISMA) evaluations are being met so that the audit is successfully complete.

¹ The role of CIO has inherent U.S. Government authority and is assigned to government personnel only.

- Ensuring CNCS appropriately trains personnel to comply with cybersecurity requirements and protect CNCS assets.

2.3. Chief Information Security Officer (CISO)

The CISO² carries out the CIO's security and privacy responsibilities under the Federal Information Security Modernization Act 2014 (FISMA), and other laws, policies, and regulations listed in APPENDIX A: [Appendix A: Applicable Laws and References](#) and is responsible for managing the Cybersecurity Program. The CISO must: (i) possess professional qualifications, including training and experience, required to administer the cybersecurity functions; (ii) maintain information assurance duties as a primary responsibility; and (iii) head an office with the mission and resources to assist the organization in achieving more secure information and information systems. The CISO is responsible for:

- Developing an organization-wide Cybersecurity Program that provides adequate security for all CNCS information and information systems.
- Advising and updating senior management on the effectiveness of the Cybersecurity program.
- Working with senior management to ensure IT security protection policies are accepted, implemented, reviewed, maintained and governed effectively.
- Supervising compliance with the Corporation's security policies, standards and procedures.
- Ensuring that personnel with significant system security responsibilities are adequately trained.
- Centralized reporting of information security-related activities. Reporting duties include developing and submitting an annual FISMA report.
- Monitoring security incidents and providing assistance when required.
- Auditing existing systems and providing comprehensive risk assessments.
- Keeping abreast of the latest security threats and security posture of CNCS network and information systems.
- Ensuring that changes to infrastructure and applications do not compromise the security of the agency beyond acceptable risk.
- Conducting training for CNCS personnel to comply with cybersecurity requirements and protect CNCS assets.

² The role of CISO has inherent U.S. Government authority and is assigned to government personnel only.

2.4. Authorizing Official (AO)

The AO is granted the authority to formally assume responsibility for operating an information system at an acceptable level of risk. The AO has budgetary oversight for an information system and is responsible for the mission/business operations supported by the system. AOs approve systems security plans (SSPs), memorandums of agreement or understanding (MOA/MOU) with review of the Office of General Counsel, and plans of action and milestones (POAMs). AOs can deny authorization to operate an information system, or if the system is operational halt operations if unacceptable risks exist. It is possible that a particular information system may involve multiple AOs. If so, agreements are established among the AOs and documented in the SSP.

The AO is responsible for:

- Designating one of the following operational statuses of a system:
 - Authority to operate (ATO), including reauthorizing information systems when required;
 - Interim approval to test (IATT); or,
 - Denial of authority to operate a system, including disconnection of an information system.
- Ensuring that the security posture of the information system is maintained.
- Assisting, when required, in CNCS's response to security incidents and privacy breaches.
- Ensuring that resources (i.e., people and budget), are available to secure the system.
- Appointing the Information System Owner (ISO).

2.5. Information System Owner (ISO)

The ISO is responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system and the data/information processed and retained by the information system. The ISO serves as the focal point for the information system and is the central point of contact (POC) during the security authorization process. The ISO is responsible for:

- Planning, directing, and managing resources for an information system.
- Ensuring that the system is operating in a manner consistent with federal and agency requirements.
- Ensuring that the system is compliant with the required security controls.
- Appointing an Information System Security Officer (ISSO) for the information system to carry out the day-to-day security responsibilities.
- Fulfilling the duties of the Data/Information Owner/Steward role identified by National Institute of Standards and Technology (NIST)
- If needed, appointing an ISSM to coordinate system security tasks and provide oversight responsibilities to ensure security activities are performed.
- Reviewing system security documents (e.g., SSP, POAM, etc.).

- Ensuring that remediation activities for the system are performed as needed to maintain the authorization status.
- Determining, in coordination with the ISSO/M, access privileges and rights to the system.
- Categorizing the sensitivity level of the information processed and stored in the system.
- Establishing rules for appropriate use and protection of the information.
- Ensuring that the PII inventory is updated.
- Assisting in CNCS's response to security incidents and privacy breaches.
- Establishing an independent validation of security controls.

2.6. Information System Security Manager (ISSM)

The ISSM coordinates system security tasks and provides oversight responsibilities to ensure security activities are performed. The ISSM serves as the liaison between the ISSO and the ISO. In these situations, the ISSO coordinates directly with the ISSM for all system security related issues. The ISSM is responsible for:

- Providing oversight of system security activities.
- Acting as the liaison between the ISSO and ISO.
- Monitoring system compliance with CNCS cybersecurity policies and federal guidance.
- Ensuring that quarterly reviews (e.g., accounts, POAMs, etc.) are conducted.
- Reviewing system security documents (e.g., SSP, POAMs, etc.) and advising the ISO.
- Ensuring that remediation activities for the system are performed as needed to maintain the authorization status.
- Assisting in CNCS's response to security incidents and privacy breaches.

2.7. Information System Security Officer (ISSO)

The ISSO works closely with the ISO and ISSM to ensure that system security controls are implemented and monitored. The ISSO serves as a principal advisor on all the security related issues of an information system. The ISSO must have the detailed knowledge and expertise required to manage the security aspects of an information system and is responsible for the day-to-day security operations of a system. ISSO responsibilities include:

- Day to day security related tasks.
- Ensuring system compliance with security policies and procedures.
- Ensuring that changes to the system are conducted in accordance with security policy and procedures.
- Assessing the security impact of any changes.
- Monitoring the system and its environment.

- Developing and updating the SSP, POAM, and other security related documentation.
- Coordinating with and supporting the ISO with security responsibilities.
- Developing system-level security procedures that are consistent with CNCS's cybersecurity policies.
- Performing or overseeing remediation activities to maintain the authorization status.
- Creating the ATO package for submission to the AO.
- Managing identified vulnerability remediation.
- Managing security incidents.
- Supporting audits and investigations.
- Other security tasks as assigned.

3.0 INFORMATION SYSTEM SECURITY

3.1. Scope

CNCS must ensure that security controls are implemented considering the risk and magnitude of the harm that would result from loss, misuse, denial of service, unauthorized access, or modification of CNCS information assets.

Control families are defined in the NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, as amended. CNCS information systems must have documented procedures for each control family that explains how security controls are implemented. Procedures must be maintained, reviewed annually, and updated when changes occur or annually. The following sections provides details to the CNCS policies, procedures, and/or programs associated with each security control family. Details pertaining to organizationally defined requirements are included in the *CNCS Cybersecurity Control Families* document.

3.2. Control Noncompliance

Waivers and/or risk acceptance for delaying, modifying, or not implementing a control must be submitted to the CISO, CIO, or delegated representative for decision or guidance.

3.3. Information Security Controls

Documents identified in this section are accessible from the COO: Office of Information Technology: Cybersecurity – Important Links: [Cybersecurity Policies, SOPs and Template](#) SharePoint page, CNCS Policies or the internet.

3.3.1. Program Management (PM)

The program management controls are implemented at the organizational level and are addressed through the *CNCS Cybersecurity Control Families*, this policy and other relevant documentation.

3.3.2. Access Control (AC)

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. Please refer to *CNCS Cybersecurity Control Families* for further details regarding established CNCS access control measures.

3.3.2.1 Acceptable Use

All CNCS users must sign and accept the CNCS Rules of Behavior (ROB) prior to gaining access to CNCS systems and resources, and re-sign annually. The intent of the ROB is to provide guidance for all CNCS employees, contractors, interns/temporary employees, and volunteer personnel

concerning information and personal security. By signing the ROB, users certify they have completed all required user training, and have read and understood the Cybersecurity ROB agreement.

All privileged users must sign the CNCS Privileged Users Agreement and Rules of Behavior and re-sign it annually.

3.3.3. Awareness and Training (AT)

The Federal Information Security Modernization Act 2014 Act (FISMA)³ requires each federal agency to provide mandatory annual information security training to all personnel, including contractors and other users of information systems, involved in the use or management of federal computer systems. Further, the Office of Management and Budget (OMB) Circular A-130, Appendix III, requires that such training be completed prior to the granting of access, and be provided as periodic refreshment. CNCS provides this required security awareness training to all CNCS users (including managers, senior executives, and contractors) prior to granting network access, and annually thereafter. Users with elevated privileges, referred to as privileged users, will be provided enhanced security training applicable to their role as a privileged user. Additionally, users assigned a specific cybersecurity role for CNCS systems, e.g. ISSM, ISSO, etc., will be provided security role-based training.

Refer to

Table 1: Cybersecurity Training Requirements for cybersecurity training details.

Table 1: Cybersecurity Training Requirements

Type	Objective	Required Participation
Cybersecurity User Training, including Privacy and Phishing	Understanding of information security and privacy policies	All
Role Based Cybersecurity Training	Provide users with significant cybersecurity responsibilities an understanding of their roles and responsibilities for ensuring information systems operates at acceptable level of risk.	Individuals with program level security roles ⁴
Elevated Privileges Training	Provide privileged users an understanding of their roles and responsibilities as a privileged user, and the importance of safeguarding access to CNCS system resources	Individuals with elevated program/system level roles

³ 44 U.S. Code § 3544.

⁴ Program levels roles include: CIO, CISO, AO, ISO, ISSO, and system/software developers.

3.3.4. Audit and Accountability (AU)

Audit logs are used to investigate security incidents, monitor any and all use of CNCS resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. Accordingly, automated audit logs of access to CNCS information systems must be maintained. Audit trails must provide sufficient information to, at a minimum, establish the type of event, when the event took place (i.e. date and time), where the event occurred, the source of the event, and the outcome of the event. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding established CNCS audit control measures.

3.3.5. Certification, Accreditation, and Security Assessments (CA)

CNCS will perform security assessment of its information systems in accordance with the FISMA.⁵ CNCS will adhere to NIST security authorization guidance as set forth in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, as amended, and subsequent publications. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for assessment and authorization procedures.

3.3.6. Configuration Management (CM)

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. 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.

Please refer to the *CNCS Cybersecurity Control Families* for specific details and procedures regarding established CNCS measures for configuration management and change control.

3.3.7. Contingency Planning (CP)

CNCS has developed and formally documented a contingency planning policy, *CNCS Continuity of Operations Plan (COOP)*, as amended. The COOP is reviewed annually and updated, as necessary, to ensure it is applicable to the CNCS environment and compliant with applicable federal laws, directives and policies, regulations, standards, and guidance.

The COOP outlines the major activities CNCS will perform to ensure it can maintain or resume operations within a reasonable time during and after a wide range of emergencies, including localized acts of nature, accidents and technological failures, or attack-related emergencies. The COOP addresses how CNCS will continue data processing if services, use, or access is disrupted for an extended period of time.

⁵ 44 U.S. Code § 3544(b)(1).

Please refer to the *CNCS Continuity of Operations Plan (COOP)* for specific details regarding CNCS established policy and procedures for contingency and disaster recovery.

3.3.8. Identification and Authentication (IA)

CNCS will establish unique identifiers, e.g. user name and password, for all CNCS users accessing CNCS information resources. 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). Please refer to *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for identification and authentication.

3.3.9. Incident Response (IR)

CNCS has developed and formally documented the *CNCS Incident Response Plan*, as amended. The plan, is reviewed annually and updated, as necessary, to ensure its applicability to the CNCS environment and compliant with applicable federal laws, directives and policies, regulations, standards, and guidance. Please refer to the *CNCS Incident Response Plan* for further details regarding established CNCS measures for incident reporting and handling.

3.3.10. Maintenance (MA)

CNCS information system resources are maintained in accordance with industry best practices to ensure their availability, integrity, and confidentiality. 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. Please refer to *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for system maintenance.

3.3.11. Media Protection (MP)

CNCS data is stored on a variety of media and 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, and provide staff with guidance as to how IT property is purchased, installed, loaned, tracked, and disposed of by the agency. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding media protection and management.

3.3.12. Physical and Environmental Protection (PE)

CNCS will limit physical access to information systems, equipment, and the respective operating environments to authorized individuals. 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. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding physical and environmental protection.

3.3.13. Planning (PL)

CNCS has developed and formally documented a policy and procedures policy, *Preparing Policies and Procedures*, as amended. The policy is reviewed annually and updated, as necessary, to ensure it is applicable to the CNCS environment and compliant with applicable federal laws, directives and policies, regulations, standards, and guidance. OIT adheres to this policy and will ensure that all OIT-specific policies and procedures are developed in accordance with this policy.

NIST 800-53, as amended, requires all systems and applications have a documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. Accordingly, all CNCS systems must have a documented System Security Plan (SSP). Please refer to *CNCS Cybersecurity Control Families* for further details regarding CNCS established policy and procedures for system security planning.

3.3.14. Personnel Screening for Information and Information System Access (PS)

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. Please refer to *CNCS Cybersecurity Control Families* for further details regarding CNCS established policies and procedures for personnel screening.

3.3.15. Risk Assessment (RA)

CNCS will use NIST SP 800-39, *Managing Information Security Risk Organization, Mission and Information System View*, as the guidance for 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. Risk management procedures must be integrated into the System Development Lifecycle (SDLC) for each CNCS information resource. Security considerations must be included in the initiation, development/acquisition, implementation, operation/maintenance, and disposal of all CNCS information resources. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding CNCS policy and procedures for risk management.

3.3.16. System and Services Acquisition (SA)

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 Federal Information Processing Standards (FIPS) 199 security category of the

system covered by the contract. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding established CNCS measures for system and service acquisitions.

3.3.17. System and Communications Protection (SC)

CNCS monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding system boundary protection.

3.3.18. System and Information Integrity (SI)

CNCS will adhere to patch management and maintenance guidance as set forth in NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, and subsequent publications. 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. Please refer to the *CNCS Cybersecurity Control Families* for further details regarding system integrity.

APPENDIX A: Applicable Laws and References

This Cybersecurity Policy is in accordance with laws, directives, Executive Orders, requirements, and guidance that include the following:

- 44 U.S.C. § 3501, et. seq.; 44 U.S.C. §§ 3601-3606 (E-Government Act of 2002 (Pub. L. 107–347 (2002))
- 44 U.S.C. § 3541 et seq. (*Federal Information Security Modernization Act 2014 Act of 2002 (FISMA)*) (as amended)
- 18 U.S.C. § 1030 (*Computer Fraud and Abuse Act*)
- 5 U.S.C. § 552a (*The Privacy Act of 1974*)
- Standards prescribed under 40 U.S. C. § 11331.
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 2015
- OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 2015
- OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, October 2014
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013
- OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Modernization Act 2014 Act and Agency Privacy Management*, September 2012
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007
- OMB Memorandum, A-130, Appendix III, *Management of Federal Information Resources*, November 2000
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006
- 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
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*
- NIST SP 800-16 (as amended), *A Role-Based Model for Federal Information Technology / Cyber Security Training*
- NIST SP 800-39 (as amended), *Managing Information security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40 (as amended), *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations*

- NIST SP 800-53A (as amended), *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
- NIST SP 800-60 Volume I Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-60 Volume II Revision 1, *Appendices to Volume I, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61 (as amended), *Computer Security Incident Handling Guide*

APPENDIX B: Acronyms and Abbreviations

Acronym	Acronym Definition/Name/Title
AO	Authorizing Official
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CNCS	Corporation for National & Community Service
COO	Chief Operating Officer
COR	Contracting Officer's Representative
FISMA	Federal Information Security Modernization Act 2014Act
FOIA	Freedom of Information Act
IA	Information Assurance
IAM	Information Assurance Manager
IAP	Information Assurance Program
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology

CNCS Cybersecurity Policy

Acronym	Acronym Definition/Name/Title
NARA	National Archives and Records Administration
NIST	National Institute of Standards & Technology
OGC	Office of General Counsel
OHC	Office of Human Capital
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPS	Office of Personnel Security
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POAM	Plan of Action and Milestones
POC	Point of Contact
ROB	Rules of Behavior
SAOP	Senior Agency Official for Privacy
SDLC	System Development Lifecycle
SORN	System of Records Notice
SP	Special Publication

Acronym	Acronym Definition/Name/Title
SSP	System Security Plan
SSN	Social Security Number
ST&E	Security Test and Evaluation
VPN	Virtual Private Network