



Corporation for National & Community Service (CNCS)

Office of Information Technology

INFORMATION ASSURANCE

PROGRAM

November 2012

Table of Contents

- 1. Information Assurance Program 1**
 - 1.2 What are the objectives of the IAP?1
 - 1.3 Who is responsible for developing and reviewing the IAP and policies?1
 - 1.4 Who must comply with these policies?1
 - 1.5 Are systems owned by a contractor required to comply with these policies?1
 - 1.6 Are there consequences for not complying with these policies?1
 - 1.7 What is required if a policy or a section of policy cannot be implemented?.....2
 - 1.8 Is progress in meeting system security and privacy requirements reported?.....2
 - 1.9 Where can I find more information about the IAP and the policies in this document?.....2
- 2. Roles and Responsibilities..... 3**
 - 2.1 Chief Executive Officer (CEO)3
 - 2.2 Chief Information Officer (CIO)3
 - 2.3 Chief Information Security Officer (CISO).....3
 - 2.4 Authorizing Official (AO)4
 - 2.5 Information System Owner (ISO).....4
 - 2.6 Information Owner (IO)5
 - 2.7 Information System Security Officer (ISSO)6
 - 2.8 Information Assurance Manager (IAM)6
 - 2.9 Information System Security Manager (ISSM)6
 - 2.10 Contracting Officer’s Representative (COR)7
 - 2.11 Security Assessment Team (SAT).....7
- 3. System Security Policies..... 8**
 - 3.1 System Security Controls9
 - 3.2 IA Awareness and Training10
 - 3.3 Personnel Screening for Information and Information System Access12
- 4. Privacy Policies 15**
 - 4.1 Privacy Act Requirements16
 - 4.2 Employee Responsibilities under the Privacy Act.....18
 - 4.3 Determining the Sensitivity Level of Personally Identifiable Information (PII)20
 - 4.4 PII Collection Requirements.....22
 - 4.5 Privacy Impact Assessment (PIA)24
 - 4.6 Accounting and Disclosures of Privacy Information.....25
 - 4.7 Privacy Notices (SORNs and Privacy Act Statements).....27
 - 4.8 Information Sharing with Third Parties29
 - 4.9 De-identification of PII for Use in Testing, Training, and Surveys.....30

4.10	Privacy Policies on Websites.....	31
4.11	Computer Data Matching	33
4.12	Data Extracts Policy	34
5.	Program Management Policies.....	35
5.1	IA Program Management	36
Appendix A: References.....		39
Appendix B: Acronyms and Abbreviations		40
Appendix C: Glossary		41

1. Information Assurance 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](#)). To meet these requirements, CNCS has developed an Information Assurance Program (IAP) based on a risk and cost/benefit approach to secure information systems and protect privacy information.

1.2 What are the objectives of the IAP?

The objective of this document is to establish an IAP that:

- Protects Privacy and Business Sensitive Information
- Implements Best Security Practices Based on a Risk and Cost/Benefit Approach
- Implements a More Efficient and Less Burdensome System Authorization Process
- Leverages Continuous Monitoring to Improve Awareness of Threats and Risks
- Provides Training and Awareness to Promote a Better Understanding of the IAP and IA Policies

1.3 Who is responsible for developing and reviewing the IAP and policies?

The Chief Information Security Officer (CISO) is responsible for developing and maintaining CNCS's IAP and IA policies. The IAP and IA policies are reviewed and updated annually to address changes and problems identified during plan implementation, audits, Federal Information Security Management Act (FISMA) reviews, or security control assessments. The IAP and associated policies in this document are forwarded to the Chief Information Officer (CIO) and policy council for review and when complete submitted to the Chief Executive Officer (CEO) for approval.

1.4 Who must comply with these policies?

These policies apply 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.

1.5 Are systems owned by a contractor required to comply with these policies?

Yes. To the extent that contractor, state, or grantee systems process, store, or house CNCS information (for which CNCS continues to be responsible for maintaining control), they must comply with these policies and implement system security controls which must be assessed against the same NIST criteria and standards used by Federal agencies.

1.6 Are there consequences for not complying with these policies?

Violation of these policies 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.

1.7 What is required if a policy or a section of policy cannot be implemented?

Waivers for delaying, changing, or not implementing a control must be submitted to the CISO. The CISO will ensure that a risk management review is conducted and includes involvement from senior management providing the strategic vision and top-level goals and objectives for CNCS; to mid-level managers planning, executing, and managing projects; to individuals on the front lines operating the information systems and supporting CNCS's mission/business functions.

1.8 Is progress in meeting system security and privacy requirements reported?

Yes, reports are made annually to the Office of Management and Budget (OMB) and Congress to demonstrate accountability with regulatory system security and privacy program mandates.

1.9 Where can I find more information about the IAP and the policies in this document?

The IA SharePoint site provides a resource site with procedures and templates for policies in this document.

2. Roles and Responsibilities

The following sections describe the roles and responsibilities of key participants involved in the IAP.

2.1 Chief Executive Officer (CEO)

The CEO is responsible for ensuring that the IAP 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 IAP. In support of the IAP, the CEO ensures that the CIO and CISO positions are filled and appoints an Authorizing Official (AO) and Information System Owner (ISO) for each information system.

2.2 Chief Information Officer (CIO)

The CIO¹ is responsible for the execution of CNCS's overall IT program and delegates authority to the CISO for the management of the IAP. The CIO is the focal point for IT management and governance of IT portfolios and is responsible for:

- Ensuring information security management processes are integrated with strategic and operational planning processes.
- Ensuring CNCS has trained personnel sufficient to assist in complying with the information assurance requirements in related legislation, policies, directives, instructions, standards, and guidelines.
- Coordinating with senior management to report annually to the head of the federal agency on the overall effectiveness of CNCS's IAP, including progress of remedial actions.

2.3 Chief Information Security Officer (CISO)

The CISO² carries out the CIO's security and privacy responsibilities under FISMA and is responsible for managing the IAP. The CISO must: (i) possess professional qualifications, including training and experience, required to administer the IAP 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 in accordance with FISMA and Privacy Act requirements. The CISO is responsible for:

- Developing an organization-wide IAP that provides adequate security for all CNCS information and information systems.
- Centralized reporting of information security-related activities.
- Developing and maintaining information security and privacy policies.
- Defining CNCS-specific security requirements, tools, templates, and checklists to support the IAP.

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

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

- Ensuring that personnel with significant system security responsibilities are adequately trained.
- Assisting senior management concerning their security responsibilities.
- Ensuring the implementation of information privacy and security protections as required by the Privacy Act, FISMA, and OMB memoranda.
- Monitoring security incidents and providing assistance when required.
- Managing the Office of Information and Technology (OIT) audits and program reviews and supporting Office of the Inspector General (OIG) investigations.
- Reporting to the CIO and other senior management on the effectiveness of CNCS's IAP and developing and submitting the annual FISMA report.

2.4 Authorizing Official (AO)

The AO is appointed by the CEO and 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), and plans of action and milestones (POA&Ms). 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:

- Ensuring the security posture of the Agency's information systems is maintained.
- Reviewing security status reports and security documents and determining if the risk to the Agency of operating the system remains acceptable.
- Reauthorizing information systems when required.
- Assisting in CNCS's response to security incidents and privacy breaches.
- Appointing, when required, a designated representative to coordinate and carry out system security responsibilities³.

2.5 Information System Owner (ISO)

The ISO is appointed by the CEO and serves as the focal point for the information system and is the central point of contact during the security authorization process. The ISO is responsible for:

- Coordinating data protection requirements with Information Owners (IOs) that have information stored and processed in the system.
- Deciding, in coordination with the IO and Information System Security Officer (ISSO), who has access to the system.

³ The Authorizing Official's Designated Representative (AODR) can be empowered to act on behalf of the AO in security authorization activities for which the AO is responsible with the following exceptions: (i) making the system authorization decision, and (ii) signing the system authorization decision letter.

- Determining access privileges and rights to the system.
- Ensuring that system users and support personnel receive the required security training (e.g., instruction in the Rules of Behavior).
- Ensuring that the system is compliant with the required security controls.
- Appointing an ISSO for the information system to carry out the day-to-day security responsibilities.
- Reviewing system security documents (e.g., SSP, POA&M, etc.).
- Ensuring that system-specific security training is provided to the users and administrators of the systems.
- Ensuring that remediation activities for the system are performed as needed to maintain the authorization status.
- Appointing an Information System Security Manager (ISSM) to coordinate system security task and provide oversight responsibilities to ensure security activities are performed.

2.6 Information Owner (IO)

The IO is a CNCS official with regulatory, management, or operational authority for specified information and is responsible for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.⁴ The IO is responsible for:

- Providing input to ISOs regarding the security requirements and controls for the systems where the information is processed, stored, or transmitted.
- Retaining information in accordance with the National Archives and Records Administration (NARA) record schedule.
- Categorizing the sensitivity level⁵ of the information stored and processed in the system.
- Establishing rules for appropriate use and protection of the information.⁶
- Coordinating with the ISO when security requirements change.
- Assisting in the response to security incidents.
- Ensuring that the PII inventory is updated.

⁴ Federal information is an asset of the Nation, not of a particular federal agency or its subordinate organizations. In that spirit, many federal agencies are developing policies, procedures, processes, and training needed to end the practice of information ownership and implement the practice of information stewardship. Information stewardship is the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.

⁵ See Privacy Policy 4.2 for details about determining the sensitivity of information.

⁶ Rules of behavior, access control procedures, role matrix with separation of duties/least privilege association

2.7 Information System Security Officer (ISSO)

The ISSO is appointed by the ISO and works closely with the ISO or ISSM to ensure that the appropriate security posture is maintained for the information system. 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. This ISSO supports activities at the system level and includes, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The ISSO is responsible for:

- Ensuring system compliance with security policies and procedures.
- Managing and controlling changes to the system.
- Assessing the security impact of any changes.
- Monitoring the system and its environment.
- Developing and updating the SSP.
- Coordinating with and supporting the ISO with security responsibilities.
- Preparing or overseeing the preparation of system security documents⁷ and security activities.
- Developing security policies and procedures that are consistent with CNCS's IA policies.
- Performing or overseeing remediation activities to maintain the authorization status.
- Assisting the ISO assemble the security authorization package for submission to the AO.
- Assisting in the investigation of security incidents.

2.8 Information Assurance Manager (IAM)

The IAM serves as the primary liaison for the CISO to individuals with security and privacy responsibilities and supports activities at the IAP level. The IAM is responsible for:

- Monitoring compliance with Federal requirement and CNCS IA policies.
- Providing guidance on the implementation of IA policies.
- Providing security and privacy training.
- Investigating system security and privacy incidents.
- Providing support for audits and reviews.
- Managing the vulnerability management program.

2.9 Information System Security Manager (ISSM)

The ISSM (Federal employee) coordinates system security task and provide oversight responsibilities to ensure security activities are performed and serves as the liaison between the

⁷ Documents include the system security plan, POA&M, security impact analysis, privacy impact assessment, monitoring strategy, etc. Activities include annual reviews, mitigation of system vulnerabilities, etc.

Information System Security Officer (ISSO) and the Information System Owner (ISO). In these situations, the ISSO (contractor) coordinates directly with the ISSM for all system security-related issues. The ISSM is responsible for:

- Providing oversight of system security activities performed by the ISSO.
- Acting as the liaison between the IAM and the ISSO.
- Monitoring system compliance with CNCS Information Assurance policies and federal guidance.

2.10 Contracting Officer's Representative (COR)

The COR⁸ is nominated by the Agency and assists the Contracting Officer (CO) by performing the following functions:

- Acting as a technical liaison between the CO and the contractor.
- Providing technical assistance.
- Performing onboarding and off boarding activities for the contractors assigned to the contract.
- Ensuring that contractors have the proper background investigations before accessing CNCS information or systems.
- Ensuring that contractors properly maintain information and information systems in accordance with the IAP.

2.11 Security Assessment Team (SAT)

The SAT conducts assessments of the security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., 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). The SAT is responsible for:

- Developing a security assessment plan for each subset of security controls that will be assessed.
- Submitting the security assessment plan for approval prior to conducting the assessment.
- Conducting the assessment of security controls as defined in the security assessment plan.
- Providing an assessment of the severity of weaknesses or deficiencies discovered in the information system.
- Recommending corrective actions to address identified vulnerabilities.
- Preparing the final security assessment report containing the results and findings from the assessment.

⁸ The COR may also be a ISSM.

3. System Security Policies



3.1 System Security Controls

What is the purpose of this policy?

The purpose of this policy is to outline the controls that must be employed within an information system. These controls protect the confidentiality, integrity, and availability of the information processed in the information system.

What are the threats if this policy is not followed?

Trustworthy information systems are systems that are capable of operating despite the environmental disruptions, human errors, structural failures, and intentional attacks that are expected to occur in any environment. The controls listed in the table below play a critical part in achieving trustworthy information systems—systems that have the reliability to successfully carry out assigned missions/business functions.

What controls must be implemented?

The following table provides a list of the controls that must be implemented within an information system. The controls selected and implemented for an information system depend on the security impact of the system (Moderate or Low). The information system must have documented procedures for each control family that explains how the controls are implemented. Procedures must be maintained in the IA SharePoint repository, updated when changes occur, and reviewed annually. Select the Moderate or Low link to view the controls that must be implemented for the information system.

Table 1: System Security Controls

Security Control Family	Security Controls Link
Access Control	<u>Contact CNCS IA for a copy of the System Security Control Spreadsheet</u>
Audit and Accountability	
Security Assessment and Authorization	
Configuration Management	
Contingency Planning	
Identification and Authentication	
Incident Response	
Maintenance	
Media Protection	
Physical and Environmental Protection	
Planning	
Risk Assessment	
System and Communication Protection	
System and Information Integrity	

What is required if a security control cannot be implemented or needs to be modified?

Waivers for delaying, modifying, or not implementing a control must be submitted to the CISO. The CISO will ensure that a risk-based review is conducted and forwarded to the AO and CIO for a decision.

3.2 IA Awareness and Training

What is the purpose of this policy?

The purpose of this policy is to ensure that training and awareness is provided so that individuals understand information security and privacy requirements.

Who is responsible for developing and implementing IA awareness and training?

The CISO is responsible for developing and implementing a program level training and awareness program. The ISO is responsible for ensuring that system specific training is developed and implemented at the system level.

What are the types of training I must take and how often am I required to take them?

Refer to the following table for program and system specific types of training that must be taken and the frequency.

Table 2: IA Training Requirements

TYPE	OBJECTIVE	FREQUENCY	TRAINING PROVIDER	REQUIRED PARTICIPATION
PROGRAM LEVEL TRAINING				
Security Training	Understanding of information security and privacy policies.	1) Annually 2) When changes are made to policy	CISO	All
Security Awareness	Basic understanding of how to respond to risk.	1) Annually	CISO	All
Security Role-Based Training	To carry out IA risk management roles at the program level (e.g., AO, ISO, ISSO, etc.).	1) Initial training 2) Annually	CISO	Individuals with Program level Security Roles ⁹
SYSTEM SPECIFIC LEVEL TRAINING				
System Specific Security Training	Understanding of system specific security and privacy procedures. (e.g., Rules of Behavior)	1) Initial training (before access to systems or information) 2) When changes are made to procedures 3) Annually	ISO	All
Security Role-Based Training	Provides security-related training specifically tailored for their assigned duties at the system level (e.g., Incident Response training, etc.).	1) Initial training (before performing duties) 2) Policy is changed 3) Annually	ISO	Individuals with Security Roles ¹⁰

Is IA training recorded and maintained?

Yes, training at the program level and the system level must be recorded and maintained for at least three years.

⁹ Program levels roles include: CIO/Risk Executive, CISO, AO, ISO, IO, ISSO, security control assessors, system/software developers, acquisition/procurement, and Users.

¹⁰ System level roles include: AO, ISO, IO, ISSO, system/network administrators, security control assessors, system/software developers, and other personnel having access to system-level software.

What training is needed for contractors?

Contractors are required to take the IAP program level training and are responsible for developing, implementing, and taking system-specific training.

Is a CNCS network account needed to take the security/awareness and role-based training?

No, all IA training can be taken from outside the CNCS network. Send an email to InformationAssurance@cns.gov for a training account and instructions.

3.3 Personnel Screening for Information and Information System Access

What is the purpose of this policy?

The purpose of this policy is to establish requirements for screening individuals participating in the design, development, operation, or maintenance of systems and applications, as well as those requiring access to CNCS information.

Are there different levels of screening?

The level of screening varies from minimal checks to full background investigations, depending on the sensitivity of the information to be handled and the risk and magnitude of loss or harm that the individual could cause by accessing the information.

What are the levels of screening?

Every position within CNCS must be designated at either a High, Moderate, or Low level risk, as determined by the position's potential for adverse impact on the Agency's mission.

Who determines the level of screening?

The Office of Personnel Security (OPS) develops, implements, and administers CNCS's personnel security, suitability, and investigation processes. The CISO is responsible for identifying risk levels to OPS for access to information and Information systems.

What are the position risk levels?

The risk level, description, position, and the required background investigation are listed in the table below.

Table 1: Background Investigation Requirements

Risk Level	Risk Level Description	Positions	Required Background Investigation
High	Includes positions at the highest level of risk to the information or information system. This includes positions in which the individual: <ul style="list-style-type: none"> Is responsible for the planning, direction, and implementation of a computer security program. Has a major responsibility for the direction, planning, and design of an information system, including the hardware and software. Can access a system during the operation or maintenance in such a way as to incur a relatively high risk of causing grave damage or realizing a significant personal gain. 	CIO CISO IAM Criminal Investigators Personnel Security Specialist CFO COO	BI
Moderate	Includes positions at a moderate level of risk to the information system. The individual is responsible for the direction, planning, design, operation, or maintenance of a information system, but the work is	Program Managers System/ Database	MBI

	<p>technically reviewed by a higher authority at the high level to ensure the integrity of the system. Such positions involve:</p> <ul style="list-style-type: none"> • Major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and management of systems hardware and software. • Elevated system or application privileges on a system categorized as Moderate. • System, code, or application development responsibilities on systems categorized as Moderate. • Broad financial or internal control responsibility directly involving the accounting, disbursement, or authorization for disbursement from systems. • Autonomous purchasing authority. 	<p>administrators ISSO Security Control Assessors Code Developers Customer Agents¹¹</p>	
Low	<p>Includes positions not falling into one of the above risk levels. Such positions involve:</p> <ul style="list-style-type: none"> • Standard access to CNCS systems and information. • Elevated system or application privileges on systems categorized as Low. • System, code, or application development responsibilities on systems categorized as Low. • Limited financial control responsibility/purchasing authority. 	<p>Program Managers System Users System/Database Administrator ISSO Security Control Assessor Code Developers System Users</p>	NACI
Low	<p>Includes access <i>that will not exceed 180 days</i> and access is limited to non-sensitive information.</p> <p><i>Note: Controls must be in place to ensure that these individuals do not have access to sensitive (i.e., Privacy information, Financial, or other sensitive information). If a compelling need requires access to sensitive information, a waiver must be submitted to the CISO with details of the mitigating controls in place to protect the sensitive information. The waiver must be approved by the CIO, AO, ISO and IO before access is provided.</i></p>	<p>Interns Contractors Members System Users</p>	Limited Access (Agency Check)

Can access to CNCS information or information systems be granted before the investigation is completed?

¹¹ Individuals providing customer support and have access to PII.

Yes, temporary access will be granted for standard access upon confirmation that the required background investigation documentation has been submitted to OPS. **Note:** Individuals must not be given roles in applications (e.g., Trust, Momentum, etc.) that will allow them to access PII until a completed investigation by OPM has been received.

Can individual's requiring elevated privileges have access before the investigation is completed?

Yes, individuals requiring elevated privileges (e.g., system administrators, system developers) must submit a credit report, Commercial Background Investigation (CBI), and background investigation documentation to OPS before privileges are granted.

Note: Individuals requiring access to PII (e.g., database administrators, customer agents, etc.) must not be given privileges that will allow them to access PII until a completed investigation by OPM has been received.

4. Privacy Policies



4.1 Privacy Act Requirements

What is privacy?

Privacy is the right of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Why do we need this policy?

An awareness of the Privacy Act requirements will reduce the risk of being in violation of the law.

What is the Privacy Act?

The Privacy Act is a federal law that balances the Government's need to maintain information about individuals with the right of the individuals to be protected against unwarranted invasions of their privacy. The Privacy Act establishes special requirements required by statute or Executive order which authorizes the Government to collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other identifier (whether in paper or electronic form). The Privacy Act guarantees individuals three primary rights:

- (1) The right to view records about oneself, subject to the Privacy Act's exemptions.
- (2) The right to amend a nonexempt record if it is inaccurate, irrelevant, untimely, or incomplete.
- (3) The right to sue the government for violations of the Privacy Act, such as permitting unauthorized individuals to read an individual's records.

Who is responsible for complying with the above Privacy Act requirements?

Everyone who: (i) handles information on individuals; (ii) responds to requests for information in a system of records, or about individuals; (iii) collects information and files it by name or unique identifier; and (iv) manages a database with information on individuals.

What are the Privacy Act requirements?

The Privacy Act core requirements are:

- (1) Limitations on the collection, use and dissemination of PII about an individual.
- (2) Disclosure restrictions to third parties.
- (3) Access and amendments rights of the individuals who are subjects of the files.
- (4) Notification to the public about information collections that create a system of records (obtained through paper forms or Web sites), and publishing the system of records notice in the Federal Register. Secret records on individuals cannot be maintained.
- (5) Requirements for data collection include determining answers to the following questions:
 - Is the information relevant and necessary?
 - Is the information accurate, timely, and complete?
 - Is the information collected directly from the subject?
 - Is there a notice addressing the purpose and use of the information?
 - Are safeguards in place to protect the integrity of the information?

- (6) Interagency data sharing requirements apply when matches are made with another Federal or state government agency when the matches are used to verify an initial eligibility for federal benefits programs.

4.2 Employee Responsibilities under the Privacy Act

What is the purpose of this policy?

The purpose of this policy is to provide direction for handling PII.

How can I protect PII?

Consider how you handle the information you work with, and what measures you need to take to safeguard the personal information that you have about others. Safeguarding requirements include:

- Storing paper records in a locked room or file cabinet.
- Storing electronic records in folders limited to only those individuals with a legitimate need to access the information.
- Transferring PII only to mobile devices that are encrypted.
- Never placing privacy or sensitive Agency data on a personal computer or on personal mobile devices.
- Accessing PII through the VPN¹² when teleworking and ensuring that you protect the information while working from home from inadvertent viewing.
- When disclosing Privacy Act information to others:
 - Be careful that personal information is not disclosed to anyone unless that individual has received prior permission to see the information from the subject of the record, or disclosures of the record are authorized by law. Under the law, only employees who have a legitimate need in the performance of their duties may have access to the information. Even if you may have legitimate access, sharing information on individuals to others who do not have a legitimate need to know the information and would not have access to this information otherwise is a violation of the law
 - When the subject of the file requests to inspect or obtain information that is in a Privacy Act System of Records direct the requestor to consult CNCS's Privacy Act regulations available at [45 C.F.R. §§ 2508.1 - .20](#).
- When Collecting Personal Information:
 - Employees may collect only personal information from an individual that is relevant and necessary to accomplish an authorized business function. When personal information is collected you must inform the individual in writing¹³ of the:
 - Legal authority
 - Purpose for collecting it

¹² Ensure that you never place PII on your personal computer. PII must stay within protected CNCS boundaries.

¹³ The information above is usually provided in a Privacy Act Statement given to the person providing the information. See CNCS Privacy Policy 4.7 for details.

- What related uses will be made of this information
- Whether a response is mandatory or voluntary, and
- The effect if they refuse to respond

Note: See CNCS Privacy Policy [4.4, PII Collection Requirements](#) for details about collecting personal information.

4.3 Determining the Sensitivity Level of Personally Identifiable Information (PII)

What is the purpose of this policy?

The purpose of this policy is to ensure that the sensitivity level of the PII is determined so that it can be properly protected.

What is PII?

PII is defined in OMB Memorandum M-07-16 as “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”

The definition of PII was further defined in OMB Memorandum M-10-23, that “PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.”

What are the risks to individuals and CNCS if PII is compromised?

If the information breached is sufficient to be exploited by identity thieves, individuals can suffer from a loss of money, damage to credit, a compromise of medical records, threats, and/or harassment. CNCS may also suffer financial losses in compensating the individuals, assisting them in monitoring their credit ratings, or addressing administrative concerns, and our public reputation and public confidence may be damaged. If a loss of PII constitutes a violation of relevant law, the Agency and/or its staff may be subject to criminal or civil penalties.

What are some examples of PII?

Provided below is a baseline of types of PII and corresponding confidentiality impact levels:

Table 3: PII Confidentiality Impact Level

Type	Example	Confidentiality Impact Level
Name:	Full name, maiden name, mother’s maiden name, or alias	Low
Personal Identification Numbers:	SSN, passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number	High
Telephone Numbers:	Mobile, business, and personal numbers	Low
Personal Characteristics:	Photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry)	Low
Information Identifying Personally Owned Property:	Vehicle registration or identification number, title numbers, and related information	Low or Mod

Information About an Individual That Is Linked Or Linkable To One Of The Above:	Date of birth, place of birth, or financial information.	Mod or High
Information About an Individual That Is Linked Or Linkable To One Of The Above:	Race, religion, weight, activities, employment information, or education information	Low or High

What is the confidentiality impact level in the chart above based on?

The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or CNCS if PII were inappropriately accessed, used, or disclosed.

Who decides the confidentiality impact level?

The *IO* considers relevant factors that might indicate a different impact level than those listed in the table above. Factors that the Information Owners must keep in mind are:

- (1) **Aggregation and Data Field Sensitivity.** The IO must evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields when combined. For example, an individual’s SSN or financial account number is more sensitive than an individual’s phone number or zip code.
- (2) **Context of Use.** The IO must also assess the context of use because it is important to understanding how the disclosure of data elements can potentially harm individuals and the CNCS. Consider what harm is likely to be caused if the PII is disclosed (either intentionally or accidentally). Examples of context include: statistical analysis, determining eligibility for benefits, administration of benefits, and research.

4.4 PII Collection Requirements

What is the purpose of this policy?

The purpose of this policy is to ensure compliance with the Privacy Act and to protect individual's privacy by ensuring that before collecting PII: (i) there is a legal authority for collecting the PII; (ii) the purpose(s) for which the PII is collected is specified in the notice; (iii) a SORN is developed and published in the Federal Register, (iv) Privacy Act Statements are developed; and (v) the CNCS PII Inventory is updated.

What must I do before I collect PII?

Before collecting PII you must:

- (1) **Determine Authority to Collect** - Determine the legal authority that permits the collection, use, maintenance and sharing of PII. You must consult with the Office of General Counsel regarding the authority of any program or activity to collect PII. The authority to collect PII must be documented in the System of Records Notice (SORN).
- (2) **Determine What PII Will Be Collected** – Determine what PII will be collected to meet the requirements. Only collect what is necessary.
- (3) **Develop Purpose Specification** - Describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.¹⁴
- (4) **Identify an Existing SORN or Develop and Publish a New SORN**¹⁵ – Identify or develop a SORN for each system of records containing PII. The purpose of a SORN is to inform the public what types of records the agency maintains, who the records are about, and what uses are made of them. Accurate SORNs must be published in the Federal Register. Visit the IA SharePoint Resource Site for the steps to develop and submit a SORN for publication.
- (5) **Develop Privacy Act Statements**¹⁶ – Develop Privacy Act Statements if PII is collected using forms. Visit the IA SharePoint Resource Site for the steps to develop and request approval for a PII collection form.
- (6) **Develop a Privacy Impact Assessment (PIA)**¹⁷ – Conduct a PIA analysis to assess the privacy risk to individuals that may result from collecting, sharing, storing, transmitting, or using PII within an information technology system.
- (7) **Update the CNCS PII Inventory** – Update the CNCS inventory to indicate the type, location, and point of contact for the PII.

Are there related maintenance activities I must perform?

Yes, to ensure that only PII identified in the SORN is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose, an evaluation of PII holdings must reviewed annually. The collection must be reviewed to ensure that only PII

¹⁴ Privacy documentation includes, but is not limited to, Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements if forms are uses to collect PII.

¹⁵ See [Privacy Policy 4.7 Privacy Notices](#) for details.

¹⁶ See [Privacy Policy 4.7 Privacy Notices](#) for details.

¹⁷ See [Privacy Policy 4.5 Privacy Impact Assessment](#) for details.

identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

What do I do if I no longer need the information collected?

NARA provides retention schedules that govern the disposition of federal records containing PII. If the collection is no longer needed you must retain the PII in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access (e.g., delete Social Security numbers if their use is no longer needed after consultation with the CNCS Records Officer).

How do I destroy the PII if it does not have to be saved or sent to NARA?

Contact the [Information Assurance](#) team at InformationAssurance@cns.gov for deletion methods.

4.5 Privacy Impact Assessment (PIA)

What is the purpose of this policy?

The purpose of this policy is to ensure privacy protections are addressed throughout the development, design, and deployment of information systems by providing an analysis of how PII is collected, maintained, used, and disseminated.

What is a PIA?

A PIA assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, and use of PII in an information system.

Who is responsible for developing the PIA?

The ISO and IO are responsible for ensuring that the PIA is completed.

When are PIAs conducted?

PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks.

Is there a process for conducting and approving PIAs?

Yes, each information system that collects, maintains, or disseminates PII about members of the public must have a PIA as part of its security authorization package.¹⁸ The PIA must be reviewed annually and updated when system changes occur.

¹⁸ The Security Authorization package is submitted to the information system Authorizing Official and the Risk Executive Official to make a risk management decision on whether the system will be authorized to operate.

4.6 Accounting and Disclosures of Privacy Information

What is the purpose of this policy?

The purpose of this policy is to ensure that the required accountings of disclosures of records are properly maintained.

What is a disclosure?

The Privacy Act requires that records may not be disclosed to any third party (including other Federal agencies) without the advance written consent of the person to whom the records pertain. There are, however, exceptions which permit disclosures without the consent of the individual of record. These exceptions are described below.

- (1) **Internal Disclosures** - The first exception to the basic disclosure restriction permits disclosures to officers and employees of CNCS who have a need for the record in the performance of their duties.
- (2) **Disclosures Under the Freedom of Information Act (FOIA)** - The second exception to the Privacy Act's basic disclosure restrictions is for those disclosures which are required by the FOIA. When the FOIA does not require disclosure, however, the Privacy Act disclosure restriction is applicable and provides a further safeguard for the privacy of individual citizens.
- (3) **Routine Use** - Disclosures may be made for routine use as described and published in the SORN describing the system of records.
- (4) **Bureau of the Census** - Disclosures may be made to the Bureau of the Census for purposes of planning or carrying out a census, survey or related activity.
- (5) **Statistical Research/Reporting** - Disclosures may be made to a recipient who has provided the Agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.
- (6) **Preservation of Records** - Disclosures may be made to NARA of a record which has sufficient historical or other value to warrant its continued preservation by the United States Government or for evaluation by the Archivist of the United States or the Archivist's designee to determine whether the record has such value.
- (7) **Civil or Criminal Law Enforcement** - Disclosures may be made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to CNCS specifying the particular portion desired and the law enforcement activity for which the record is sought.
- (8) **Health or Safety** - Disclosures may be made to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.

- (9) **Congressional Disclosure** - Disclosures may be made to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, and joint committee of Congress or subcommittee of any such joint committee.
- (10) **General Accounting Office (GAO)** - Disclosures may be made to the GAO for the purpose of carrying out the duties of that office.
- (11) **Court Order** - Disclosures may be made pursuant to the order of a court of competent jurisdiction. However, a subpoena issued as part of the routine discovery in a court proceeding rather than by a judge as a specific order to produce is not a court order permitting disclosure under this exception.
- (12) **Debt Collection** - Disclosures may be made to a consumer reporting agency in accordance with section 3(d) or the Federal Claims collections Act of 1966 (31 U.S.C. 3701 (a) (3)).

What do I do when I receive a request for information?

Refer to CNCS Policy CEO-2012-01, [Processing Privacy Act Information](#), for detailed instructions.

How long is the accounting of the disclosure kept?

Accounting of disclosures must be retained for the life of the record or five years after the disclosure is made, whichever is longer.

Who do I provide the disclosure too?

All disclosures except those made under the law enforcement exception are to be available to the person named in the record upon request.

4.7 Privacy Notices (SORNs and Privacy Act Statements)

What is the purpose of this policy?

The purpose of this policy is to ensure that the purpose (s), for which PII is collected, used, maintained, and shared is described in privacy notices.

What is a privacy notice?

A privacy notice provides information to individuals regarding: (i) activities that impact privacy, including collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how PII is used by the Agency and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary. Privacy notices include:

- System of Records Notices (SORNs)
- Privacy Impact Assessments ([See Section 4.5 of this document](#))
- Website Privacy Policy ([See Section 4.10 of this document](#))
- Privacy Act Statements¹⁹

What is a SORN?

A SORN provides the public notice regarding PII collected in a system of records, which the Privacy Act defines as “a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier.” The SORN explains how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. SORNs for information systems containing PII must be kept current and published in the Federal Register. The point of contact for each SORN is required to:

- Update the SORN if it does not accurately and completely describe the system of records and its routine uses
- Annually review the SORN and validate its accuracy. (Visit the IA SharePoint Resource Site for the steps to develop and submit a SORN for publication.)

What is a Privacy Act Statement?

Privacy Act Statements are used during the collection of PII to provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. Privacy Act Statements are on forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. The point of contact for collections requiring a Privacy Act Statement must:

¹⁹ As required by the Privacy Act, the Corporation must also provide direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII

- Update the Privacy Act Statement if it does not accurately and completely describe the collection of PII and its routine uses.
- Annually review the Privacy Act Statement and validate its accuracy.

4.8 Information Sharing with Third Parties

What is the purpose of this policy?

The purpose of this policy is to ensure that external sharing of PII to include sharing with other public and private sector entities is reviewed and approved.

What is examined during this review?

The review is to ensure that:

- (1) The sharing of PII is only for the authorized purposes identified in the Privacy Act and/or described in existing CNCS public notice(s) or in a manner compatible with those purposes.
- (2) Where appropriate, the CNCS enters into MOAs/MOUs, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.
- (3) Proposed new instances of sharing PII with third parties are evaluated to determine whether they are authorized and whether additional or new public notice²⁰ is required.

Who are the reviewer and approver?

The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and OGC must review and approve proposed external sharing of PII.

²⁰ Public Notices include: Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), website privacy policies, and other public notices

4.9 De-identification of PII for Use in Testing, Training, and Surveys

What is the purpose of this policy?

The purpose of this policy is to ensure that PII is protected during testing, training, and surveys.

What is de-identification?

De-identified information is when enough PII is masked so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

Is de-identification required for PII used in testing, training, and surveys?

Yes, to minimize the risk of loss or breach of PII it must be de-identified.

How is PII de-identified?

De-identification can be accomplished by removing account numbers, names, SSNs, and any other identifiable information from a set of records. By de-identifying the information, a trend analysis team can perform an unbiased review on those records without compromising the PII or providing the team with the ability to identify individuals.

Another example is used in survey analysis. Remove all of the identifying PII fields and assign a identification to each individual that is associated with a cross-reference table located in a separate system. The only means to reconstruct the original (complete) PII records is through authorized access to the cross-reference table.

Additionally, de-identified information can be aggregated for the purposes of statistical analysis, such as making comparisons, analyzing trends, or identifying patterns. An example is the aggregation and use of multiple sets of de-identified data for evaluating several types of education loan programs. The data describes characteristics of loan holders, such as age, gender, region, and outstanding loan balances. With this dataset, an analyst could draw statistics showing that 18,000 women in the 30-35 age group have outstanding loan balances greater than \$10,000. Although the original dataset contained distinguishable identities for each person, the de-identified and aggregated dataset would not contain linked or readily identifiable data for individuals.

4.10 Privacy Policies on Websites

What is the purpose of this policy?

To ensure that visitors to CNCS websites know what information is collected about them, why it is collected, and how it will be used.

What are the requirements?

Every CNCS web site must include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record. This statement tells the visitors to your site how information they provide is handled.

Why do we need this policy?

Posting a privacy policy helps ensure that individuals have notice and choice about, and thus confidence in, how their personal information is handled when they use the Internet. Federal agencies are required to protect an individual's right to privacy when they collect personal information. This is required by the Privacy Act, 5 U.S.C. 552a, OMB Circular No. A-130, *Management of Federal Information Resources*, 61 Fed. Reg. 6428 (Feb. 20, 1996), OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, and OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*.

What information is required in the privacy policy statement?

Privacy policies must be clearly labeled and easily accessed when someone visits a web site and must:

- (1) Identify when tracking technology is used to personalize the interaction, and explain the purpose of the feature and the visitor's option to decline it.
- (2) Clearly explain when information is maintained and retrieved by a personal identifier in a Privacy Act system of records.
- (3) Clearly explain an individual's rights under the Privacy Act or provide a link to a Privacy Act Statement or SORN²¹ when Privacy Act information is solicited.
- (4) Clearly explain where the user may consent to the collection or sharing of information and notify users of any available mechanism to grant consent.
- (5) Make website privacy policies "readable" by privacy protection technology.
- (6) Explain the use of web measurement and customizing technology²², voluntary nature of, and the safeguards applicable to the customizing device.

Do we need a privacy policy for websites that are not operated by CNCS?

When using a third-party website or application to engage with the public you must forward a request with the third party's privacy policy to the SAOP for approval.

²¹ Information about rights under the Privacy Act may be provided in the body of the web privacy policy or via link to a Privacy Act Statement or published SORN.

²² These technologies are used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience allowing users to customize their settings, avoid filling out duplicative information, and navigate the website more quickly.

If you create a link that leads to a third-party website or any other location that is not managed by CNCS, you must provide to the SOAP your plan to alert visitors, such as a statement adjacent to the link or a “pop-up,” explaining that visitors are being directed to a nongovernment website that may have different privacy policies from those of official CNCS websites.

If you incorporate or embed a third-party application on a CNCS website, you must disclose the third party’s involvement and update the CNCS website privacy policy.

4.11 Computer Data Matching

What is the purpose of this policy?

The purpose of this policy is to establish computer matching requirements.

What is the scope of this policy?

This policy applies to electronic comparison of records which meet the following criteria:

- Records are from two or more automated systems of records maintained by CNCS and/or other Federal agencies, or a contractor on CNCS's behalf.
- Records pertain to applicants, program beneficiaries, or providers of services to programs.
- The purpose of the matching is to establish or verify initial or continuing eligibility for Federal benefit programs; verify compliance with the statutory or regulatory requirements of such programs; or recoup payments or delinquent debts under such Federal benefit programs.
- Matches comparing records from automated Federal personnel or payroll systems of records, or such records with automated records of State and local governments.

Exclusions:

- Statistical matches with the sole purpose of aggregating data stripped of personal identifiers.
- Routine administrative matches using predominantly federal personnel records provided the purpose is not to take adverse action against personnel.
- Law enforcement investigative matches by agencies whose principal function involves enforcement of law.
- Internal matches using only CNCS's own records if the purpose is not to take adverse action against personnel.
- Background investigations.

What are the requirements when computer matching is required?

CNCS has established a Data Integrity Board (DIB) to oversee and coordinate the computer matching program. The board reviews and approves proposed matches, pilot matches, exclusions, extensions, renewals and annually assesses the utility of ongoing programs in terms of their benefits, costs, and reviews.

4.12 Data Extracts Policy

What is the purpose of this policy?

The purpose of this policy is to ensure that data extracts containing sensitive information are erased when they are no longer needed.

Why do we need this policy?

While the use of the computer readable data extracts helps productivity, it also exposes the data to risks. Once data has been extracted, it is no longer protected by all of the security measures and procedures that protected it in the original system. Additional measures must be taken to track and protect these extracts and to ensure that they are erased when they are no longer needed. This reduces the likelihood of sensitive information being breached. This is required by OMB M-7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

What are the requirements of this policy?

Log all computer-readable data extracts from databases that contain sensitive information and verify every 90 days whether each extract, has been erased or its use is still required.

What is a computer-readable data extract from a database?

A computer-readable data extract is when you retrieve data from a database through a query and save the data into a separate computer-readable entity such as another database, a spreadsheet, or a text file.

Which data extracts need to be logged?

All data extracts from databases that contain sensitive information need to be logged.

What information must be maintained on the IA SharePoint site?

The logs must include the following:

- (1) Date and time of the extract.
- (2) Name of the system/database from which the data was extracted.
- (3) Type of extract (spreadsheet, database, text files, etc.).
- (4) Name of person who performed the extract.
- (5) Output of the extract.
- (6) The type of sensitive information in the extract (SSN, DOB, banking information, etc.).
- (7) Purpose of the extract.
- (8) Length of time the extract is needed

5. Program Management Policies



5.1 IA Program Management

What is the purpose of this policy?

FISMA requires agencies to develop and implement an organization-wide information security program to address information security for information and information systems that support the operations and assets of the Agency. The following program management controls are independent of any particular information system and are essential for managing the IAP.

Table 4: Program Management Controls

Control	Policy
PM-1 Information Assurance Program Plan	<p>Description -This control ensures that the information security policies provide sufficient information about the controls to enable implementation.</p> <p>Policy: This document is the IAP plan and provides an overview of the security requirements for information systems and privacy security; includes roles, responsibilities, management commitment, coordination, and compliance; and is reviewed annually by the CISO.</p> <p>Procedures: IA SharePoint Resource Site</p>
PM-2 Information Security Resources	<p>Description - This control ensures that that Capital Planning and Investment Control (CPIC) requests involving information systems includes funding to meet information assurance requirements.</p> <p>Policy: The CISO is responsible for coordinating with the Plans and Policy Director to ensure CPIC policy and procedures includes requirements that: (i) investment requests include the resources needed to implement the information security program and all exceptions are documented; (ii) a business case is used to record the resource required; and (iii) ensures that information security resources are available for expenditure as planned.</p> <p>Procedures: CPIC Policy</p>
PM-4 Plan of Action and Milestones Process (POA&M)	<p>Description - This control ensures that a process for ensuring that the POA&Ms for the IAP and Agency information systems are developed, maintained, and reviewed.</p> <p>Policy: The CISO is responsible for implementing a process for ensuring that plans of action and milestones are: (i) developed and maintained and adequately document the remedial actions to respond to the associated risk to operations, assets, and individuals; and (ii) reviewed for consistency with the CNCS’s risk management strategy and risk response actions.</p> <p>Procedures: IA SharePoint Resource Site</p>
PM-5 Information System Inventory	<p>Description - This control ensures that an inventory of all the CNCS information systems is maintained.</p> <p>Policy: The CISO will maintain a system inventory in accordance with OMB requirements.</p> <p>Procedures: IA SharePoint Resource Site</p>

Control	Policy
PM-6 Information Security Measures of Performance	<p>Description - This control ensures that information security measures of performance are developed that measure the effectiveness of the IAP.</p> <p>Policy: The CISO will develop information security measures of performance that are outcome-based. The effectiveness of the information security program and the security controls employed in support of the program measures will be monitored and reported.</p> <p>Procedures: IA SharePoint Resource Site</p>
PM-7 Enterprise Architecture	<p>Description -This control ensures information security requirements are integrated into enterprise architecture in the system development life cycle.</p> <p>Policy: The CISO will coordinate with the Policy and Plan Director to ensure that the information security requirements and associated security controls are integrated into the CNCS’s enterprise architecture.</p> <p>Procedures: IA SharePoint Resource Site</p>
PM-8 Risk Management Strategy	<p>Description -This control ensures that an agency-wide risk management strategy is developed and maintained.</p> <p>Policy: The CISO will develop a risk assessment procedure that ensures that: (i) a process is in place for evaluating risk across the Agency; (ii) the risk management process includes the risk executive (function) and a designated AO for each information system; and, (iii) the risk executive function is used to facilitate a consistent, CNCS-wide application of the risk management strategy.</p> <p>Procedures: IA SharePoint Resource Site</p>
PM-9 Security Authorization Process	<p>Description - This control ensures that a security authorization process for information systems is developed and maintained.</p> <p>Policy: The CISO will develop a security authorization process that: (i) documents, tracks, and reports the security state of the information systems and the environments in which the systems operate; (ii) ensure that security authorization process follows the CNCS -wide risk management process, NIST Risk Management Framework, and FISMA security standards and guidelines; (iii) ensure that a designated AO and ISO is assigned for each information system; (iv) information protection needs are derived from the mission/business needs and the risk management strategy; and (v) the security authorization process is integrated with CNCS’s continuous monitoring process to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, and other organizations.</p> <p>Procedures: IA SharePoint Resource Site</p>
PM-11 Testing, Training, and Monitoring	<p>Description - This control ensures that CNCS provides oversight for the security testing, training, and monitoring activities that are routinely conducted as part of ongoing assessments.</p> <p>Policy: The CISO will implement a process for ensuring that plans for conducting security testing, training, and monitoring are developed and maintained and executed in a timely manner. Plans will be reviewed for</p>

Control	Policy
	<p>consistency with the risk management strategy.</p> <p>Procedures: IA SharePoint Resource Site</p>
<p>PM-12 Incident Response</p>	<p>Description - This control ensures the effective implementation of incident response plans and procedures.</p> <p>Policy: The CISO will: (i) develop and coordinate an incident response plan; (ii) will track and document information system security incidents; (iii) develop incident reporting requirements and provide an incident response support resource; (iv) test the incident response capability for the information system annually using checklist or tabletop exercises to determine the incident response effectiveness and document the results; and (v) ensure that ISOs provide incident response training to individuals with incident response responsibilities.</p> <p>Procedures: IA SharePoint Resource Site</p>

Appendix A: References

LEGISLATION

1. [E-Government Act \[includes FISMA\] \(P.L. 107-347\), December 2002.](#)
2. [Federal Information Security Management Act \(P.L. 107-347, Title III\), December 2002.](#)
3. [Paperwork Reduction Act \(P.L. 104-13\), May 1995](#)
4. [The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974](#)
5. [Children’s Online Privacy Protection Act \(COPPA\)](#)
6. [Freedom of Information Act \(FOIA\)](#)

POLICIES, DIRECTIVES, INSTRUCTIONS

1. [OMB, A-130, Appendix III, Management of Federal Information Resources, November 2000.](#)
2. [OMB Memorandum Privacy and System Security Memorandums.](#)
3. [Cyber Security Research and Development Act of 2002.](#)
4. [FIPS 140-2, Security Requirements for Cryptographic Modules](#)
5. [FIPS 199, Standards for Security Categorization of Federal Information and Information Systems](#)
6. [FIPS 200, Minimum Security Requirements for Federal Information and Information Systems](#)

GUIDELINES

1. [National Institute of Standards and Technology Special Publication.](#)

OTHER

1. [Common Vulnerabilities and Exposures \(CVE\)](#)
2. [Common Vulnerability Scoring System \(CVSS\)](#)
3. [National Vulnerability Database](#)
4. [United States Government Configuration Baseline \(USGCB\)](#)

Appendix B: Acronyms and Abbreviations

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 Management Act
FOIA	Freedom of Information Act
IA	Information Assurance
IAM	Information Assurance Manager
IAP	Information Assurance Program
IO	Information Owner
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
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
POA&M	Plan of Action and Milestones
POC	Point of Contact
ROB	Rules of Behavior
SAOP	Senior Agency Official for Privacy
SDLC	Systems Development Lifecycle
SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
ST&E	Security Test and Evaluation
VPN	Virtual Private Network

Appendix C: Glossary

The attached glossary provides system security and privacy definitions for technical terms used throughout these policies.

[IA Glossary Link](#)