Community Gold Standard

Version 2.0

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

The Community Gold Standard Framework

Version 2.0

26 June 2014

Table of Contents

Summary of Changes

Date	Reason	Version
30 June 2011	Initial Release	1.0
30 July 2012	Inclusion of new IAD document template and synopsis	1.1
TBD	CGS v2.0 Initial Release	2.0

CGS v1.1 to CGS v2.0 capability mapping is included in Appendix D.

1 Introduction

The Community Gold Standard (CGS) is a compendium of mission-enhancing security best practices for National Security Systems (NSS). CGS provides a holistic view of Information Assurance (IA) considerations for decision makers to efficiently plan, and security engineers to implement, the necessary measures for a defensible enterprise.

1.1 Background

CGS began as a charge from the Director of the National Security Agency (DIRNSA) to capture best practices in IA. In response to the challenge, National Security Agency (NSA) experts developed the CGS framework and began populating it with best practices. In July 2012, NSA published CGS v1.1.1 and began working with customers to drive IA business decisions. Since the initial CGS publication, NSA has applied lessons learned from customer engagements and developed the next generation of CGS. This document, CGS v2.0, addresses updates and changes to NSS community policy and guidance since the onset of CGS.

1.2 Purpose

CGS provides comprehensive IA guidance for securing NSS enterprises and enables the mission in the face of continuous attack. CGS characterizes the best practice for IA capabilities in accordance with policies and standards, while considering the limitations set forth by current technologies and other constraints.

1.3 CGS Framework

The CGS framework encompasses four overarching cybersecurity functions: Govern, Protect, Detect, and Respond & Recover. These cybersecurity functions focus on the capabilities and activities required to provide confidence in cyberspace.

- Govern: Guidance for agencies to fully understand the enterprise mission and environment, manage portfolios and resources, ensure the workforce is informed and engaged, and establishes resilience across the enterprise.
- Protect: Guidance to help the enterprise safeguard the physical and logical environment, assets, and data.
- Detect: Guidance to help identify and defend against vulnerabilities, anomalies, and attacks on the physical and logical elements of the enterprise.
- Respond & Recover: Guidance for efficient response mechanisms to address threats and vulnerabilities.

The CGS framework is designed to be applicable to organizations facing many different challenges. While CGS does not prescribe one single approach to selecting and implementing capabilities, the framework is arranged in a logical flow, with the organizational understanding and govern infrastructure providing a foundation for the framework, with the protect and detect capabilities working together to safeguard the enterprise.

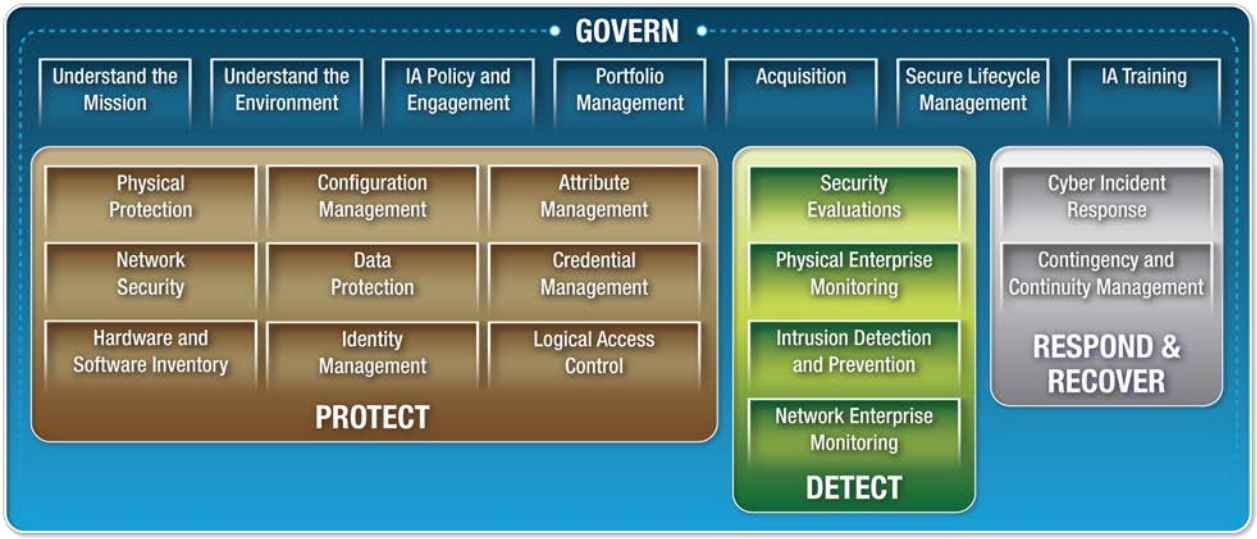


Figure 1: CGS Framework Diagram

1.4 How to Use This Document

Organizations will ensure a comprehensive approach to security from implementing recommended activities and/or aligning security practices to the CGS framework structure. This document describes people, process, and technology considerations for each capability. Each capability includes the following elements:

- Definition – This section describes the capability, including the main activities discussed within the capability guidance. Refer to the Glossary (Appendix F) for related terms discussed in the definition and capability guidance.
- Discussion – This section includes the high-level context for the capability and guidance provided.
- Example Threats –This section offers sample threats related to the capability. Proper implementation of the guidance can help mitigate the listed threats, among others.
- Capability Guidance – This section outlines actionable capability guidance statements that offer best practices to improve enterprise security posture. Detailed implementation guidance is referenced, where available, by the capability guidance statements.
- Informative References – This section highlights additional IA/cybersecurity resources (Appendix A) that may provide context and implementation information to complement CGS guidance.

This document is intended to provide decision makers responsible for setting organizational security goals with a context and starting point to mature enterprise capabilities. The arrangement of the content offers System Security Engineers (SSE) a comprehensive view as it helps the reader gain an understanding of key IA and cybersecurity concepts by reading the document in its entirety, or by leveraging specific guidance and references.

2 Govern

Figure 2: Govern Function Diagram

Strong governance provides a foundation for the protection and defense activities that support and sustain enterprise resilience. Governance helps the enterprise ensure mission effectiveness during standard operations and in the presence of adversarial elements. Additionally, the Govern capabilities establish processes to securely obtain, maintain, and understand resources within the enterprise. The capabilities within this area provide a context for the risk management process detailed in the National Institute of Standards and Technology (NIST) Risk Management Framework,[1] helping the enterprise manage risk by identifying and prioritizing potential threat events in the environment, addressing security compliance requirements, and establishing a performance management program.

Despite all best efforts, security breaches, emergencies, system failures, and disasters may still occur. With the support of the Protect, Detect, and Respond & Recover capabilities, the Govern capabilities guide mission assurance before, during, and following incidents. Actively establishing plans and procedures for addressing security incidents and emergency situations assists to quickly and adequately maintain and restore data and network activity.

2.1 Understand the Mission

Definition: The *Understand the Mission* capability defines the relationship and dependencies between the mission and its supporting people, processes, technology, and environmental elements.

Discussion: Understanding mission(s), goals, objectives, and success criteria is critical to managing successful and secure operations. Mission objectives assist an organization in meeting goals such as understanding how data, information services, and information transactions support specific missions. It is important for personnel at all levels to understand how their efforts support these mission objectives.

Example Threats: Asset Loss, Communication Disruption, Denial of Service (DoS)

2.1.1 Mission Identification

Each enterprise should identify and understand its unique operational objective(s) and supporting missions.

- Determine or validate the vision, goals, and operational objective(s) the enterprise mission(s) support.[2]
- Determine and document the key measure(s) for mission success.
- Identify mission relationships, impacts, and prioritization.

[1] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[2] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

- Identify applicable laws, directives, and policy guidance issues pertinent to the organization's mission.[3]
- Define both core and related missions, prioritizing them with respect to enterprise goals and objectives.[4]

- Identify and prioritize mission functions.[5]
  - Understand mission interrelationships and dependencies.
- Make unique mission allocation decisions based on mission priority, precedence, and preemption.[6]

2.1.2 Mission Sustainment

Mission security priorities may change due to evolving threats to the environment; therefore, mission sustainment and reevaluating risk is critical to ensure overall mission objectives are met.

- Understand the risks which can potentially affect the mission, and what impact would be to the mission.[7]
- Coordinate with stakeholders to establish standards dictating common metrics, formats, etc. to enable consistent monitoring of security and mission readiness.[8]
- Determine and incorporate mission driven modifications to security objective(s).

2.1.3 Understand Mission Data and Risks

Organizations must make informed mission assurance decisions by understanding how data supports missions and what risks are present within its environment.

- Define and document data relationships and interdependencies.[9]
  - Assess the strength of trust relationships.
  - Evaluate how data either directly or indirectly supports the mission.
- Review consolidated data flow information on an ongoing basis to support near-real-time risk management.[10]
- Prioritize data flows based on the risk to mission needs including data protection, data availability, and critical function continuity.[11]

[3] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
[4] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[5] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
[6] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
[7] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[8] DoDI 8410.02, NetOps for the Global Information Grid (GIG), December 2008
[9] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
[10] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[11] Ibid.

2.1.4 Utilization and Performance Management

Ensuring quality of service to operational components is a key enabler of mission success, and effective communication is an integral part of that process. Data performance and enterprise utilization thresholds must be closely managed to facilitate decision making, improve performance, and increase accountability.

- Identify and review information security performance goals and objective(s), and related policies and guidelines.[12]
- Prioritize performance measures based on mission needs.[13]
- Coordinate with stakeholders to develop information security measurements.[14]
- Utilize network operations trend information to establish performance targets (e.g., bandwidth consumption).[15]
    - Monitor and evaluate service delivery and resource consumption (e.g., network bandwidth, power, cooling, space, Central Processing Unit [CPU], Random-Access Memory [RAM], and media storage).
- Document performance measures in a standard format that provides the level of detail required for measures collection, analysis, and reporting.[16]
- Analyze performance measures to identify trends and determine progress against information security goals and objectives.[17]
- Provide reports of network utilization and trigger alerts when thresholds are exceeded or Service Level Agreements (SLA) are not met.[18]
- Develop and implement a plan to correct unsatisfactory performance reports.[19]

Understand the Mission Informative References (Appendix A)

2.2 Understand the Environment

Definition: The *Understand the Environment* capability defines physical and logical environments, and identifies physical and logical threats facing the enterprise.

Discussion: The global nature of enterprises and the threats facing them necessitate an understanding of the factors within the external physical environment (e.g., location and socio-political considerations) and internal logical environment (e.g., network architecture and data flows) that may impact security needs. An understanding of these enterprise environments will enable the development of a robust threat intelligence program that provides the foundation to select security measures and inform the organizational risk posture.

Example Threats: Asset Loss

[12] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[13] NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security, July 2008
[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] Ibid.
[18] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PM-6, "Information Security Measures of Performance," April 2013
[19] NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security, July 2008

2.2.1 Understand the Physical Environment

An understanding of the external physical environment establishes a foundation for the internal physical and logical environments.

- Identify all aspects of the physical environment to include infrastructure, socio-economic, and political considerations.[20]
- Identify adversarial, friendly, and neutral actors relevant to the enterprise.[21]
- Identify pertinent facilities housing system resources, including the mechanisms used to support facility operation (e.g., power, telecommunications, gates, cameras, alarms, checkpoints, and locks).[22]
- Document physical communication link locations.
- Retain maintenance records for repairs or modifications performed on the facility or subsystems.[23]
    - Ensure collected physical environment information is centrally managed, protected, and accessible for reference.

2.2.2 Understand the Logical Environment

An understanding of the logical environment is a critical foundational element in establishing enterprise baselines, identifying risks, and facilitating network security.

- Conduct real-time (or near real-time) automated mappings of all network components, using manual means when automation is not possible.[24]
- Protect network diagrams at an appropriate classification for the network they depict.[25]
- Map both internal and external network boundaries.[26]
    - Identify the risk(s) that each enterprise network boundary introduces.
- Categorize information systems based on applicable policies, regulations, and standards.[27]
    - Include details of how devices (logical and physical) work together to fulfill a necessary function.
    - Clearly define software characteristics for the major functional units of the enterprise (e.g., systems, subsystems, services).[28]
- Document mission-supporting data flows, articulating how data supports mission elements.[29]

---

[20] DoD Joint Publication 5-0, Joint Operation Planning, August 2011
[21] Ibid.
[22] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
[23] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control MA-2, "Controlled Maintenance," April 2013
[24] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-8, "Information System Component Inventory," April 2013
[25] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-11, "Developer Security Testing and Evaluation," April 2013
[26] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, October 2013
[27] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control RA-2 "Security Categorization," April 2013
[28] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-10 "Developer Configuration Management," April 2013
[29] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010

- Include source, destination, data type, and full path of the data flow.
- Ensure data flow documents are stored in a standard format that trace back to the source of data relating to the mission asset.
- Share data flow documents and reports with leadership to facilitate analysis.

2.2.3 Understand the Threat Environment

An understanding of enterprise physical and logical environments enables the use of threat intelligence.

- Select authoritative sources of threat information.[30]
- Identify any threats deriving from the physical or logical environment design.[31]
- Share information on threats to U.S. information infrastructure and systems through the strategic indications and warnings (I&W) process.[32]
- Categorize threat sources by capability, intent, and targeting characteristics (for adversarial threats) or range of potential effects (for non-adversarial threats).[33]
- Prioritize threat information, and inform appropriate security personnel and affected organizations.
- Determine the likelihood of identified threats in order to prioritize mitigations.[34]
  - Monitor threats and perform trend analysis to assist in determining the intent and capabilities of the attackers.[35]
  - Model, develop, and analyze threat scenarios.[36]
  - Increase levels of assurance, as appropriate, for potential high-value enterprise targets with a high level of threat likelihood.[37]
- Assign a value of relevance to each threat, which is directly linked to organizational risk tolerance.[38]
- Report threats in accordance with established requirements to specified personnel.[39]
  - Share threat information with stakeholders, as required or agreed upon.[40]

Understand the Environment Informative References (Appendix A)

2.3 Information Assurance (IA) Policy and Engagement

Definition: The *Information Assurance (IA) Policy and Engagement* capability creates and manages policies in accordance with legal authorities and shares information to enhance the enterprise security posture.

[30] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012
[31] FEMA 430, Risk Management Series, Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks, December 2007
[32] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[33] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012
[34] FEMA 430, Risk Management Series, Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks, December 2007
[35] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012
[36] Ibid.
[37] NIST SP 800-37 Rev.1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[38] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012
[39] Ibid.
[40] Ibid.

Discussion: Legal authorities, multi-agency enterprises, and agencies are connected through compliance and collaboration to support NSS mission goals. Enforcement mechanisms are implemented to subordinate organizations from legal authorities and obligatory reporting enables performance oversight. The oversight process ensures security compliance and facilitates community information sharing and threat awareness.

Example Threats: Insider Threat, Loss of Personally Identifiable Information (PII)

2.3.1 Policy Development

Enterprise policies are developed in accordance with overarching laws and regulations in coordination with key enterprise elements to provide a critical foundation for enterprise security programs.

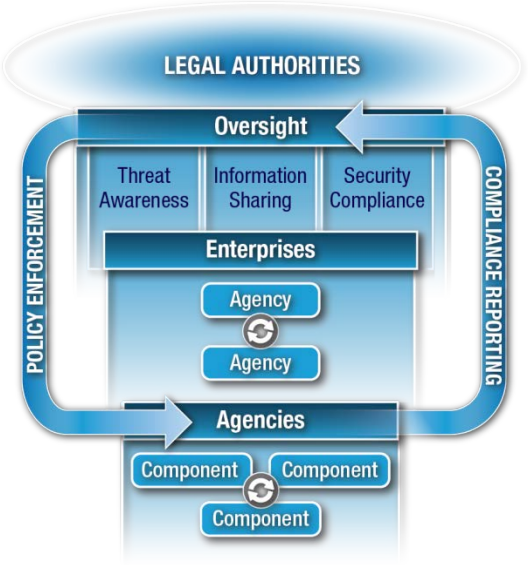


Figure 3: Legal Authorities Diagram

- Identify overarching policies, procedures, and standards (IA policies) to provide oversight for IA/cybersecurity throughout the enterprise.[41]
    - Base enterprise IA policies on applicable laws, regulations, and other applicable policies identified (e.g., intelligence community directives [ICDs] for elements within the intelligence community).
    - Align IA policies to complement similar policies at comparable organizations, as possible.[42]
- Ensure that enterprise policies are informed by and reflect organizational security requirements.[43]
    - Identify the purpose of the policy, implementation mechanisms, and outcomes.
    - Identify the policy audience.
- Map enterprise-level and lower-tier IA policies to strengthen and enhance security functionality throughout the organization.[44]
- Coordinate with subject matter experts (SME) at different levels across the enterprise (e.g., technical directors, Chief Information Security Officers [CISOs], and key project managers), when defining IA policies.
- Translate established enterprise policies into a standard executable digital format.
    - Create a policy hierarchy to allow the centralized translation of established and defined digital policies into a common formal language.

[41] CNSSI-4009, National Information Assurance (IA) Glossary, April 2010; "Information Security Policy"
[42] ICD 101, Intelligence Community Policy System, June 2009
[43] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
[44] Ibid.

2.3.2 Policy Implementation

Coordinated enterprise programs ensure IA policies are implemented in a consistent and efficient manner throughout the organization.[45]

- Develop an implementation plan for enterprise policies, including timeframe and activities.[46]
- Deconflict new policies with existing enterprise-level and local policies, particularly when implementing digital policies.
- Define policies centrally through authoritative sources within the enterprise.[47]
    - Test new or modified policies for adverse conditions prior to enterprise implementation.
- Establish programs to provide oversight for key security concepts within the enterprise. These programs may include but are not limited to:
    - Insider Threat: Establish a program to collect and address insider threat-related information, provide monitoring and training activities, and to ensure the protection of civil liberties and privacy.[48]
    - Privacy: Establish a privacy program to ensure the protection of individuals and their PII within the enterprise.[49]
    - Contingency Planning: Establish a continuity program to oversee all aspects of contingency and continuity planning and to ensure the sustainment of national essential functions and mission-essential functions in the event of an emergency.[50]
- Delegate necessary authorities and resources to implementers assigned to execute IA policies.[51]
- Develop system-level policies and procedures only when necessary to provide additional implementation details for enterprise-level guidance.[52]
- Use a secure configuration management system to provision digital policies for distribution and deployment.[53]

2.3.3 Policy Enforcement and Maintenance

Establishment of business process and organizational controls to enforce and maintain policies will help the organization sustain the alignment of IA policy to evolving enterprise requirements.

- Establish manual procedures (e.g., Human Resource [HR] actions, citation, or records reviews), automated mechanisms (e.g., automatic sign-out after period of inactivity), and business processes to ensure policies are carried out as defined.[54]
- Document all policy exceptions through a formalized exception procedure.

---

[45] Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
[46] Ibid.
[47] Ibid.
[48] Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 2012
[49] Federal CIO Council Privacy Committee, Best Practices: Elements of a Federal Privacy Program, June 2010
[50] National Security Presidential Directive 51/Homeland Security Presidential Directive 20 (NSPD-51/HSPD-20), National Continuity Policy, October 2012
[51] Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
[52] OMB Circular No. A-130 Revised, Management of Federal Information Resources, 2000
[53] NIST SP 800-128, Guide for Security Focused Configuration Management of Information Systems, August 2011
[54] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-2, "Audit Events," April 2013

- Document a process to identify any organizational roles with the authority to exempt policy for specific purposes or events.
- Review policies, standards, and procedures for necessary updates when policies or processes change, or when significant technological advances impact established policies.[55]
    - Perform periodic reviews to identify and address gaps, and to ensure continued effectiveness and applicability.
    - Establish a standard to define how often IA policies procedures and standards are reviewed.
- Establish a formal process for managing information security documents.[56]
    - Identify and document a process for archiving old policies and notifying stakeholders of new policies, procedures, and standards.
    - Implement a continuous maintenance process for IA policy documentation.
- Enforce IA policies, including digital policies, consistently across the organization.[57]

2.3.4 Information Security Collaboration

Sharing security information across the enterprise and the community enhances security postures and increases interagency engagement to establish shared situational engagement.

- Designate roles or individuals with the authority to publicly share information on behalf of the enterprise.[58]
- Coordinate with affected enterprise elements to ensure personnel, management, security officers, and system administrators are aware of changes to enterprise IA policies.[59]
- Communicate information about enterprise objectives, threats, risks, and actions to the enterprise workforce and relevant external stakeholders.[60]
- Coordinate enterprise communications with security awareness training programs to address key enterprise topics, including operations security (OPSEC), physical security, information security, and counterintelligence.[61]
- Update the IA Awareness program periodically.[62]
    - Evaluate awareness program effectiveness based on metrics and personnel feedback.
    - Update IA awareness content based on evolving mission needs, capabilities, and threats.
- Develop an information security collaboration program to coordinate with partner organizations regarding best practices, enterprise and community threats, cyber incidents, and shared capabilities.[63]

[55] Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
[56] Ibid.
[57] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-1 "Access Control Policy and Procedures," April 2013
[58] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-22 "Publicly Accessible Content," April 2013
[59] ICD 101, Intelligence Community Policy System, June 2009
[60] Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
[61] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AT-2 "Security Awareness Training," April 2013
[62] ISO/IEC 27001, Information Security Management, Human Resources Security, A.8.2.2 "Awareness, Education, and Training"
[63] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), January 2008

- Establish connections between enterprise cyber centers and other federal, state, and local cyber centers to enhance situational awareness.[64]
- Develop a threat awareness program to share threat information with partner organizations.[65]

Information Assurance (IA) Policy and Engagement Informative References (Appendix A)

2.4 Portfolio Management

Definition: The *Portfolio Management* capability analyzes, selects, controls, and evaluates current and planned IA investments against enterprise needs.

Discussion: Portfolio Management helps to ensure that the enterprise effectively allocates people, processes, and technology resources. IA performance management and oversight enables organizations to prioritize and monitor current and future investment strategies.

Example Threats: Collusion, Espionage

2.4.1 Investment Planning

IA investments must be carefully prioritized to balance maximum security benefits while optimizing mission effectiveness.

- Analyze IA program financial needs and security requirements during the budgeting process.[66]
  - Budget for development and sustainment of IA programs, products, and services throughout the enterprise.[67]
- Consider how people, process, and technology changes (e.g., technology innovations or evolved threat posture) may impact planned resource allocations.[68]
- Allocate the IA budget to support organizational risk decisions and maximize product and service reuse.[69]
  - Prioritize investments based on criticality of IA program needs.[70]
- Utilize risk-based investment planning to ensure tailored solutions to promote innovation and to maximize security.[71]
- Document best practices for determining needed allocations.[72]
- Track and evaluate risks and results of capital investments to analyze the costs and benefits of the investment for future use.[73]
- Determine and allocate resources needed to fulfill the acquisition and funding for system sustainment.[74]

[64] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), January 2008
[65] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PM-16 "Threat Awareness Program," April 2013
[66] NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[67] Department of Defense Chief Information Officer Desk Reference, Volume 1: Foundation Documents, August 2006
[68] NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security, July 2008
[69] E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899
[70] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
[71] Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise; DHS publication, November 2011
[72] Department of Defense Chief Information Officer Desk Reference, Volume 1: Foundation Documents, August 2006
[73] Ibid.

2.4.2 Performance Management

The enterprise must set and understand its performance goals in order to accurately evaluate whether IA investments are being made effectively.

- Ensure investment strategies reflect the goals and objectives of the organization.
- Manage activities to foster mission and business success.[75]
- Develop and maintain a plan of action and milestone process to prioritize risk response actions and to ensure consistency of program and organizational goals.[76]
- Leverage an Investment Review Board (or similar group) to analyze how funding will be allocated for IA programs.[77]
    - Evaluate any redundant efforts across organizations when identifying funding needs.
- Determine which IA investments are most beneficial for the enterprise according to priority, schedule, and cost.[78]
    - Incorporate input from stakeholders to identify and validate selection criteria.[79]
    - Use selection criteria to establish the overall benefit and cost of each IA investment.
    - Consider indirect costs (e.g., performance, employee morale, and retraining requirements) when selecting IA investments.[80]
- Perform status reviews and communicate program progress against intended goals.[81]
    - Address technical and budget issues.
    - Determine if goals need to be adjusted.
- Evaluate metrics against performance goals, and use quantifiable data as input.[82]
- Develop and implement a strategy to help manage risk to enterprise components (e.g., personnel, other agencies, program assets).[83]
    - Review and update the risk strategy as necessary.

2.4.3 Investment Oversight

Portfolio Management requires oversight on IA investments to ensure anticipated improvements to the enterprise security posture are achieved.

- Assign budgetary oversight responsibilities for an information system to its authorizing official.[84]

---

[74] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-2 "Allocation of Resources," April 2013
[75] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
[76] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PM-4 "Plan of Action and Milestones Process," April 2013
[77] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PM-3 "Information Security Resources," April 2013
[78] NIST SP 800-65 Rev. 1 (Draft), Recommendations for Integrating Information Security into the Capital Planning and Investment Control (CPIC) Process , July 2009
[79] Ibid.
[80] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
[81] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PM-6 "Information Security Measures of Performance," April 2013
[82] NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security, July 2008
[83] NIST SP 800-53 Rev, 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PM-9 "Risk Management Strategy," April 2013

- Utilize an enterprise architecture that allows for direct traceability between investments and performance improvements.[85]
- Comply with enterprise processes and procedures when allocating funding.
- Capture and approve financial requirements to align with the strategic direction before allocating the budget.
- Review information security programs and systems annually, and report findings to the Office of Management and Budget (OMB).[86]
- Establish a mechanism to communicate portfolio security status to oversight authorities (e.g., Federal Information Security Management Act [FISMA]).[87]
    - Reevaluate investment strategies when there are significant threat changes or advances in IA solutions.[88]

Portfolio Management Informative References (Appendix A)

2.5 Acquisition

Definition: The *Acquisition* capability manages the security considerations associated with enterprise procurements.

Discussion: Securely obtaining technology, facilities, and services presents challenges in a globally integrated economy. Threats to the secure procurement process may come from either internal or external sources; without strict acquisition security, even trusted vendors may introduce supply chain risks. In addition, the nature of the global supply environment introduces another layer of supply chain risk to the enterprise. It is essential that organizations comply with all applicable acquisition laws and regulations while balancing risk, enterprise needs, and resource constraints.

Example Threats: Backdoors, Collusion, Counterfeiting, Insider Threat, Supply Chain Injection

2.5.1 Product and Service Requirements

Product and service requirements must be clearly defined to facilitate a smooth acquisition process.

- Develop and document system and services acquisition policy and procedures.[89]
    - Conduct an annual review of acquisition policies.[90]
- Ensure that acquired products do not cause undue risk to the enterprise, and that they are cost-effective.
- Employ a sustainment plan that ensures continuity of operations during acquisition.[91]

---

[84] NIST SP 800-37 Rev, 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
[85] NIST SP 800-65 Rev, 1(Draft), Recommendations for Integrating Information Security into the Capital Planning and Investment Control (CPIC)Process, July 2009
[86] Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
[87] NIST SP 800-65 Rev. 1(Draft), Recommendations for Integrating Information Security into the Capital Planning and Investment Control (CPIC) Process , July 2009
[88] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
[89] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-1, "System and Services Acquisition Policy and Procedures," April 2013
[90] Interim DoDI 5000.02, Operation of the Defense Acquisition System, November 2013
[91] Ibid.

  - Ensure there is budgeting to sustain any necessary systems in operation.
  - Include a schedule for developing and fielding a new system.
- Determine and document product requirements based on security functionality and assurance.[92]
  - Consider how the product is going to be used in the respective environment.
  - Document information security requirements, including information and communication technology (ICT) supply chain risk management (SCRM)-specific requirements.
  - Apply ICT SCRM controls to the system and software development life cycle and the environment in which the system or software development is conducted (e.g., development environment).
- Determine if the product is new to the enterprise or on an approved list.
- Ensure that acquired IA-enabled information technology (IT) products for NSS meet National Information Assurance Partnership (NIAP) requirements.[93]
  - Leverage approved NSA Commercial Solutions for Classified (CSfC) capability packages for composed, layered IA solutions.[94]
- Ensure developers of acquired products employ secure development practices, and provide supporting documentation.[95]

2.5.2 Vendor Selection and Evaluation

Verifying quality performance and establishing trusted relationships with vendors limits supply chain security breaches.

- Consider applicable rules and regulations regarding acquisition.[96]
- Use an integrated, collaborative method to identify enterprise needs guiding the acquisition process.[97]
- Identify products and services offered by all types of suppliers (e.g., government laboratories, academia, commercial sector), both domestic and foreign.[98]
- Document and evaluate vendors using measures of effectiveness, cost, schedule, concepts of operations, and overall risk.[99]
- Consider vendor information (e.g., location, partner affiliations, clearance level, employees) as a factor in evaluating acquisition security risk.[100]
- Ensure that suppliers are vetted to meet enterprise assurance requirements.

[92] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-4, "Acquisition Process," April 2013
[93] CNSSP-11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, June 2013
[94] Ibid.
[95] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-4, "Acquisition Process," April 2013
[96] Federal Acquisition Regulation (FAR), March 2005
[97] Interim DoDI 5000.02, Operation of the Defense Acquisition System, November 2013
[98] Ibid.
[99] Ibid.
[100] NIST 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, DRAFT, August 2013

- Verify that, when the supplier is a value-added reseller, the supplier is not implementing anything malicious or anything that may degrade the product's ability to effectively implement security functions.
- Ensure that third-party suppliers who are not value-added resellers do not tamper with or modify a product between the time the original supplier produces it and the purchasing enterprise receives it.
- Document and enforce quality assurance standards to verify the genuine nature of received products.
- Establish personnel security policies for third-party suppliers.[101]
- Employ safeguards to limit the potential for supply chain harm (e.g., requiring attack/compromise reports from vendors).[102]

- Ensure all personnel receiving privileged acquisition information sign an access agreement to mitigate the risk of a conflict of interest.[103]
- Verify that no significant changes have occurred since the previous acquisition request for products or services used by the organization.

2.5.3 Acquisition Security

A secure acquisition process requires stringent supply chain security management procedures to reduce enterprise risk while obtaining products and services.

- Establish an ICT SCRM policy based on external and organizational requirements and constraints.[104]
  - Ensure SCRM policy includes the purpose and applicability, as well as investment requirements.[105]
  - Identify mission and business requirements that will influence ICT SCRM (e.g., cost, schedule, performance, security, privacy, quality, safety).[106]
  - Identify how ICT SCRM is integrated into organization-wide business/mission processes and enterprise architecture.[107]
  - Document organizational risk tolerance for supply chain risks.[108]
  - Define the risk response strategy for critical business/mission acquisitions.[109]
- Establish an enterprise ICT SCRM team.[110]

[101] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PS-7, "Third-Party Personnel Security," April 2013
[102] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-12, "Supply Chain Protection," April 2013
[103] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PS-6, "Access Agreements," April 2013
[104] NIST 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, DRAFT, August 2013
[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] NIST 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, DRAFT, August 2013

- Uniquely identify the elements, processes, and people involved in SCRM.[111]
    - Engage subject matter experts (e.g., counterintelligence [CI], information assurance, logistics, analysis, and security), as applicable, to manage supply chain risk.[112]
- Limit the access of individuals and organizations to supply chain elements.[113]
- Implement auditing and separation of duties to reduce the risk of collusion.[114]
- Ensure information on past performance of SCRM evaluations (e.g., known supply chain compromises) is shared among stakeholders.[115]
- Ensure that programs containing classified information have written authorization prior to entering discussions with potential foreign partners.[116]
- Identify and document policies and procedures to minimize acquisition time and facilitate rapid procurement in special conditions.[117]
    - Employ approved vendor lists.[118]
- Ensure thorough review and approval of acquisition decisions, based on security and/or funding level.[119]
- Inform contractors and subcontractors of security classifications and requirements assigned to documents, materials, tasks, subcontracts, and components of the classified contract.[120]
- Maintain records and oversight of contractor information systems used to process and store classified information.[121]
- Consider how aggregated acquisition information may pose a risk to the enterprise.[122]
- Ensure the appropriate disposition occurs for all classified material received or generated under the contract.[123]
    - Designate a senior agency official to direct and administer contract implementation and compliance with the National Industrial Security Program.[124]

2.5.4 Procurement Acceptance

Once a proposed acquisition has been evaluated against stated requirements, custody of procured goods and services must be transferred in a secure manner.

[111] NIST, ITL Bulletin November 2012, Practices for Managing Supply Chain Risks to Protect Federal Information Systems
[112] ICD 731, Supply Chain Risk Management, December 2013
[113] NIST, ITL Bulletin November 2012, Practices for Managing Supply Chain Risks to Protect Federal Information Systems
[114] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-5, "Separation of Duties," April 2013
[115] NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems, October 2012
[116] Interim DoDI 5000.02, Operation of the Defense Acquisition System, November 2013
[117] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-12 "Supply Chain Protection," April 2013
[118] Ibid.
[119] Interim DoDI 5000.02, Operation of the Defense Acquisition System, November 2013
[120] Federal Acquisition Regulation (FAR), March 2005
[121] DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)
[122] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-12 "Supply Chain Protection," April 2013
[123] Federal Acquisition Regulation (FAR), March 2005
[124] Executive Order 12829, National Industry Security Program

- Use secure physical and logical delivery mechanisms that protect confidentiality, integrity, and availability.[125]
- Evaluate all acquisitions to ensure required security, interoperability, and supportability.[126]
- Assess changed environmental or technical factors that may affect operational effectiveness (e.g., new threat environments). [127]
    - Assess the cost and benefit of delaying or stopping the acquisition process if the program is not ready to proceed.[128]
- Document acceptance and disposition of acquired assets and services.[129]

Acquisition Informative References (Appendix A)

2.6 Secure Lifecycle Management

Definition: The *Secure Lifecycle Management* capability ensures security considerations are included throughout system and software lifecycles, including initiation, development, operation, and termination.

Discussion: Secure lifecycle management addresses all phases of a system (i.e., hardware, software, or combined solution), including conception, design, development, implementation, operation, maintenance, and disposal. Lifecycle management includes the interactions of people, processes, and technology, while addressing the need to introduce and embed security at the earliest possible phase in the development of new IT systems (e.g., infrastructure and custom developed software). It is imperative that systems and software are installed following the approved implementation plan since most enterprise vulnerabilities occur from poor configurations.

Example Threats: Architecture Flaws, Code Errors, Development Re-Work, Supply Chain Compromise

2.6.1 Initiation

The initiation phase enables the organization to document the purpose for a proposed system, while identifying the requisite enterprise security requirements and controls.

- Identify and document business requirements that must be addressed by any proposed solution.
    - Integrate IA requirements into all system and acquisition requirements.
- Define and develop a Concept of Operations (CONOPS) to document the system purpose and expected functionality.[130]
    - Document the system concept, which is decomposed to define granular requirements.
    - Identify key security roles.
    - Evaluate the security requirements for information that will be processed, transmitted, or stored.
- Ensure the proposed project supports mission goals, organizational prioritization, and enterprise risk posture.[131]

[125] NIST, ITL Bulletin November 2012, Practices for Managing Supply Chain Risks to Protect Federal Information Systems
[126] DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), April 2007
[127] Interim DoDI 5000.02, Operation of the Defense Acquisition System, November 2013
[128] Ibid.
[129] Federal Acquisition Regulation (FAR), March 2005
[130] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[131] NDIA, System Assurance Committee, Engineering for System Assurance Ver. 1.0, October 2008

- Determine and document requirements based on confidentiality, integrity, and availability.[132]
- Conduct a criticality analysis to identify mission critical functions and critical components.[133]
- Tailor controls in accordance with organizational security posture and system or software security categorization.[134]
- Establish specific and measurable requirements between the design or development team and key stakeholders to achieve formal acceptance.[135]
- Develop an assurance case to demonstrate how critical security requirements will be met in the anticipated environment(s).[136]

2.6.2 Design and Development

Design and development plans incorporating traceable system requirements and tailored security controls provide secure and maintainable systems.

- Ensure designers and developers understand security requirements.
- Create detailed system and security design specification documentation.[137]
    - Ensure system and software-level security architecture is consistent with organizational mission, data flows, and network mapping.[138]
    - Document the required product, process, and material specifications.
    - Specify interfaces between the system and other network components.
    - Evaluate logical, maintenance, and support requirements.
    - Reduce the vulnerability of functions and components identified during criticality analysis through secure system design.[139]
- Ensure the design addresses specific business requirements identified during the initiation phase.
- Ensure the system is acquired or built according to best practices.
- Enforce secure software development practices commensurate with system risk within development teams.[140]
    - Implement tailored controls to address required software security features.
    - Monitor and audit development teams' compliance with identified practices.
    - Implement security testing and code reviews for validation.
- Conduct risk assessments to supplement baseline security controls.
    - Categorize the system in accordance with Federal Information Processing Standard (FIPS) 199 and 200.
    - Select appropriate security controls and assurance requirements.
- Perform functional and security testing.
- Coordinate Certification and Accreditation (C&A) or Assessment and Authorization (A&A) with the SSEs.[141]

[132] NIST SP 800-64 Rev.2, Security Considerations in the System Development Life Cycle, October 2008
[133] DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), November 2012
[134] NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006
[135] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[136] NDIA, System Assurance Committee, Engineering for System Assurance Ver. 1.0, October 2008
[137] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[138] Ibid.
[139] DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), November 2012
[140] Ibid.

2.6.3 Test and Implementation

The test phase validates the security of the proposed system, in preparation for implementation.

- Ensure system certification activities are planned and conducted in synchronization with testing security controls.[142]
    - Assign severity categories to identified system vulnerabilities.[143]
    - Consider reliability and viability of the system, as well as its behavior within the environment, when making a certification decision.[144]
- Ensure security categorization and controls are met by the security solution(s) and provide documentation to aid in the Authorizing Official's (AO) approval of the implementation of the overall solution.[145]
    - Ensure that the AO coordinates with the development team.[146]
- Conduct integration testing to ensure introducing the system or software into the environment will not negatively impact the organizational security posture.
- Enable control settings in accordance with manufacturer instructions as well as security implementation guidance and specifications.[147]
- Assess system security and share assessment results with the system owner, system security officer, system administrator, and developers.[148]
- Incorporate secure and ordered deployment practices during implementation.
- Evaluate and certify all Government off-the-shelf (GOTS) IA and IA-enabled IT products intended for NSS use.[149]
- Employ an independent testing team to perform security control testing in a segregated environment that emulates the organization's operational needs.[150]
    - Conduct testing consistent with an approved organizational test and evaluation (T&E) strategy.[151]
    - Ensure detailed test plans are vetted through an appropriate approval authority, with consideration of the potential system risks introduced by testing in an operational-like environment.[152]
- Test and evaluate systems being developed or modified prior to implementation, using functional, developmental, and security testing processes.[153]

---

[141] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[142] Ibid.
[143] DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014
[144] Ibid.
[145] CNSSP-11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, June 2013
[146] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[147] Ibid.
[148] Ibid.
[149] CNSSP-11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, June 2013
[150] DoDD 5000.01, The Defense Acquisition System, November 2007
[151] DoD Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, Incorporating Test and Evaluation into Department of Defense Acquisition Contracts, October 2011
[152] Ibid.
[153] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008

- Ensure that acceptance tests are scoped to specific security requirements and are iterated a number of times in order to verify consistency in results. [154]
- Utilize automated testing tools when possible.[155]

2.6.4 Operations and Maintenance

To ensure accurate operability, systems must be maintained, reviewed, and assessed.

- Automate enterprise maintenance activities and records, where possible, to facilitate maintenance control.[156]
- Conduct periodic operational reviews to ensure unplanned modifications to the system have not occurred.[157]
- Ensure all system changes are approved through the enterprise change management process and a Change Control Board (CCB) documents the process.[158]
- Reauthorize the system, as appropriate, when modifications are performed.

2.6.5 Disposal

Systems and software must be sanitized and removed from the enterprise when they are no longer needed.

- Develop a disposal/transition plan to include the necessary steps, decisions, and approvals to close down or move information residing on a system.[159]
- Update the disposal/transition plan when required to reflect changes (i.e., security relevant changes).[160]
  - Ensure archived critical information can be retrieved for future use.
- Sanitize media by utilizing organization approved equipment and procedures to ensure confidentiality on a network system.[161]
  - Determine the appropriate sanitization process (i.e., destruction or reuse) depending on factors such as risk to confidentiality, categorization of importance, cost, and environmental impact.[162]
  - Track and document media to ensure it is not compromised during the sanitization or destruction process.
  - Periodically test the equipment and procedures used to perform sanitization.
- Decommission hardware and software as necessary when updating system components.
  - Follow organizational procedures for decommissioning hardware and software; specific requirements may be necessary when decommissioning classified hardware equipment and software for classified use.[163]

[154] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[155] Ibid.
[156] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control MA-2, "Controlled Maintenance," April 2013
[157] Ibid.
[158] Ibid.
[159] Ibid.
[160] Ibid.
[161] NIST SP 800-88 Rev. 1 (Draft), Guidelines for Media Sanitization, September 2012
[162] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008

- Ensure maintenance agreements are updated to reflect decommission activities for both hardware and software components.

Secure Lifecycle Management Informative References (Appendix A)

2.7 Information Assurance (IA) Training

Definition: The *Information Assurance (IA) Training* capability reinforces the importance of a well-informed workforce on the principles of data integrity, network security, and assuring information.

Discussion: Enterprise requirements exist for users to maintain IA awareness as well as role-based training. IA awareness is limited to activities that focus an individual's attention to a security issue.[164] Building strong information security awareness establishes required baseline security behaviors for the entire workforce.[165] Through role-based training, staff skills are maintained and frequently updated to ensure effectiveness in countering enterprise threats.[166] Implementing a robust training and awareness program is essential to enterprise security.

Example Threats: Social Engineering, Spear Phishing, Insider Threat

2.7.1 IA Awareness

Personnel must complete required trainings and obtain appropriate certifications to remain compliant with organizational and community standards.

- Require personnel, including contractors, to satisfy established standards of IA Awareness and certification requirements.[167]
  - Ensure IA awareness programs address technical, physical, personnel, and environmental concerns.
  - Refresh awareness material on a periodic basis, including updates based on new physical, logical, and environmental threats.
- Accomplish OPSEC, physical security, information security, and counterintelligence training at organizationally defined intervals.[168]
- Leverage enterprise training capabilities to communicate security awareness messages to personnel.[169]
- Ensure all personnel are trained to execute their responsibilities for incident response and continuity of operations activities.[170]

[163] NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle, October 2008
[164] NIST IR 7298 Rev. 2, Glossary of Key Information Security Terms, "Awareness," May 2013
[165] OMB Circular No. A-130 Revised, Management of Federal Information Resources, 2000
[166] NIST SP 800-16 Rev. 1 (3rd Draft), A Role-Based Model for Federal Information Technology/Cyber Security Training, March 2014
[167] Ibid.
[168] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, October 2013
[169] NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003
[170] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control IR-2, "Incident Response Training," April 2013

2.7.2 Workforce Development Requirements

An enterprise needs to align functional roles with qualified staff resources to accomplish objectives.

- Define and document roles and authorities along with assigned position responsibilities.[171]
  - Ensure knowledge, skills, and competencies for each role include technical and nontechnical requirements and basic through advanced concepts.[172]
- Designate positions to fill functional requirements to meet organizational needs.[173]
  - Determine the scope, boundaries, and operation for each position.
  - Develop specific and dynamic role requirements to ensure personnel hiring addresses the evolving needs of the organization.
  - Store documentation for future reference.
- Align hiring and workforce development requirements with established position qualifications.[174]
  - Correlate and document each IA functional requirement with a category and level.[175]
  - Categorize workforce development requirements in accordance with identified position descriptions.

2.7.3 Program Administration

Enterprise training programs require centralized administration to manage cross-cutting operational needs.

- Develop a security training policy that addresses the following areas: purpose, roles and responsibilities, management commitment, coordination among organizational entities, and compliance requirements.[176]
- Establish an IA training program to include funding, personnel, tools, methods, equipment, and courses.[177]
  - Meet with stakeholders to gather training requirements and identify gaps in existing training programs.
  - Implement, maintain, and evaluate training courses regularly to ensure training relevancy.
  - Use a variety of media to deliver training.[178]
- Maintain IA training courses, materials, and personnel training requirements through periodic reviews and updates.
  - Ensure personnel provide feedback for security awareness and training programs.[179]
  - Update the training program as the mission or environment changes (e.g., new technology or security issues).[180]

---

[171] NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006
[172] DoDI 8570.01-M, Information Assurance Workforce Improvement Program, January 2012
[173] OMB Circular No. A-130 Revised, Management of Federal Information Resources, 2000
[174] DoDI 8570.01-M, Information Assurance Workforce Improvement Program, January 2012
[175] Ibid.
[176] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AT-1, "Security Awareness and Training Policy and Procedures," April 2013
[177] NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003
[178] NIST SP 800-16 Rev. 1 , (3rd Draft), A Role-Based Model for Federal Information Technology/Cyber Security Training, March 2014
[179] NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006
[180] NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006

- Document and retain records of security training activities.[181]
  - Hold personnel accountable for compliance with training policies and procedures.
- Use a centralized performance management system to track personnel training requirements and completed training.[182]

2.7.4 Role-Based Training

Providing role based training ensures situational awareness, proper knowledge transfer, and targeted skill development to accomplish mission objectives.

- Document expected knowledge, skills, and competencies to be gained through role-based training.[183]
  - Train personnel to understand the proper scope and limitations of their role and responsibilities.
  - Ensure personnel have received appropriate training to fulfill their assigned functions.
- Require specialized training for anyone with privilege access.[184]
- Establish partnerships, when appropriate, with outside vendors or universities to fulfill additional or specialized training needs.[185]

2.7.5 Exercise and Evaluation

A Training, Test, and Evaluation (TT&E) program enables collective performance assessments to assure mission success.[186]

- Create a TT&E program to complement the training program.[187]
- Determine the portions of an IT plan that need to be exercised.[188]
- Design training exercises based on organizational needs and objectives.[189]
- Conduct functional exercises to evaluate operational readiness.[190]
  - Conduct various types of exercises (e.g., tabletop, functional, and cyber war games).[191]
- Establish mechanisms to validate the effectiveness and manage exercise maintenance and improvement.[192]
- Document lessons learned and after action reports to influence operational changes and remedy deficiencies.[193]

Information Assurance (IA) Training Informative References (Appendix A)

[181] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AT-4, "Security Training Records," April 2013
[182] NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003
[183] NIST SP 800-16 Rev. 1(3rd Draft), A Role-Based Model for Federal Information Technology/Cyber Security Training, March 2014
[184] Ibid.
[185] NIST, National Initiative for Cybersecurity Education (NICE), Component 4: Training and Professional Development
[186] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006
[187] Ibid.
[188] Ibid.
[189] Ibid.
[190] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006
[191] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, October 2013
[192] NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006
[193] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, October 2013

3 Protect

Figure 4: Protect Function Diagram

Information compromise may occur from as little as one weakness within an environment, and protections must be implemented in depth and breadth for effective security. The Protect cybersecurity function secures and ensures access to information. Procuring facilities and systems are managed leveraging Govern capabilities, whereas the Detect function assesses and monitors the effectiveness of Protection measures (i.e., a system should be tracked via the Hardware and Software Inventory capability before it is hardened within the Configuration Management capability).

The Protect capabilities establish defense in depth, beginning with physical measures that should be considered and progresses through the network architecture, device configuration, and securing data. The capabilities also establish identity and access management for a system or user by creating an identity, assigning respective attributes and metadata (including privileges) to an entity, providing respective credentials, and controlling access.

3.1 Physical Protection

Definition: The *Physical Protection* capability controls physical access and secures enterprise facilities, resources, and utilities.

Discussion: Protections must be implemented to defend against outages, malicious activity, and natural disasters and to maintain availability of physical resources. Physical protection safeguards personnel as well as enterprise information.

Example Threats: Asset Theft, Espionage, Natural Disaster, Sabotage, Terrorism

3.1.1 Physical Security Planning

Planning for physical security involves developing strategies to ensure all aspects of the physical environment, including classified or sensitive information, are properly secured.

- Identify the physical security plan's purpose, scope, security perimeter, roles, responsibilities, service agreements, and applicable regulatory and legal requirements.[194]
- Create the physical security plan to address all aspects of the physical security program (e.g., environmental controls, natural threats, facility management, fire prevention and protection, facility services, physical access controls, and portable system controls).[195]
    - Reconcile the organizational safety plans with the physical security plan to ensure cohesion and compliance with safety requirements.

[194] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-1, "Physical and Environmental Protection Policy and Procedures," April 2013
[195] NIST SP 800-16 Rev. 1 , (3rd Draft), A Role-Based Model for Federal Information Technology/Cyber Security Training, March 2014

- Identify facility services (e.g., electrical power, telecommunications, water, and Heating, Ventilation, and Air Conditioning [HVAC]) and prioritize critical services for backup.

- Use both active and passive physical security measures (e.g., guard dogs, bollards, and lighting).[196]
- Create performance metrics for physical access control mechanisms.[197]
- Identify enforcement mechanisms for removable media and sensitive document transport procedures.[198]
  - Identify courier procedures for transporting high-value and sensitive information or other assets.
- Establish varying levels of physical protections commensurate with the threat environment.[199]
  - Ensure physical protection levels are based on identified risk scenarios.[200]
  - Integrate physical security efforts with antiterrorism/force protection enhancements when required by the threat condition.[201]
  - Identify physical security procedures to coordinate with other enterprise elements (i.e., Human Resources) concerning adverse personnel events.
  - Document safe handling and security procedures to coincide with special enterprise considerations (e.g., fuel, hazardous material, and ordinance handling).
  - Enforce dual authorization for privileged or sensitive actions.

3.1.2 Facilities Security

The enterprise must integrate security considerations into the planning and construction of facilities, especially those that process and store classified or sensitive information.

- Designate a Facility Security Officer (FSO) or Physical Security personnel to oversee and ensure compliance with the security requirements during facility construction and operations.
- Coordinate physical security implementation efforts with law enforcement, emergency management, and medical organizations.[202]
  - Place work locations within an acceptable proximity to emergency services and reaction forces commensurate with organizational threats.
- Implement access control and intrusion detection mechanisms at ingress/egress points and for critical assets.
  - Leverage facility blueprints and construction plans to ensure all ingress/egress points and critical assets are secured.
- Maximize crime prevention through environmental design (CPTED) principles to enhance deterrence and detection of unauthorized personnel: [203]

[196] DoD 5200.08-R, Physical Security Program, May 2009
[197] DHS, National Infrastructure Protection Plan, 2009
[198] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control MP-5, "Media Transport," April 2013
[199] Ibid.
[200] Ibid.
[201] DoD 5200.08-R, Physical Security Program, May 2009
[202] Ibid.
[203] FEMA 430, Risk Management Series, Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks, December 2007

- Activity Support: Creates common areas where groups can congregate, enhancing the sense of "safety in numbers" (e.g., plazas and cafes).
- Maintenance: Provides validation that territorial boundaries (e.g., landscaping, border hedges), markings (e.g., signage), and technology (e.g., cameras and lighting) are maintained to avoid disruption of surveillance capabilities.
- Natural Access Control: Physically guides the flow of traffic to and from a facility (e.g., clear paths and entrances) and discourages access to private areas.
- Natural Surveillance: Maximizes the visibility of people, parking areas, and building entrances (e.g., large windows with clear line of sight).
- Target Hardening: Employs architectural elements to prohibit unauthorized access (e.g., door locks, window locks, interior door hinges, etc.).
- Territorial Reinforcement: Uses physical attributes to delineate private and public spaces (e.g., fences).

- Implement appropriate levels of access control for different areas (e.g. common and restricted areas).[204]
- Implement physical access controls to prevent unauthorized physical access to facilities, systems, or other resources.[205]
  - Develop physical access control procedures and implement mechanisms[206] using an up-to-date access control list.[207]
  - Change shared access codes (door ciphers) periodically to ensure that only personnel with current authorization and access codes can obtain entry.
  - Use biometric, electronic, and/or mechanical access control mechanisms to reduce reliance on fixed security forces.[208]
- Implement anti-tamper devices to ensure physical integrity of assets.[209]
- Incorporate significantly higher levels of protection for mission critical facilities.[210]
- Ensure redundancies for environmental control systems (e.g., electrical power, water, and HVAC) and prioritize the restoration of critical services.[211]
  - Institute fail-safe control system processes that do not cause cascading events.[212]
  - Implement tailored protections for industrial control (i.e., Supervisor Control and Data Acquisition [SCADA] systems).[213]

[204] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-3, "Physical Access Control," April 2013
[205] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
[206] Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors
[207] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-2, "Physical Access Authorizations," April 2013
[208] DoD 5200.08-R, Physical Security Program
[209] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-18, "Tamper Resistance and Detection," April 2013
[210] UFC 4-010-01, Unified Facilities Criteria (UFC) , DoD Minimum Antiterrorism Standards for Buildings, October 2013
[211] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-2, "Contingency Plan," April 2013
[212] NIST 800-82 Rev. 1, Guide to Industrial Control Systems (ICS) Security, April 2013
[213] Ibid.

3.1.3 Physical Information Security

Classified or sensitive document handling and storage requires secure environments with specific facility requirements.

- Establish specific handling and storage procedures (e.g., control logs, storage safes) for sensitive or classified information.[214]
- Ensure personnel in secure spaces are cleared to the highest level of information being handled in that area.[215]
- Implement protection mechanisms for information leakage through electromagnetic signal emanations.[216]
- Follow established Director of National Intelligence (DNI) and Department of Defense (DoD) policies to store, use, discuss, and/or process sensitive compartmented information (SCI).[217]
    - Ensure that any sensitive compartmented information facility (SCIF) construction plans include detailed security considerations (e.g., materials, escorts, and vetting of workers).[218]
- Physically destroy sensitive or classified information, in accordance with organization or community policy, to ensure that any residual medium can withstand laboratory reconstruction techniques.[219]
    - Maintain chain of custody until sensitive or classified information is destroyed.[220]
    - Ensure the correct number of witnesses are present for classified document destruction (e.g., two person integrity is required when destroying TOP SECRET documentation).[221]
    - Document destruction of physical media as directed by policy.[222]

Physical Protection Informative References (Appendix A)

3.2 Network Security

Definition: The *Network Security* capability defines security boundaries and controls the exchange of data across security perimeters.

Discussion: Security boundaries mark the separation of entities, such as enclaves or enterprises, by emphasizing the transition to or from different security policies or threat environments. Enterprise boundaries may require additional levels of security due to the increasing use of devices for secure communication outside of traditional physical boundaries (e.g., mobility and in-theater operations), while still allowing coordination and collaboration between people and resources to occur.

[214] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control MP-1, "Media Protection Policy and Procedures," April 2013
[215] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-2, "Physical Access Authorizations," April 2013
[216] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-19, "Information Leakage," April 2013
[217] Director of Central Intelligence Directive 6/1, March 2003
[218] DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), February 2006
[219] NIST SP 800-88 Rev. 1 (Draft), Guidelines for Media Sanitization, September 2012
[220] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control MP-6, "Media Sanitization," April 2013
[221] DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), February 2006
[222] Ibid.

Example Threats: Data Exfiltration, Distributed Denial of Service (DDoS), Malware, Spam

3.2.1 Security Architecture

Establishing a secure network architecture requires the implementation of mission-aligned enterprise architecture and the adoption of defense-in-depth strategies for the network.

- Develop, maintain, and facilitate the implementation of a sound and integrated IT architecture.[223]
  - Leverage the organization enterprise architecture to develop and refine security designs for systems and services.
- Ensure system interconnections are properly planned, implemented, maintained, and (if necessary) terminated.[224]
  - Coordinate with all involved parties and document mutually agreed-upon considerations (e.g., Memorandum of Understanding [MOU], Interconnection Security Agreement [ISA]).
  - Control communications at key internal and external boundaries.[225]
- Establish traffic flow policy (e.g., port filtering and content filtering) for each managed interface, including encrypted traffic.
- Design all managed interfaces using layered and secure protection devices (e.g., firewalls, gateways, routers, cross domain solutions, and email guards) for enclave boundary protection.[226]
- Ensure all managed interfaces are inventoried, physically secured, and protected from tampering.

3.2.2 Network Boundary Protection

A secure network requires a multi-tiered architecture and segmentation to protect network resources.[227]

- Establish managed interfaces at network interconnection points to provide bidirectional information screening and filtering, block prohibited traffic, and prevent data leakage.[228]
  - Configure managed interface to deny all traffic by default and only allow traffic by exception.[229]
  - Deny communications with known malicious IP addresses (i.e., blacklist) and limit access to trusted sites (i.e., whitelist).[230]
  - Limit the number of external connections.
  - Ensure managed interfaces fail securely.[231]
- Create a demilitarized zone (DMZ) for publically accessible services (e.g., email, web, and domain name systems [DNS]).[232]

---

[223] Clinger-Cohen Act of 1996, 40 U.S.C. 1401 et seq. (P.L. 104-106 Division E.)
[224] NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002
[225] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-7, "Boundary Protection," April 2013
[226] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[227] Community Gold Standard Technical Guidance: Manageable Network Plan (MNP) Ver. 3.0, September 2013
[228] NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy, September 2009
[229] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-7, "Boundary Protection," April 2013
[230] NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy, September 2009
[231] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-7, "Boundary Protection," April 2013
[232] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013

- Place DMZs as close to the network boundary as possible.
- Limit connectivity to the DMZ to specific hosts in the internal network.
- Ensure sensitive data does not reside on the DMZ.

- Segment the internal network physically and/or logically into multiple sub-networks.[233]
  - Place network security devices at the edge of security domains and at logical network boundaries.
  - Use private virtual local area networks (VLAN) for logical segregation.
  - Protect sensitive accounts in segregated networks and organizational functions.
- Deploy a split (i.e., hierarchical) DNS structure in which machines on the internal network are configured to send requests to DNS servers.[234]
  - Employ multiple authoritative name servers.[235]
  - Verify the authenticity and integrity of DNS responses.[236]
- Provide remote access through a service that provides both confidentiality and integrity assurance, such as a Virtual Private Network (VPN).[237]
  - Provide two-way authentication between the remote user and local system each time a connection is attempted.
  - Permit encrypted traffic to traverse only approved access points in the case of site-to-site VPN implementations.
  - Individually verify VPN connections each time a connection is attempted.
- Manage network boundary protection solutions using an out-of-band network.[238]

3.2.3 Managing Ports, Protocols, and Services

Proper management and correlation of ports, protocols, and services is required to mitigate risk across the enterprise.

- Identify all available ports, protocols, and services and determine which of these should be allowed based on the mission need and risk to the enterprise.
- Document all ports, protocols, and services that are accessible to the enterprise in a centralized registry.[239]
- Configure boundary devices to use approved ports, protocols, and services.[240]
  - Limit the use of ports, protocols, and services by allowing only those required to support the mission and conduct official business.[241]

---

[233] Community Gold Standard Technical Guidance: Manageable Network Plan (MNP) Ver. 3.0, September 2013
[234] NIST SP 800-81 Rev. 1, Secure Domain Name System (DNS) Deployment Guide, April 2010
[235] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-22, "Architecture and Provisioning for Name/Address Resolution Service," April 2013
[236] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-21, "Secure Name/Address Resolution Service (Recursive or Caching Resolver)," April 2013
[237] NIST SP 800-77, Guide to IPsec VPNs, December 2005
[238] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-7, "Boundary Protection," April 2013
[239] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-7, "Boundary Protection," April 2013
[240] Ibid.
[241] Ibid.

- Implement physical (i.e., anti-tamper) and/or logical protections to disable all unused or unnecessary ports, protocols, and services.[242]
- Use web DNS reputation services to detect and block access to malicious web pages.

Network Security Informative References (Appendix A)

3.3 Hardware and Software Inventory

Definition: The *Hardware and Software Inventory* capability identifies and tracks all hardware and software assets.

Discussion: Hardware and software inventories encompass all assets placed on an enterprise system, and have security implications due to the transfer of data within the system. Identifying all assets within an enterprise assists organizations in maintaining accurate records and provides the ability to detect lost and unauthorized assets, and to prevent threats.

Example Threats: Malware, Rogue Devices, Theft, Unauthorized Software

3.3.1 Identify Hardware and Software Assets

Hardware and software inventories contain information that enables secure configuration management and tracking for each asset, including removable media and wireless access points.

- Develop an organizational policy to govern whether virtual machines (VM) are classified as hardware or software assets.
- Employ a consistent naming schema for hardware and software assets.
    - Uniquely identify hardware devices.[243]
- Define a consistent method to link the hardware inventory to the software inventory.[244]
- Establish cohesive inventory procedures with the organizational Privacy Program to ensure all inventories remain updated.[245]
- Identify assets and associated information relevant to configuration management.[246]
    - Employ automated discovery tools to create a preliminary asset inventory.[247]
    - Include information such as hardware inventory specifications, software license information, software version numbers, component owners, machine names, network addresses, manufacturer, device type, model, serial number, and physical location.[248]
    - Include periodic manual inventories to ensure legacy equipment is detected.

[242] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-41, "Port and I/O Device Access," April 2013
[243] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control IA-3, "Device Identification and Authentication," April 2013
[244] Council on CyberSecurity, The Critical Security Controls for Effective Cyber Defense Ver. 5, CSC 2, "Inventory of Authorized and Unauthorized Software," February 2014
[245] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SE-1, "Inventory of Personally Identifiable Information," April 2013
[246] NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
[247] Council on CyberSecurity, The Critical Security Controls for Effective Cyber Defense Ver. 5, CSC 1, "Inventory of Authorized and Unauthorized Devices," February 2014
[248] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-8, "Information System Component Inventory," April 2013

- Employ a method for identifying different versions of the same software (e.g., copy number).
- Ensure that any available production source code is inventoried and stored in a repository.

- Ensure that each hardware asset is associated with exactly one information system.[249]
  - Confirm that the asset owner acknowledges the information system association.[250]
  - Notify the system owner of changes to the associated asset.

3.3.2 Manage Hardware and Software Inventories

Up-to-date and accurate inventories enable the organization to track and manage details (e.g., location, configuration details, and ownership) of hardware and software assets.

- Determine and authorize which personnel and processes are granted access to modify or use inventory databases.
- Hold all assets in the inventories in complete, consolidated, accurate, scalable, stored, up-to-date, and centrally maintained inventory databases.[251]
  - Track all purchase requests and acquisitions.
  - Verify receipt of hardware and software deliverables.
  - Update inventory when assets are installed, changed, or removed.[252]
  - Track and monitor the location of assets using asset location technologies.[253]
  - Inventory offline hardware components by date and status (i.e., whether hardware components are checked-in or checked-out).
  - Provide a near real-time account of discoverable hardware and software in the environment.[254]
  - Maintain an up-to-date inventory of hardware spares and portable media.
- Indicate how software assets are incorporated into the inventory (i.e., through a manual or automated process).
- Test the implementation of hardware and software inventories for effectiveness.[255]
- Correct inventory inaccuracies, using a root cause analysis to determine the source.
- Perform inventories periodically, in a timeframe determined by asset criticality.
  - Use Security Content Automation Protocol (SCAP)-validated inventory processes when possible.[256]
  - Conduct manual inventories for devices that may be air-gapped or adversely affected by automated tools (e.g., SCADA systems).

[249] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-8, "Information System Component Inventory," April 2013
[250] NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
[251] Ibid.
[252] Ibid.
[253] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-20, "Asset Monitoring and Tracking," April 2013
[254] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-8, "Information System Component Inventory," April 2013
[255] Council on CyberSecurity, The Critical Security Controls for Effective Cyber Defense Ver. 5, CSC 1, "Inventory of Authorized and Unauthorized Devices," and CSC 2, "Inventory of Authorized and Unauthorized Software," February 2014
[256] NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011

3.3.3 Detect Undocumented Assets

Undocumented assets must first be detected in order to be properly handled (e.g., inventoried or removed from the network).

- Employ active and passive network scanning tools to identify assets on the network.[257]
  - Verify or audit the asset database and inventory using either external or internal sources.
  - Compare inventories and scanning results to identify undocumented or unauthorized hardware and software.[258]
- Generate alerts for detected inconsistencies between expected and existing assets.[259]
  - Ensure that detection occurs within 24 hours of the addition of assets to the network.[260]

Hardware and Software Inventory Informative References (Appendix A)

3.4 Configuration Management

Definition: The *Configuration Management* capability establishes configuration baselines and controls changes made to hardware, firmware, and software.

Discussion: Configuration management[261] provides a standardized baseline for enterprise information systems. When properly implemented,[262] configuration management enables the organization to establish an agile environment, where changes can be quickly implemented to respond to mission evolution. These changes must be implemented safely to ensure that the enterprise security posture is unaffected, and that risks are managed appropriately. Continuous monitoring, mitigation, remediation, and reporting of system configurations are all necessary elements of a successful configuration management plan.

Example Threats: Advanced Persistent Threat (APT), Malware, Unauthorized Configuration Changes

3.4.1 Develop Configuration Management Plans

Configuration Management Plans are important for managing, operating, and protecting an enterprise. These plans must be protected from access or modification by unauthorized users, but should be accessible to those who need to use and update them.

- Develop configuration management plans at the enterprise, network, and system levels.[263]
  - Enterprise: The enterprise-level configuration management plan should set the enterprise baselines and provide for a consistent, coordinated use of configuration management resources throughout the enterprise.

[257] Council on CyberSecurity, The Critical Security Controls for Effective Cyber Defense Ver. 5, CSC 1, "Inventory of Authorized and Unauthorized Devices," February 2014
[258] NSA, A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS) Ver. 1.1, August 2010
[259] Council on CyberSecurity, The Critical Security Controls for Effective Cyber Defense Ver. 5, CSC 1, "Inventory of Authorized and Unauthorized Devices," and CSC 2, "Inventory of Authorized and Unauthorized Software," February 2014
[260] Ibid.
[261] Configuration Management is not listed in the IA glossary, but is presented as "Configuration Control" as follows: Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation. SOURCE: CNSSI-4009, National Information Assurance (IA) Glossary, April 2010
[262] Community Gold Standard Technical Guidance: Manageable Network Plan (MNP) Ver. 3.0, September 2013
[263] NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011

- Networks and Systems: Network and system devices should be compliant with the enterprise baseline. If mission needs dictate, enterprise leadership may approve deviations from the standard baseline. The configuration management plan should document and describe the locations of any network, component, and system configurations used by the enterprise.
- Ensure that Configuration Management Plans are centrally managed, protected, and accessible for reference.

3.4.2 Establish and Maintain Baseline Configurations

The enterprise can protect the products and services that are part of its information systems environment by establishing and maintaining standard enterprise configuration baselines.[264]

- Review functions and services provided by information systems or individual components of information systems to ensure least functionality is achieved.[265]
  - Disable unnecessary and vulnerable ports, protocols, services, and accounts.
  - Prohibit unauthorized machine to machine communications.
  - Remove all unnecessary executables and registry entries.
  - Employ supplemental controls to protect network components that cannot be adequately configured.
- Implement application whitelisting to ensure only authorized software and applications are allowed to execute on the network.[266]
  - Deploy software with the latest anti-exploitation features.
  - Obtain patches from a trusted source inventory.[267]
  - Maintain and update whitelists when applications are installed, changed, or removed.
  - Employ location based application whitelisting to allow execution of programs only from specific locations in the file systems.
- Create secure baseline images for operating systems (OS) and common application software used by the organization.
- Deploy secure baseline configurations, including approved patches, in a timely manner from a centralized location using automated means.
- Ensure "mission-tuned configurations" are documented and maintained to allow reestablishment or reconstitution if failures, attacks, or catastrophes occur.
  - Test configuration changes in a nonproduction environment to determine impact and stability.
- Perform regression testing to verify functionality of configuration changes.

[264] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-2, "Baseline Configuration," April 2013
[265] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-7, "Least Functionality," April 2013
[266] [266] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-7, "Least Functionality," April 2013
[267] NIST SP 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies, July 2013

3.4.3 Control Configuration Change

CCBs provide a critical oversight role by considering the risks of each configuration change, and how it will impact the organization's overall security posture.[268]

- Manage configuration changes through an authorized CCB.
- Create emergency procedures to identify proper handling of configuration changes that must be expedited due to mission needs.
- Review configuration changes and other operational attributes to prioritize and make an informed risk decision.
- Analyze the security impact of configuration changes through a Configuration Review Board (CRB) and report findings to the CCB.[269]
- Update supporting and security-related documentation following configuration changes.[270]
- Conduct reassessment and reauthorization activities following security-relevant system changes, an attack, or a change in the threat landscape.
- Archive configurations for future reference.[271]
    - Retain prior configurations to allow for a "rollback" to a previous configuration, should there be an issue with an update.
    - Maintain historical records of all configuration changes made within the enterprise to allow reconstitution and recovery if required.
    - Maintain archives in a secure state consistent with the system impact level.

3.4.4 Vulnerability Management

Effective vulnerability management tracks and remediates potential vulnerabilities to help ensure that system configurations are kept up to date.[272]

- Monitor security sources (e.g. National Vulnerability Database) for known vulnerabilities, threats, and remediations.[273]
- Create a database of remediations for organization implementation.[274]
    - Use automated patch management tools to update the remediation database.
- Require system administrators to document and report risk-based decisions not to deploy a remediation.[275]
- Deploy remediations on all systems subject to the vulnerability.[276]
    - Test and document all deployed remediations.

---

[268] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-3, "Configuration Change Control," April 2013
[269] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control, CM-4 "Security Impact Analysis," April 2013
[270] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control, SA-5 "Information System Documentation," April 2013
[271] NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
[272] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SI-2, "Flaw Remediation," April 2013
[273] NIST SP 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program, November 2005
[274] Ibid.
[275] Ibid.
[276] Ibid.

3.4.5 Monitor System Configurations

Monitoring allows the enterprise to ensure that the system is operating with the correct configuration, and facilitates identification of unauthorized or improperly executed changes.[277]

- Identify automated monitoring tools that collect information on the configuration of all components and assess them against policy and approved baseline configurations.
- Implement and manage tools for secure configuration monitoring.
- Deploy automated validation mechanisms to enforce configuration baselines.
- Enforce application whitelisting to ensure only authorized software and applications are allowed to execute on the network.
- Enforce handling procedures for unauthorized or improperly implemented configuration changes.
- Report auditing that results from monitoring of configuration settings and use of maintenance tools to appropriate organizational entities.[278]

Configuration Management Informative References (Appendix A)

3.5 Data Protection

Definition: The *Data Protection* capability secures data from unauthorized modification, destruction, or disclosure.[279]

Discussion: Data is threatened by intentional or unintentional (e.g., human error) attacks. Multiple types and degrees of protections need to be considered to ensure the security of data. Additionally, data within the environment must be protected in each of the three potential states: in transit, in use, and at rest.

Example Threats: Data Exfiltration, Data Spillage, Insider Threat, Man in the Middle

3.5.1 Identify Protection Requirements

Each type of data requires different mechanisms and degrees of protection depending on its availability, sensitivity, classification, or regulation requirements.

- Identify the protection requirements for all data within the enterprise environment. When identifying requirements, consider the following criteria:
  - Type of data to be protected (e.g., PII)
  - Type of protection required (e.g., Full Disk Encryption)
  - Degree of protection required (e.g., strength of encryption key)
  - Conditions within the environment (e.g., who needs access, where the data exists, how it is stored, processed, or transmitted)
- Develop a mitigation response plan to address any sensitive data breaches, integrity failures, and non-availability. [280]
- Develop a plan for data resilience, to include data backup.

[277] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CM-6, "Configuration Settings," April 2013
[278] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-6, "Audit Review, Analysis, and Reporting," April 2013
[279] CNSSI-4009, National Information Assurance (IA) Glossary, April 2010
[280] CNSSI-1001, National Instruction for Classified Information Spillage, February 2008

- Identify all internal and external communication (e.g., information flows between servers, client hosts, networks, and applications) that needs to be protected.[281]

3.5.2 Implement Protection Mechanisms

To minimize the attack surface, only necessary information should reside on the network and security measures, such as encryption, should be utilized.

- Segregate data by type (e.g., sensitivity, classification, or regulation levels).
- Ensure systems protect the confidentiality and integrity of all information in accordance with the organizational risk posture.[282]
- Protect sensitive data based on confidentiality impact levels, operational safeguards, privacy-specific safeguards, and security controls.[283]
    - Apply the appropriate safeguards for sensitive data confidentiality impact levels (low, moderate, or high).
    - Conduct Privacy Impact Assessments to identify and mitigate risks within a system.
    - Establish detailed handling and reporting requirements when protecting classified information.[284]
    - Centrally manage and coordinate all services that enable sharing or transfer of information across multiple security levels.[285]
- Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all information on system components outside of organizational facilities (e.g., data on removable media and portable devices).[286]
- Ensure all encryption mechanisms provide confidentiality, integrity, and authentication services.
- Ensure the confidentiality of communication by using encryption and allowing access only to the parties sharing data.
    - Use implementation measures, such as VPN, to ensure Internet Protocol Security (IPsec) standards are met to secure private communications over networks.
    - Secure components for telework and remote access solutions using technologies or compensating controls protecting data at rest, in transit, and in use.[287]

3.5.3 Maintain Protection Mechanisms

Once implementation measures have been set in place, the maintenance process validates data security on a network.

- Establish a privacy program addressing Fair Information Practices (Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability).[288]

[281] NIST SP 800-77, Guide to IPsec VPNs, December 2005
[282] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SC-28, "Protection of Information at Rest," April 2013
[283] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
[284] CNSSP-18, National Policy on Classified Information Spillage, June 2006
[285] Department of Defense Information Enterprise Architecture (DoD IEA), July 2012
[286] Ibid.
[287] NIST SP 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security, June 2009
[288] Ibid.

- Establish a system and/or program to address classification, safeguarding, and declassification of national security information, including original classification, derivative classification, declassification, downgrading, safeguarding, implementation, review, and general provisions.[289]
- Implement data protection solutions that are centrally managed, protected from interference, and persistently available.
- Perform periodic audits of the enterprise to determine if sensitive data is present without protections.[290]
- Perform periodic scans to determine if the communications infrastructure is secure.[291]
- Expunge data from storage media or destroy the media itself to prevent unauthorized disclosure of information.[292]
- Ensure data is protected throughout its entire lifecycle.[293]

Data Protection Informative References (Appendix A)

3.6 Identity Management

Definition: The *Identity Management* capability definitively associates and maintains globally unique identifiers to verify users and non-human entities.

Discussion: Person and non-person identities must be validated to gain access to sensitive information and locations where sensitive information resides to prevent identity breaches and unauthorized access to information. Unique identifiers are created and issued, distributed, managed, and archived throughout the lifecycle of the identity verification process.

Example Threats: Impersonation, Masquerading, Privilege Escalation, Spoofing

3.6.1 Create and Issue Unique Identifiers

Creating and issuing unique identifiers includes collecting and correlating information from verified trusted sources and adjudicating inconsistencies in subject information prior to issuing an identity.[294]

- Require the physical presence of the subject, as well as the validation of multiple authentication factors, for identity proofing in the registration process.[295]
- Use the highest applicable assurance level for the type and strength of the identity proofing mechanism, and the tokens that transfer them, during the identity registration process.
- Validate and record identity evidence presented in support of an identity creation.
- Provide a globally unique identifier for each entity in the enterprise to ensure functionality within a dynamic, federated, globally distributed enterprise.

[289] DoDM 5200.1 Vol. 1, Information Security Program: Overview, Classification, and Declassification, February 2012
[290] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-6, "Audit Review, Analysis, and Reporting," April 2013
[291] Ibid.
[292] For more information on Data Sanitization, see NIST SP 800-88 Rev. 1 (Draft), Guidelines for Media Sanitization, September 2012
[293] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SI-12, "Information Handling and Retention," April 2013
[294] NIST SP 800-103 (Draft), An Ontology of Identity Credentials Part 1: Background and Formulation, October 2006
[295] The registration and identity proofing processes are designed based on the required assurance level of the organization, to ensure that the RA/CSP knows the true identity of the applicant. [NIST SP 800-63-2, Electronic Authentication Guideline, August 2013]

- Ensure identifiers are included within low bandwidth environments.

3.6.2 Distribute Unique Identifiers

Identity distribution should be consolidated and maintained at the enterprise level.[296]

- Update changes to the identity directory throughout the enterprise at a regularly defined interval to verify the state of an identifier (e.g., new, modified, or disabled).
- Ensure the identity directory is secure and available to enterprise resources for authentication activities.

3.6.3 Maintain Unique Identifiers

Unique identifiers need to be maintained and archived to continuously ensure the security of individual identities.

- Manage identities through enterprise plans and policies addressing:[297]
  - The establishment of unique digital identities through frameworks and schemas.
  - The utilization of identity data.
  - The protection of PII.
  - The control of identity data access.
  - The management of identity data.
  - The development of remediation processes to solve issues or defects with identity data and validation mechanisms.
  - The capability to share authoritative identity data across applications.
  - The system that provides the functions to manage identity.
- Periodically validate the status of the identifiers and compare them with other authoritative repositories to establish identities (e.g., source databases or accreditation databases).
- Use automated means for universal updates of identifiers, ensuring proper identifier archiving.
- Disable user accounts associated with inactive identifiers within an organizationally defined timeframe.

Identity Management Informative References (Appendix A)

3.7 Attribute Management

Definition*:* The *Attribute Management* capability establishes, publishes, and maintains properties associated with enterprise entities.

Discussion: The Attribute Management Capability is responsible for the properties or characteristics—referred to as attributes—associated with entities (e.g., individuals, groups, systems, or components) and data in the enterprise. [298] The binding of attributes with subjects and objects is used to enable data discovery, determine entity privileges, and implement access control policies.

Example Threats: Data Spillage, Excessive Privileges, Inconsistent Privileges, Insider Threat

[296] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0, December 2011
[297] Ibid.
[298] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-16, "Security Attributes," April 2013

3.7.1 Establish Secure Attributes

Attributes are established within a network to secure accessed information and validate authorization.

- Provide attributes to all entities and objects to support access decisions.[299]
  - Associate an entity's information assurance and security metadata with data assets to enable trust.[300]
  - Reduce the number of attributes used for Attribute Based Access Control (ABAC) to those necessary to implement a granular access policy.
  - Resolve conflicting attribute definitions to improve performance of the attribute management process.[301]
- Ensure entities with attributes that grant privileged access receive additional scrutiny.[302]
  - Separate duties to minimize the risks associated with the abuse of authorized privileges.[303]
  - Employ the principle of least privilege, ensuring entities are assigned only the necessary attributes to perform duties.[304]
- Establish an authoritative attribute repository for reference at the enterprise, enclave, and system levels.[305]
- Identify the appropriate attributes used to determine an entity's authorization based on role, function, mission, policy, sensitivity of data, and other object characteristics.
- Ensure the classification type and level, controlled access programs, foreign government information, dissemination controls, disclosure and release determinations, and other warnings are reflected within the attributes of any classified intelligence document.[306]
- Establish a name, definition, set of finite allowable values, and an assigned schema that guides how each attribute will be used.[307]
  - Ensure standardized syntax and protocols are used for the generation and maintenance of IA metadata.[308]
- Apply standardized attribute tagging, retrieval, and dissemination to increase discoverability, accessibility, and availability, and to promote information sharing throughout the NSS.[309]
- Define assurance level, quality, and service expectations for attributes.[310]

---

[299] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-16, "Security Attributes," April 2013
[300] DODD 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, August 2013
[301] Ibid.
[302] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-2, "Account Management," April 2013
[303] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-5, "Separation of Duties," April 2013
[304] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-6, "Least Privilege," April 2013
[305] Ibid.
[306] ICD 710, Classification Management and Control Markings System, June 2013
[307] Ibid.
[308] Ibid.
[309] CNSSP-24, Policy on Assured Information Sharing (AIS) for National Security Systems (NSS), May 2010
[310] Ibid.

3.7.2 Publish Attributes

Attributes must be made available to enable mission functions while ensuring integrity.

- Publish attributes to the authoritative repository for use by authorized users and systems.
- Provide assurance that published attributes have not been improperly accessed or altered.
- Share attributes and authoritative repositories with other enterprises, as appropriate and required for interoperability.

3.7.3 Maintain and Update Attributes

Attributes must be managed and updated to ensure intended access is granted and the security of the attributes is protected.

- Centrally manage attributes within the enterprise through an integrated lifecycle approach, using automated means if possible. [311]
- Protect attributes from improper access and alteration.[312]
- Examine all IA metadata to ensure it adheres to the correct syntax and complies with the appropriate policies at ingest.
- Track modifications to attributes within the authoritative repository.
- Permit caching of attributes with minimal time to live (TTL) when the mission requires (e.g., disconnected operations, areas with low bandwidth, or low storage capacity).

Attribute Management Informative References (Appendix A)

3.8 Credential Management

Definition: The *Credential Management* capability creates, issues, and maintains objects (i.e., credentials) that authoritatively bind an identity and attributes to a token possessed and controlled by a subject.[313]

Discussion: Credential Management is the means of asserting digital identity (Identity Management) and permissions (Attribute Management) to create a secure enterprise where only those with a need to know can access information. Operating in a digital environment requires enterprises to control access to their systems.

Example Threats: Collusion, Impersonation, Insider Threat, Masquerading, Privilege Escalation, Spoofing

3.8.1 Create and Issue Credentials

Identities and attributes must be correctly created, issued, verified, and bound to the proper credentials.

- Establish formal agreements with partner organizations to increase interoperability by deconflicting identifiers.
- Create unique credentials that bind a digital identity to attribute information (e.g., public key), the issuer of the credential, and other relevant information (e.g., issue date or expiration date).
- Include the following information when the credential being generated is a certificate:

[311] NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014
[312] NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-4 and multiple enhancements, "Information Flow Enforcement," April 2013
[313] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Ver. 2.0, December 2011

- Identification of the certification authority issuing the certificate.
- Name or identity of the subscriber.
- Subscriber's public key.
- Identification of the operational period (during which the certificate may be used).
- Digital signature of the certification authority issuing the certificate.[314]

- Generate credentials in a secure manner,[315] and protect the systems generating the credentials.[316]
  - Assign an expiration date to each credential when issuing credentials.
  - For lower levels of assurance, remote registration may be used. For the highest level of assurance, additional security measures such as in-person registration are required. [317]
- Ensure a high degree of confidence in issued credentials[318] by verifying the strength of encryption, digital signatures, random number generation, key agreement, key transport, key wrapping, deriving additional keys, hash functions, Message Authentication Codes (MAC),[319] and tokens that transfer credentials.[320]
- Deliver or otherwise make the credential available to the subscriber.
- Track the credentials issued to the subscriber for each token.

3.8.2 Maintain Credentials

The maintenance process provides assurance that credential validity is continued and that credentials are properly revoked when needed.

- Deploy an automated credential management service where the Credential Service Provider (CSP)[321] is able to track and maintain credentials.[322]
- Ensure Credential management systems are centrally managed, protected from disruptions, and accessible.
  - At each level of assurance, the requirements for secure storage, verification, renewal/re-issuance, revocation/destruction, records, and security controls increase.[323]
- Notify the subscriber when credential expiration is approaching to allow a request for renewal or re-issuance to be submitted.

[314] NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001
[315] Section 6 of the NIST SP 800-63-2 offers guidance for secure credential management, and provides mitigations for common token and credential threats. August 2013
[316] NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
[317] OMB M-04-04 Memorandum to the Heads of All Departments and Agencies, E-Authentication Guidance for Federal Agencies, December 2003
[318] For more detailed issuance processes on specific types of credentials refer to the FICAM Roadmap and Implementation Guidance.
[319] NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[320] NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
[321] A Credentials Service Provider is a trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. SOURCE: CNSSI 4009, National Information Assurance (IA) Glossary, April 2010
[322] M-04-04, Memorandum to the Heads of All Departments and Agencies, E-Authentication Guidance for Federal Agencies, December 2003
[323] NIST SP 800-63-2, Electronic Authentication Guideline, August 2013

- Maintain records of revocations, renewals, and updates for all credentials to ensure a user's identity is validated.
    - Maintenance is performed by the business process owner, designated agency, or cross-agency authority.[324]
- Revoke and/or destroy credentials as soon as notification is received that the credentials should be revoked or destroyed.
    - This revocation determination can be the result of a policy, account expiration, change in employee status, or manual deletion by an authorized system administrator.

Credential Management Informative References (Appendix A)

3.9 Logical Access Control

Definition: The *Logical Access Control* capability authenticates and authorizes entity permissions against a logical resource.

Discussion: Centralized logical access control mitigates risks by working in concert with Credential Management, Identity Management, and Attribute Management to ensure personnel and systems have access to necessary information to support the mission, and that access is not provided to those without a need to know. Logical access control standardizes the way access decisions are made across enterprise information systems.[325]

Example Threats: Data Spillage, Impersonation, Insider Threat, Non-Compliant Devices, Rogue Devices

3.9.1 Resource Authentication

Authentication is the process of verifying the identity or other attributes claimed by or assumed of an entity (i.e., user, process, or device), or to verify the source and integrity of data.[326]

- Perform authentication of entities prior to allowing access to network resources.[327]
- Enforce password complexity and expiration requirements.
    - Enforce a limit for unsuccessful authentication attempts.[328]
- Enforce multifactor authentication for all entities requesting access to network resources.[329]
    - Restrict systems that privileged accounts can access.
    - Remove standard users from the local administrative group.

[324] M-04-04, Memorandum to the Heads of All Departments and Agencies, E-Authentications Guidance for Federal Agencies, December 2003
[325] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0, December 2011
[326] CNSSI-4009, National Information Assurance (IA) Glossary, April 2010
[327] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control IA-2, "Identification and Authentication (Organizational Users)," and IA-8, "Identification and Authentication (Non-Organizational Users)" April 2013
[328] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-7, "Unsuccessful Logon Attempts," April 2013
[329] Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004

- Ensure periodic re-authentication is enforced when authenticators change, roles change, security categories of information systems change, executions of privileged functions occur, a fixed period of time elapses, or when session inactivity occurs.[330]
- Remove network and remote interactive logon privileges from local, non-service, and administrator accounts.

3.9.2 Resource Authorization

Authorization grants access privileges to entities[331] and provides a framework for combining information about resources, users, and the environmental context to make access determinations.

- Verify all resources have access policies assigned to them.[332]
    - Ensure the access policy contains rules that specify how to determine authorization by comparing the requesting entity's attributes against the resource's attributes.
    - Enforce dual authorization for privileged or sensitive actions.
- Deploy automated access management systems to enforce authorization decisions for logical access.[333]
- Ensure access management systems are centrally managed, protected from disruptions, and accessible.
- Invoke access control mechanisms for a user or non-human entity requesting access to a resource.[334]
- Establish a process to handle situations where the implemented access controls do not adequately address individual, group, or non-person entity operational authorities.
- Use ABAC for the most flexibility in implementing the roles and authorities of groups and individuals.[335]

Logical Access Control Informative References (Appendix A)

[330] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-11, "Session Lock," April 2013
[331] CNSSI-4009, National Information Assurance (IA) Glossary, April 2010
[332] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-3, "Access Enforcement," April 2013
[333] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-24, "Access Control Decisions," April 2013
[334] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0, December 2011
[335] ICPG 500.2, Attribute-Based Authorization and Access Management, November 2010

4 Detect

Figure 5: Detect Function Diagram

An enterprise cannot maintain security without vigilance. The Detect cybersecurity function provides guidance to accomplish situational awareness. Protect capabilities may discuss programmatic monitoring, but the Detect function implements the enterprise security monitoring functions. Industry continuous monitoring initiatives and technologies may relate to other capabilities, but the intent is described within the Detect function. The Detect capabilities establish security monitoring within the enterprise by detecting anomalies and attacks from people, processes, and technology.

4.1 Security Evaluations

Definition*:* The *Security Evaluations* capability comprehensively analyzes a system or network, identifies vulnerabilities, and provides feedback to system owners.

Discussion: Security evaluations assist organizations with protecting the security posture of the environment by identifying vulnerabilities in systems, networks, architectures, and processes. A combination of continuous vulnerability scanning and independent security evaluation offers the enterprise a means of obtaining objective assessment information. Security evaluations identify weaknesses and provide vulnerability assessment results for leadership to make risk-based decisions for the enterprise.

Example Threats: APT, Data Exfiltration, Malware

4.1.1 Security Evaluation Planning

Determining the appropriate scope and approach of the security evaluation establishes how an organization plans to identify vulnerability gaps within the enterprise.

- Review published vulnerabilities and prior assessment reports to identify known or potential gaps.
- Identify vulnerability scanning tools to enumerate vulnerabilities within the enterprise.
- Identify the scope of the assessment.
- Identify a security evaluation approach or set of approaches, including Blue Teams, Red Teams, and internal vulnerability assessments to review the security posture of the enterprise.[336,337]
    - Blue Team: Conducts independent system and network vulnerability evaluations, providing a technical review of a network's security posture. Blue Team evaluations identify security threats and risks and provide recommendations to improve the network security posture. Blue Team evaluations may be conducted as part of the development process, to provide internal metrics, or in preparation for a Red Team assessment.

[336] CNSSI-4009, National Information Assurance (IA) Glossary, April 2010
[337] NIST SP-800-115, Technical Guide to Information Security Testing and Assessment, September 2008

- Vulnerability Assessment: Conducts internal reviews—continuous or periodic—of enterprise networks to assess security, identify gaps, and evaluate applied mitigations.
- Red Team: Emulates adversary attacks and/or exploits against the enterprise to independently identify network vulnerabilities and assess enterprise defensive capabilities.

- Develop rules of engagement[338] to ensure security evaluations are conducted in accordance with all policy, legal, and enterprise requirements.

4.1.2 Security Assessments

Security evaluations may be conducted to assess enterprise or network security postures in support of continuous monitoring, to prepare for external assessments, in response to cyber incidents or suspected vulnerabilities, or as a routine part of system development.

- Utilize a defined set of security protections applicable to the enterprise to conduct security evaluations.
- Conduct Blue Team Evaluations to assist in the following:[339]
  - Determining the security posture of an environment.
  - Evaluating roles of an organization as well as individual employees.
  - Prioritizing identified vulnerabilities.
- Conduct vulnerability scans to assess the security posture of the enterprise.[340]
  - Use security classification guides[341] to classify vulnerabilities.[342]
  - Identify security gaps associated with detected vulnerabilities.
- Determine how the Red Team operations will occur at the organizational level:[343]
  - Utilize the appropriate resources (personnel and techniques).
  - Execute operations in compliance with the law.
  - Focus on system and network level security.
  - Perform external testing before internal testing.
- Prioritize vulnerability information based on device mission, potential impact, and location on a network (e.g., operational versus non-operational, behind a firewall versus wider exposure, test lab).

4.1.3 Vulnerability Mitigation and Response

Once security evaluation results have been analyzed and documented, mitigation and response strategies are developed, and results are provided to assist stakeholders with assessing and maintaining their security postures.

- Consider how identified vulnerability trends may affect the enterprise.
- Compose and review analysis to minimize false positives.

---

[338] PPD 20, U.S. Cyber Operations Policy [Classified]
[339] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[340] Ibid.
[341] An index of security classification guides aimed at assisting DoD component officials is available at http://www.dtic.mil/dtic/stresources/standards/securityclassindex_desc.html.
[342] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[343] Ibid.

- Score and report results based on the analysis of vulnerability information.
- Develop mitigation strategies to address identified vulnerabilities.[344]
  - Allocate resources to address high-priority vulnerabilities.
  - Determine whether to accept or mitigate risks associated with lower priority vulnerabilities.
- Provide Red Team and Blue Team Assessment reports to leadership for review.[345]
  - Develop response plans, including mitigation strategies, based on evaluation findings.
  - Schedule additional evaluations to assess mitigations.
  - Share vulnerability information with peer organizations as appropriate.
- Track and work toward addressing identified vulnerabilities.[346]
- Verify effective mitigations through re-evaluation.
- Remove or protect assessment data (and consolidated vulnerabilities) from the network as soon as feasible to prevent the information from being compromised.
- Collect and share lessons learned across the enterprise and with stakeholders, as appropriate.

Security Evaluations Informative References (Appendix A)

4.2 Physical Enterprise Monitoring

Definition: The *Physical Enterprise Monitoring* capability maintains awareness of physical access and the status of enterprise facilities, resources, and utilities, while ensuring that affiliates have and maintain proper authorization and clearances.

Discussion: Within the physical enterprise, facilities and utilities must remain available and monitored to ensure information and operations are not compromised. Careful monitoring of personnel, records, and physical access to these resources reduces risk to the enterprise. As with logical access control, management of physical access is particularly important when dealing with facilities housing classified information.

Example Threats: Asset Theft, Impersonation, Insider Threat, Terrorism, Unauthorized Physical Access

4.2.1 Facilities and Utilities

Threats in the physical environment can impact enterprise systems, buildings, and supporting infrastructure.

- Detect anomalies associated with the physical components of a network and with the facilities in which the network resides (e.g., tampering, system malfunctions, or unauthorized access).[347]
- Perform evaluations (e.g., TEMPEST or Technical Surveillance Countermeasures [TSCM]) of physical protections.[348]

[344] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
[345] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[346] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
[347] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-3, "Physical Access Control," April 2013
[348] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control RA-6, "Technical Surveillance Countermeasures Survey," April 2013

- Monitor physical systems (e.g., workstations, case sensors, or routers), environmental systems (e.g., HVAC), and unauthorized cell phone usage through automated monitoring tools.[349]
    - Detect prohibited use of wireless technologies in facilities that house classified data.[350]
    - Obtain alerts including the date and time information was captured, location, system information, type of event, and who or what reported the alert.[351]
- Identify and monitor sensitive unclassified facilities information that may have OPSEC implications.[352]

4.2.2 Physical Access Control

Unauthorized physical access to systems and facilities poses numerous security risks, including threats to data integrity and personnel safety.

- Use a combination of manual and automated means to detect physical intrusions and provide notification of the presence of unauthorized individuals.[353]
    - Develop a layered physical access control plan confirming facility, work area, and data center access and justification prior to granting access.
    - Provide assurance that personnel and visitors granted access to facilities, resources, and information are properly cleared to access them.[354]
    - When appropriate, implement mandatory escort requirements for any sensitive environment access (e.g., data center).
    - Ensure that individuals accessing classified facilities, resources, and information have a need to know.[355]
    - Monitor suspicious physical access (e.g., access outside of normal work hours, access for unusual lengths of time, or access to areas not required by duties).[356]
- Monitor physical access audit logs for entry and exit points.[357]

4.2.3 Personnel Screening and Reinvestigation

Access to sensitive or classified information must be controlled through standardized processes of screening, indoctrination, reevaluation, and debriefing.

- Conduct a background investigation on all affiliates in accordance with the investigative protocols outlined in community policies.[358]
    - Screen affiliates using a variety of processes (e.g., background investigations, National Agency Checks, Local Agency Checks, and polygraph examinations).[359]

[349] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
[350] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, October 2013
[351] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-6, "Monitoring Physical Access," April 2013
[352] CJCSI 3213.01D, Joint Operations Security, May 2012
[353] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
[354] DoD 5200.1-R, Information Security Program, January 1997
[355] Ibid.
[356] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control PE-3, "Physical Access Control," April 2013
[357] Ibid.
[358] DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program, January 1992
[359] DoD 5200.1-R, Information Security Program, January 1997

- Make adjudication decisions based on judgments by appropriately trained adjudicative personnel.[360]
- Notify appropriate adjudication authorities when making the decision to reject another agency's clearance eligibility determination.[361]
- Grant additional special accesses, in accordance with applicable policies, when required by the affiliate's mission or organizational role.[362]
- Notify affiliates of specific reasons for unfavorable clearance decisions and allow opportunity for an appeal.[363]

- Ensure every affiliate accessing an information system that processes, stores, or transmits classified information is cleared and indoctrinated to the highest classification level of the information on the system.
- Conduct an initial security briefing before granting affiliates access to sensitive or classified information.[364]
- Provide continuous personnel security and counterintelligence evaluation of all affiliates who have access to classified information.[365]
  - Perform periodic reinvestigations at least every five years to ensure personnel remain trustworthy and reliable, and resources are protected.[366]
  - Require a reinvestigation if an affiliate requiring access has had a break in service lasting over two years.[367]
- Allow for clearance reciprocity in accordance with national policy.[368]
  - Local clearance reciprocity policies should consider the risk tolerance of both participating organizations.
- Debrief affiliates and revoke access when there is no longer a need to know and update databases to reflect the current information.[369]

4.2.4 Personnel Event Handling

Events causing concern for the suitability of an affiliate's clearance or access should prompt investigation and response, as appropriate.

[360] DoDD 5200.2-R, DoD Personnel Security Program, April 1999
[361] ICPG 704.4, Reciprocity of Personnel Security Clearance and Access Determinations, October 2008
[362] DoD WHS Administrative Instruction No. 23, Personnel Security Program and Civilian Personnel Suitability Investigation Program, December 2006
[363] DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program, January 1992
[364] DoD WHS Administrative Instruction No. 23, Personnel Security Program and Civilian Personnel Suitability Investigation Program, December 2006
[365] ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, October 2008
[366] ICPG 704.1, Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, October 2008
[367] DoDM 5105.21 Vol. 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, October 2012
[368] Ibid.
[369] DoDM 5105.21 Vol. 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, October 2012

- Identify events that may impact an affiliate's ability to maintain their clearance or access (e.g., adverse result of a drug test, changing financial situation, or unofficial foreign travel to certain locations).
    - Past history of identified events should trigger additional checks.
    - Require affiliates to report identified events and any significant change in personal status.[370]
- Establish profiles for high-risk personnel or for personnel with derogatory history to determine the appropriate level of analysis.
- Suspend security clearances of affiliates whose access to classified information has been determined to be a threat until a final clearance decision has been reached.[371]
- Retain data records for two years for subjects who have been debriefed or terminated, seven years for subjects whose clearances have been revoked or denied, and indefinitely for subjects with active or suspended clearances.[372]

Physical Enterprise Monitoring Informative References (Appendix A)

4.3 Intrusion Detection and Prevention

Definition: The *Intrusion Detection and Prevention* capability relies on technology that detects and analyzes events in order to execute appropriate courses of action, including generating alerts, as well as redirecting and blocking anomalous or malicious activity.

Discussion: Automated intrusion detection and prevention is key to minimizing the number of infected systems and the potential for damage to the enterprise. The concept of defense in depth advocates layered protections, both network- and host-based, throughout the enterprise. By combining automated and manual intrusion detection and prevention, the enterprise gains the ability to respond in near real time to malicious or anomalous activities.

Example Threats: Collusion, Impersonation, Insider Threat, Masquerading, Privilege Escalation, Spoofing

4.3.1 Detection and Prevention Methods

Host and network intrusion detection and prevention systems should be used in concert to address potential threats from multiple vectors.[373]

- Use a combination of active intrusion prevention systems (IPS) and passive intrusion detection systems (IDS).
- Deploy both host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS).
- Use a combination of signature-based, anomaly-based, and manual methods of event identification.
    - Signature-based intrusion detection and prevention (IDP) identifies malicious activity through comparison against sets of known characteristics (i.e., signatures).

[370] DoDM 5105.21 Vol. 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, October 2012
[371] DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program, January 1992
[372] ICPG 704.5, Intelligence Community Personnel Security Database Scattered Castles, October 2008
[373] NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling, July 2013

- Anomaly-based IDP identifies previously unknown malicious activity by identifying patterns in the network's activity.
- Manual detection uses non-automated processes to identify threats and activities that could indicate an intrusion or evidence of attack against the network.

- Employ a combination of vendor provided signatures, custom signatures, and reputation services.[374]
  - Employ Antivirus Cloud Lookup (e.g., File Reputation Lookup or Cloud Heuristics) to obtain the latest signatures from vendor databases.
- Ensure intrusion detection and prevention systems react in near real-time and are able to initiate action based on the source and type of threat.

4.3.2 Device Placement

A combination of network-based and host-based IDP improves the overall malware incident prevention rate and helps share the load of malware handling between two sets of technical controls.

- Deploy network-based IDP technologies to the following locations, at a minimum:
  - Perimeter firewall
  - DMZ
  - Logical or physical network segments that house sensitive intranet services, critical resources, or network and security management servers
  - Wide Area Network (WAN) junction points between the regional enclave and the local enclave networks[375]
  - VPN concentrators
  - Remote Access Servers (RAS)
  - Tunnel endpoints
  - Databases
- Install host-based (e.g., application sandboxing, anti-virus, anti-spyware, and host-based firewalls) IDP products on all devices that access the network.

4.3.3 Manage Intrusion Detection and Prevention Systems

Proper management is critical to enable prompt response to attacks against the IDP system, and ensure sensitive information contained on the IDP components is not compromised.

- Manage IDP devices from a centralized location on an out-of-band (OOB) network.[376]
- Ensure IP addresses are not assigned to IDP monitoring interfaces (i.e., stealth mode) to prevent hosts from initiating connections.[377]
- When tuning devices, conduct analysis to optimally balance security and availability considerations for the environment.
  - Monitor and tune IDP devices to increase accuracy; numerous false positives can cause alerts to be ignored and intrusions to remain undetected.
  - Establish baselines for the enterprise to ensure abnormal activities are detected.

[374] DISA, Intrusion Detection and Prevention Systems (IDPS) SRG Ver. 1, December 2012
[375] Ibid.
[376] NIST SP 800-83 Rev.1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013
[377] DISA, Intrusion Detection and Prevention Systems (IDPS) SRG Ver. 1, December 2012

- Configure IDP products to update signature files and scan engines when vendors publish updates.
- Employ a registry monitor to protect information about the programs installed, OS configurations and a list of recently executed programs.
- Employ a file integrity monitor to report on changes to critical system and application files.
- Employ a process/application behavior monitor to study the behavior of processes that are running on the system and alert if an application attempts some action that is outside of its normal or allowed actions.

Intrusion Detection and Prevention Informative References (Appendix A)

4.4 Network Enterprise Monitoring

Definition: The *Network Enterprise Monitoring* capability employs active and passive network monitoring, at an enterprise level, to achieve situational awareness regarding the state of the network and associated devices.

Discussion: Continuously monitoring enterprise network connections and configurations enables mission activities by ensuring security has not been compromised and data is protected. Security log management enables organizations to maintain accurate records and understand events occurring on a network.

Working in concert, data monitoring, log management, and analysis provide the enterprise with the capability to understand, in near-real-time, its networks, and to offer historical context for network events.[378]

Example Threats: APT, DoS, Insider Threat, Malware

4.4.1 Data Monitoring and Analysis

Data Monitoring and Analysis includes strategy development, evaluating IA events and how they affect security throughout an enterprise, recording the changes found, and sharing the information to establish more effective information sharing decisions.

- Develop procedures to guide information processing and to support data fusion and analysis, diagnostics, long-term trend and pattern analysis, and warning communications channels and procedures.[379]
- Employ enterprise-level active and passive network monitoring[380] to detect security- or performance-relevant changes or events.[381]
    - Enable near-real-time network monitoring through a managed system of sensors.
    - Configure network monitoring technologies to allow for signature development based upon available I&W information.[382]
    - Monitor the state of the network and networked devices throughout the enterprise, using both physical and logical monitoring mechanisms.
    - Monitor the health and status of devices and links between devices.

[378] Community Gold Standard Technical Guidance: Manageable Network Plan (MNP) Ver. 3.0, September 2013
[379] ICD 502, Integrated Defense of the Intelligence Community Information Environment March 2011
[380] CNSSI-4009, National Information Assurance (IA) Glossary, April 2010
[381] NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
[382] CJCSM 6510.01B, Cyber Incident Handling Program, July 2012

- Monitor traffic flow in accordance with the established baseline, and provide notification when traffic flow deviates from this baseline.
- Monitor for unauthorized information disclosure.[383]
- Support failover and redundancy for critical monitoring functions.
- Identify anomalous network traffic and host behavioral changes.

- Review audit records and report indications of inappropriate or unusual network activity.[384]
- Ensure that operation security is applied to data collection and aggregation, including data at rest and in transit.
- Establish a manned network operations center to provide near-real-time analysis and facilitate event response.[385]
- Establish specific frequency requirements for network enterprise monitoring, analysis, and reporting, based on organizational need and enterprise policy.
- Provide monitoring results in a standardized format for correlation locally or with peer networks.
  - Present monitoring results and relevant external information in a user interface with the ability to drill down into component detail when needed.
  - Provide reports in both human- and machine-readable format to facilitate collaboration and automated notification and analysis for various monitoring tools.
  - Ensure alternate status reporting procedures for devices unable to support automatic monitoring.[386]
- Aggregate network health and status, traffic flows, and external information to support activities, such as trending analysis, throughout the enterprise.
- Monitor the network for indications of logical tampering.[387]
- Increase system monitoring activity when there is I&W of an increased threat.
- Ensure that information systems provide alerts to the appropriate parties when indications of potential compromise occur.[388]
- Conduct monitoring activities out of band to ensure information is protected from system disruptions, and that monitoring does not interfere with normal network operations.

4.4.2 Security Log Management

Security Log Management helps the enterprise organize records and formalize an approach that provides insight to events within the network.

- Determine which events are auditable and when they are to be audited.[389]

[383] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-13, "Monitoring for Information Disclosure," April 2013
[384] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-6, "Audit Review, Analysis, and Reporting," April 2013
[385] NIST IR 7800 (Draft), Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains, January 2012
[386] NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
[387] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SA-18, "Tamper Resistance and Detection," April 2013
[388] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control SI-4, "Information System Monitoring," April 2013

  - Record security-relevant events and store log data securely to prevent unauthorized tampering or disclosure of the log data.[390]
  - Conduct regular self-assessments and/or third-party audits to ensure compliance with privacy related controls.[391]
  - Report results of system monitoring to leadership on a regular basis.[392]
- Collect and retain logs to support technical analysis relating to misuse, penetration reconstruction, or other investigations (e.g., network component audit information).[393]
- Maintain audit logs with sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation.[394]
- Ensure sufficient storage capacity is available for archiving audit data.[395]
- Use standardized formats to normalize log data to increase ease of reporting and analysis of disparate data sets.[396]
- Use audit reduction tools to increase log retention and maximize efficiency within the auditing process.[397]
- Ensure logs are centrally managed, protected from disruptions, and accessible.[398]
- Ensure audit logs are archived and backed up, as necessary, based on the information system security categorization.
- Provide a backup audit system in the event of a failure or corruption of the primary audit system to prevent a single point of failure.[399]

Network Enterprise Monitoring Informative References (Appendix A)

[389] NIST SP 800-92, Guide to Computer Security Log Management, September 2006
[390] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[391] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995
[392] NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
[393] CJCSM 6510.01B, Cyber Incident Handling Program, July 2012
[394] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)," October 2013
[395] NIST SP 800-92, Guide to Computer Security Log Management, September 2006
[396] Ibid.
[397] Ibid.
[398] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-3 (2), "Content Of Audit Records | Additional Audit Information," April 2013
[399] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AU-15, "Alternate Audit Capability," April 2013

5 Respond & Recover

Figure 6: Respond & Recover Function Diagram

An enterprise must be able to efficiently and effectively respond and recover to threats and vulnerabilities that have affected their environment. Respond & Recover capabilities disucss mechanisms, policies, and measures for restoring mission operations when emergencies have occurred or there have been disasters. Implementing cyber incident response functions will help to ensure the environment stabilizes and operations can maintain usual activity as soon as possible.

5.1 Cyber Incident Response

Definition: The *Cyber Incident Response* capability plans and executes activities to analyze, respond to, and recover from security incidents.

Discussion: Incident handling provides the operational application of incident management principles, managing the lifecycle of an incident from identification through post-incident analysis. Effective incident handling bridges missions across the strategic operation centers, which are often the first line of defense for cyber incidents. Whether the organization performs its own cyber defense, or it works with a service provider, the Cyber Incident Response capability ensures effective response and recovery.

Example Threats: APT, Data Exfiltration, DoS, Distributed Denial of Service (DDoS), Malware

5.1.1 Incident Response Assistance

Leveraging outside incident response assistance becomes critical when the scope of a cyber incident extends past internal response capabilities.[400]

- Identify a supplemental incident response provider, in advance of an incident, in the event that enterprise response capabilities are exceeded.
- Establish MOUs or SLAs in advance to ensure timely support.
    - Define incident response assistance scope, capabilities, expected response times, and engagement processes.
    - Establish one or more agreements with different providers, as appropriate.
    - Ensure all service providers meet requirements set forth in established policies and regulations.

5.1.2 Establish an Incident Handling Program

Adaptable incident handling policies and procedures offer the enterprise flexibility in effectively handling many forms of cyber incidents.

[400] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control IR-7, "Incident Response Assistance," April 2013

- Establish an incident handling policy defining incident criteria and severity rating, as well as enterprise roles, responsibilities, and authorities.[401]
- Develop incident handling plans and procedures to provide consistent response to incidents, performance measures, and timeline details to the enterprise incident handling policy.[402]
- Create a common process within the enterprise for: requests for information, alerts, warnings, and notifications to enable timely receipt and dissemination of information and appropriate response.[403]
- Ensure incident response team services are defined with a team structure and staffing model appropriate for the specific organization.
- Establish coordination mechanisms between the enterprise and other federal, state, and local cyber centers to facilitate cyber incident response.[404]
    - Determine the limitations of coordination through legal authorities.[405]
    - Document established stakeholder partnerships.[406]

5.1.3 Manage Operations

Effective operations management incorporates threat intelligence to proactively defend networks against potential cybersecurity events.

- Analyze I&W information to gain insight into potential threats to the network.[407]
- Establish an integrated information security analysis team (e.g., forensic/malicious code analysts, tool developers, and operations personnel) to identify adversary tactics, techniques and procedures (TTPs).[408]
- Monitor the network for indicators of threat events characterized by known adversary TTPs (e.g., perimeter network scanning, wireless jamming, session hijacking, etc.).[409]
- Monitor the network for indicators of compromise such as:
    - Intrusion detection alerts
    - Security logs showing auditing configuration changes
    - Multiple failed login attempts from unfamiliar remote systems
    - Unusual network traffic flow

5.1.4 Identify and Prioritize Events

The prevalence of cybersecurity-related incidents requires around-the-clock (24x7x365) identification and near-real-time incident response and reporting.

---

[401] NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, August 2012
[402] Ibid.
[403] White House, National Strategy for Information Sharing and Safeguarding, December 2012
[404] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), January 2008 [Classified]; unclassified summary located at http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
[405] NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, August 2012
[406] White House, National Strategy for Information Sharing and Safeguarding, December 2012
[407] CJCSM 6510.01B, Cyber Incident Handling Program, July 2012
[408] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control IR-2, "Integrated Information Security Analysis Team," April 2013
[409] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012

- Obtain alerts containing the originating device, time stamp, event description, and the severity of identified events in near real-time.
- Identify potential events, incidents, or attacks through fully automated, partially automated, and/or manual means.
- Determine whether a detected event is a reportable cyber incident based on predefined criteria.[410]
- Conduct initial triage of reportable cyber incidents.
    - Contain the incident to protect the affected system(s) in situations posing an imminent threat.
    - Quarantine affected systems to protect unaffected systems from further contamination.[411]
    - Preserve the integrity of incident data to ensure it has not been altered.[412]
    - Acquire volatile data using forensic tools, duplicate non-volatile data prior to data analysis, and secure the original non-volatile data sources.[413]
- Create an initial incident report that contains all available incident information (e.g., general description, location, current status, actions taken, and number of systems affected).[414]
- Conduct information sharing through technical and operational reporting channels.[415]

5.1.5 Analyze Incidents

Analysis is performed at the enterprise level to identify the technical details, root cause, systemic problems, and potential impact(s) of an incident.

- Gather all information relevant to the incident (e.g., previously acquired data, event logs, audit trails, and all-source intelligence).
    - Coordinate with other organizations to gather additional information.
    - Provide updates if there are changes in the incident status.
    - Use a database to maintain records of security incidents and to safeguard incident data.
- Perform analysis to determine the validity of the incident, identify delivery vectors and system weaknesses, and determine root cause(s) and impact.
- Research and identify incident response actions.

5.1.6 Conduct Response and Recovery

In addition to addressing the initial impacts of the incident ("stopping the bleeding"), looking ahead to how other systems or partners may be vulnerable will help to ensure the overall health of enterprise networks.

- Identify all affected hosts within the organization that require remediation.[416]

[410] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[411] CJCSM 6510.01B, Cyber Incident Handling Program, July 2012
[412] NIST SP 800-86, Guide to Integrating Forensic Techniques Into Incident Response, August 2006
[413] Ibid.
[414] CJCSM 6510.01B, Cyber Incident Handling Program, July 2012
[415] Ibid.
[416] NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, August 2012

- Implement containment/response actions, as outlined in the enterprise disaster recovery plan, to restore affected hosts and data to normal operations.[417]
- Perform hardening activities (e.g., updating baselines, tuning IDS/IPS/antivirus signatures, or conducting user training) to prevent similar incidents.
- Conduct post-incident analysis to review the effectiveness of incident handling. Issues identified may include missing policies, procedures, or inadequate defenses.[418]
- Collect and share lessons learned across the enterprise and with stakeholders, as appropriate.[419]

Cyber Incident Response Informative References (Appendix A)

5.2 Contingency and Continuity Management

Definition: The *Contingency and Continuity Management* capability establishes policy, procedures, and technical measures designed to maintain or restore operations in the event of emergencies, system failures, or disasters.

Discussion: Properly implemented contingency and continuity management ensures that vital missions remain functional and the enterprise can recover from technical, environmental, and manmade incidents. The potential for change in the environment requires that contingency and continuity plans be periodically reevaluated and tested to prove effectiveness.

Example Threats: Natural Disaster, Power Loss, Service Disruption, Terrorism

5.2.1 Establish Contingency and Continuity Strategies

Prior to developing individual contingency plans, strategies must be in place to ensure that plans consider mission needs and desired interoperability.

- Define impact levels and related contingency controls for each impact level.[420]
- Establish MOUs with stakeholders regarding continuity and contingency planning efforts.[421]
- Define allowable levels of disruption and timeframe for restoration (i.e., maximum tolerable downtime) of mission critical resources.[422]
    - Conduct impact analyses to characterize the consequences of disruptions.[423]
    - Define a process to assess incidents and determine which contingency plan to implement.
    - Establish SLAs with outside vendors to identify response methods for incidents related to noncompliance, including negative financial or other consequences for failure to meet SLAs.[424]
- Establish the order of succession of key personnel.

[417] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-2, "Contingency Plan," April 2013
[418] CJCSM 6510.01B, Cyber Incident Handling Program, July 2012
[419] NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, August 2012
[420] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
[421] FEMA, National Disaster Recovery Framework, September 2011
[422] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-2, "Contingency Plan," April 2013
[423] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
[424] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-2, "Contingency Plan," April 2013

- Gain stakeholder decision makers' acceptance of contingency strategies and ensure these strategies are made known to implementers.
- Consider the security risks associated with allowing a third-party vendor to recover data from a failed or obsolete storage device.[425]
    - Vet service providers before turning over equipment.
    - Ensure third-party vendor and employees sign non-disclosure agreements before accessing data.

5.2.2 Develop Contingency and Continuity Plans

Each continuity and contingency plan must incorporate an introduction with supporting information, descriptions of plan phases, and appendices with other relevant information.

- Develop and document continuity and contingency plans for each foreseeable event that could affect the enterprise.[426]
    - Business Continuity Plan (BCP): Maintenance of business practices during and after a disruption.
    - Continuity of Operations (COOP) Plan: Procedures to restore mission essential functions at an alternate location.
    - Crisis Communications Plan: Communication techniques for sharing incident details.
    - Critical Infrastructure Protection (CIP) Plan: Policies and procedures used to recover information.
    - Cyber Incident Response Plan: Procedures for reacting to attacks.
    - Disaster Recovery Plan (DRP): Techniques for restoring a system.
    - Information System Contingency Plan (ISCP): Procedures for system recovery at the location of the attack or an alternate location.
    - Occupant Emergency Plan (OEP): Procedures for removing personnel and property from a location encountering an attack.
- Develop plans for protecting, removing or destroying classified information in the case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action.
- Develop emergency protection plans for classified Communications Security (COMSEC) material in accordance with governing directives.[427]
- Describe supporting information including background, scope, assumptions, system description, and overview of contingency plan phases.[428]
- Securely transport kits containing records and equipment that cannot be pre-positioned (e.g., fly-away kits).
- Ensure that contingency plans provide for adequate enterprise operations both during and after an incident requiring plan activation.
    - Designate teams to implement strategies and respond when the contingency plan is activated.[429]

[425] NIST SP 800-34 Rev.1, Contingency Planning Guide for Federal Information Systems, May 2010
[426] Ibid.
[427] CNSSP-16, National Policy for the Destruction of COMSEC Paper Material, January 2006
[428] Ibid.
[429] Ibid.

  - Ensure contingency plan operations are financially sustainable.
  - Specify prompt notification procedures to ensure announcements are distributed to affected personnel, customers, and external stakeholders.
- Define criteria for plan activation, operational recovery, and enterprise reconstitution.[430]
  - Prioritize analysis findings to allow the sequence of recovery activities to quickly and effectively restore the identified enterprise functions.
  - Provide detailed procedures for system restoration (e.g., move to an alternate site and obtain replacement equipment).[431]
  - Describe events that trigger escalation and additional actions.
  - Define reconstitution, to include successful recovery validation and plan deactivation.[432]
  - Incorporate emergency management considerations into information security plans and policies.[433]
- Include relevant supplemental information (e.g., contact information, checklists, agreements with other organizations, etc.) in plan appendices.[434]
- Prepare plans for effective withdrawal or destruction of information data and records for deployed elements in hostile or unstable conditions.[435]
- Develop and follow any emergency procedures documented in operating procedures for classified materials and their transport.
  - Ensure that personnel are aware of and trained in emergency protection procedures.
- Develop procedures for receiving first responders, while ensuring protection of classified materials.[436]
  - Assign on-the-scene responsibility for ensuring protection of classified material.
  - Ensure emergency facility security personnel are easily identifiable.
- Ensure that contingency plans are available and accessible to appropriate entities.
  - Include a means to store and access hard copies of contingency plans.
  - Review plans for accuracy at intervals dependent upon the security implications within the plan.[437]
  - Update plan as necessary and provide to management for review and approval.

5.2.3 Test and Exercise Contingency and Continuity Plans

Exercises, workshops, and seminars verify the effectiveness of contingency and continuity plans.[438]

- Conduct emergency response exercises to validate that contingency plans meet mission assurance requirements.
  - Conduct full-scale exercises based on the level of the criticality and mission impact in preparation for potential security incidents.

[430] CNSSP-16, National Policy for the Destruction of COMSEC Paper Material, January 2006
[431] Ibid.
[432] Ibid.
[433] Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
[434] Ibid.
[435] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[436] CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material, October 2008
[437] Ibid.
[438] FEMA, National Disaster Recovery Framework, September 2011

- Define type and scope of an exercise needed if a full-scale exercise is deemed unnecessary.
- Ensure exercises do not create undue risks to the mission or to personnel.[439]

- Conduct exercises at least annually.[440]
  - Document the functions and results of the exercise and update contingency plans as needed.
  - Document lessons learned through contingency and continuity plan testing.[441]

5.2.4 Emergency Management

Establishing an emergency plan to restore all security aspects in the event of an emergency is an essential part of contingency and continuity planning.

- Provide arrival briefings and test available support (e.g., voice communications, information systems, radio) as appropriate for the prevailing OPSEC environment.[442]
- Determine which mission essential functions have been affected, and establish restoration efforts.
- Designate personnel to maintain access control to secure facilities in the event of an emergency.[443]
- Determine and coordinate secure procurement for any additional equipment and supplies needed to support emergency operations.
- Ensure any emergency disclosures of classified national security information are made in accordance with applicable laws and regulations.[444]
- Designate alternative security mechanisms if an emergency situation renders the primary mechanisms insufficient or unusable.[445]

5.2.5 Maintain Contingency and Continuity Plans

Contingency and continuity plans are maintained to ensure continued effectiveness even when changes occur in the environment.

- Manage contingency and continuity plans centrally.
- Reevaluate and update contingency plans regularly[446] and monitor for new contingency and continuity management needs.[447]
- Obtain stakeholder buy-in for significant changes to contingency and continuity plans.
- Design, develop, and manage information systems for capturing and exploiting lessons learned from previous crisis training and exercises.

[439] NIST 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006
[440] CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), October 2013
[441] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-13, "Alternative Security Mechanisms," April 2013
[442] DoDI 3020.42, Defense Continuity Plan Development, February 2006
[443] DoD 5200.08-R, Physical Security Program, April 2007
[444] DHS, Code of Federal Regulation, Title 6, Part 7: Classified National Security Information, January 2005
[445] NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-4, "Contingency Plan Testing," April 2013
[446] NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-2, "Contingency Plan," April 2013
[447] NIST 800-34, Contingency Planning Guide for Federal Information Systems, May 2010

- Notify stakeholders of new and updated contingency and continuity plans. Establish a record of changes made to contingency and continuity plans.[448]

Contingency and Continuity Management Informative References (Appendix A)

[448] NIST 800-34, Contingency Planning Guide for Federal Information Systems, May 2010

Appendix A: Informative References

- Committee on National Security Systems (CNSS) Issuances (https://www.cnss.gov/CNSS/issuances/Issuances.cfm)
- Department of Defense Issuances (http://www.dtic.mil/whs/directives/)
- Executive Orders (http://www.whitehouse.gov/briefing-room/presidential-actions/executive-orders)
- NIST Special Publications (http://csrc.nist.gov/publications/PubsSPs.html)
- NSA, Community Gold Standard Technical Guidance: Manageable Network Plan (MNP) Ver. 3.0
- Office of the Director of National Intelligence (ODNI) Policies and Reports (http://www.dni.gov/index.php/intelligence-community/ic-policies-reports)

Understand the Mission References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- DoDI 8410.02, NetOps for the Global Information Grid (GIG)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- IC Policy Memorandum for Uniform Data Standards (Draft)
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security
- NIST SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

Back to Understand the Mission

Understand the Environment References

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CNSSD-502, National Directive on Security of National Security Systems
- CNSSP-22, Policy on Information Assurance Risk Management for National Security Systems
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- DoD Joint Publication 5-0, Joint Operation Planning
- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) Ch. 1
- DoD 5220.22-R, Industrial Security Regulation
- DoDI 8500.01, Cybersecurity
- DoDI 3020.45, Defense Critical Infrastructure Program (DCIP) Management

- DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
- FEMA 430, Risk Management Series, Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks
- ICD 503, Intelligency Community Information Technology Systems Security Risk Management, Certification and Accreditation
- ICD 705, Sensitive Compartmented Information Facilities
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-35, Guide to Information Technology Security Services
- NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security

Back to Understand the Environment

Information Assurance (IA) Policy and Engagement References

- CNSSD-502, National Directive on Security of National Security Systems
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- DoDD 5144.02, DoD Chief Information Officer (DoD CIO)
- DoDD 8000.01, Management of DoD Information Enterprise
- DoDI 8500.01, Cybersecurity
- Executive Order 12333, United States Intelligence Activities
- Federal CIO Council Privacy Committee, Best Practices: Elements of a Federal Privacy Program
- Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
- ICD 101, Intelligence Community Policy System
- ISO/IEC 27001, Information Security Management
- National Security Presidential Directive 51/Homeland Security Presidential Directive 20 (NSPD-51/HSPD-20), National Continuity Policy
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23), Comprehensive National Cybersecurity Initiative

- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- OMB Circular No. A-130 Revised, Management of Federal Information Resources
- Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

Back to Information Assurance (IA) Policy and Engagement

Portfolio Management References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- Department of Defense Chief Information Officer Desk Reference: Volume 1 Foundation Documents
- DHS, Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise
- DoDD 5100.20, National Security Agency/Central Security Service (NSA/CSS)
- DoDD 5144.02, DoD Chief Information Officer (DoD CIO)
- DoDD 7045.20, Capability Portfolio Management
- DoDD 8000.01, Management of DoD Information Enterprise
- DoDD 8115.01, Information Technology Portfolio Management
- DoDI 8500.01, Cybersecurity
- DoDI 8115.02, Information Technology Portfolio Management Implementation
- DoDI 8410.02, NetOps for the Global Information Grid (GIG)
- E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899
- Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
- ICD 500, Director of National Intelligence, Chief Information Officer
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security
- NIST SP 800-65 Rev. 1 (Draft), Recommendations for Integrating Information Security into the Capital Planning and Investment Control (CPIC) Process
- NIST SP 800-100, Information Security Handbook: A Guide for Managers

Back to Portfolio Management

Acquisition References

- CNSSD-505, Supply Chain Risk Management (SRCM) [Classified]
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSP-11, Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products
- DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- DoDD 5144.02, DoD Chief Information Officer (DoD CIO)
- DoDD 8000.01, Management of DoD Information Enterprise
- DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- Interim DoDI 5000.02, Operation of the Defense Acquisition System
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System
- DTM 09-019, Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)
- Federal Acquisition Regulation (FAR)
- ICD 500, Director of National Intelligence, Chief Information Officer
- ICD 731, Supply Chain Risk Management
- ICD 801, Acquisition
- ICPG 801.1, Acquisition
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems
- NIST, ITL Bulletin November 2012, Practices for Managing Supply Chain Risks to Protect Federal Information Systems
- NIST SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- NIST SP 800-35, Guide to Information Technology Security Services
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-161 (Draft), Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- NSTISSP No. 11 Revised Fact Sheet, National Information Assurance Acquisition Policy

Back to Acquisition

Secure Lifecycle Management References

- CJCSI 3170.01H, Joint Capabilities Integration and Development System (JCIDS)
- CJCSI 6212.01F, Net Ready Key Performance Parameter (NR KPP)
- CJCSM 3170.01C, Operation of the Joint Capabilities Integration and Development System (JCIDS)
- CMMI for Development, Ver. 1.2, CMU/SEI 1-2006-008, ESC-TR-2006-008

- CNSSP-11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products
- Defense Acquisition Guidebook
- DoD Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, Incorporating Test and Evaluation into Department of Defense Acquisition Contracts
- DoDD 4151.18, Maintenance of Military Material
- DoDD 5000.01, The Defense Acquisition System
- DoDI 4151.22, Condition-Based Maintenance Plus (CBM+) for Material Maintenance
- Interim DoDI 5000.02, Operation of the Defense Acquisition System
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
- DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System
- ICD 801, Acquisition
- ICPG 801.1, Acquisition
- IEEE 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process
- IEEE 1362-1998, IEEE Guide for Information Technology System - Definition - Concept of Operations (CONOPS) Document
- INCOSE, Systems Engineering Handbook Ver. 3.2
- ISO/IEC 15288:2008, Systems and Software Engineering -- System Life Cycle Processes
- ISO/IEC 19501:2005, Information Technology-Open Distributed Processing-Unified Modeling Language (UML)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NDIA, System Assurance Committee, Engineering for System Assurance Ver. 1.0
- NIST SP 800-18, Guide for Developing Security Plans for Federal Inforamtion Systems
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle
- NIST SP 800-88 Rev. 1 (Draft), Guidelines for Media Sanitization
- NIST SP 800-160, DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems
- US CERT, Requirements Analysis for Secure Software Pocket Guide
- US CERT, Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
- US CERT, Software Security Testing
- US CERT, Requirements Analysis for Secure Software
- US CERT, Architecture and Design Considerations for Secure Software

Back to Secure Lifecycle Management

Information Assurance (IA) Training References

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)

- CNSSD-500, Information Assurance (IA) Education, Training, and Awareness
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSI-4012, National Information Assurance Training Standard for Senior System Managers
- CNSSI-4013, National Information Assurance Training Standard for System Administrators
- CNSSI-4014, National Information Assurance Training Standard for System Security Officers
- CNSSI-4016, National Information Assurance Training Standard for Risk Analysts
- DoD 5200.2-R, Personnel Security Program Ch. 3
- DoD 8570.01-M, Information Assurance Workplace Improvement Program Ch. 3
- DoD WHS Administrative Instruction No. 23, Personnel Security Program and Civilian Personnel Suitability Investigation Program
- DoDD 5144.02, DoD Chief Information Officer (DoD CIO)
- DoDD 8570.01, Information Assurance (IA) Training, Certification and Workplace Management
- FEMA 430, Risk Management Series, Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks
- ICD 101, Intelligence Community Policy System
- ICD 500, Director of National Intelligence, Chief Information Officer
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST, IR 7298 Rev. 2, Glossary of Key Information Security Terms
- NIST, National Initiative for Cybersecurity Education (NICE), Component 4: Training and Professional Development
- NIST SP 800-16 Rev. 1 (3rd Draft), A Role-Based Model for Federal Information Technology/Cyber Security Training
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- NIST SP 800-100, Information Security Handbook: A Guide for Managers
- NSTISSI-4015, National Training Standard for System Certifiers
- OMB Circular No. A-130 Revised, Management of Federal Information Resources

Back to Information Assurance (IA) Training

Physical Protection References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- Director of Central Intelligence Directive (DCID) 6/1
- DHS, National Infrastructure Protection Plan
- DoD 5200.08-R, Physical Security Program
- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) Ch. 1
- Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- ICD 705, Sensitive Compartmented Information Facilities
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook

- NIST SP 800-16 Rev. 1, (3rd Draft), A Role-Based Model for Federal Information Technology/Cyber Security Training
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-82 Rev. 1, Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-88 Rev. 1 (Draft), Guidelines for Media Sanitization
- UFC 4-010-01, Unified Facilities Criteria (UFC), DoD Minimum Antiterrorism Standards for Buildings
- UFC 4-010-02, Unified Facilities Criteria (UFC), DoD Minimum Antiterrorism Standoff Distances for Buildings

Back to Physical Protection

Network Security References

- Clinger-Cohen Act of 1996, 40 U.S.C. 1401 et seq. (P.L. 104-106 Division E.)
- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- Department of Defense Information Enterprise Architecture (DoD IEA)
- DISA, DoD Internet-NIPRNet DMZ STIG – Ver. 2, Rel. 2
- DISA, Enclave STIG – Ver. 4, Rel. 4
- DISA, Network Firewall Ver. 8, Rel. 16
- DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- DoDD 8000.01, Management of DoD Information Enterprise
- DoDD 8115.01, Information Technology Portfolio Management
- Interim DoDI 5000.02, Operation of the Defense Acquisition System
- DoDI 8410.02, NetOps for the Global Information Grid (GIG)
- DoDI 8500.01, Cybersecurity
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
- DoDI 8551.1, Ports, Protocols, and Services Management (PPSM)
- ICD 501, Discovery and Dissemination or Retrieval of Information Within the Intelligence Community
- Intelligence Community (IC) Information Assurance (IA) Architecture [Classified]
- Internet Assigned Numbers Authority (IANA)
- NIST, Framework for Improving Critical Infrastructure Cybersecurity Ver. 1
- NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-77, Guide to IPsec VPNs
- NIST SP 800-81 Rev. 1, Secure Domain Name System (DNS) Deployment Guide
- NSA, Security Configuration Guide: Limiting Workstation-to-Workstation Communication
- NSA, Security Configuration Guide: Segregate Networks and Functions
- NSA, Security Configuration Guide: Web Domain Name System (DNS) Reputation

- OMB, Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework v3.1)

Back to Network Security

Hardware and Software Inventory References

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CNSSP-17, Policy on Wireless Communications: Protecting National Security Information [Classified]
- Council on CyberSecurity, The Critical Security Controls for Effective Cyber Defense Ver. 5
- DoDI 8552.01, Use of Mobile Code Technologies in DoD Information Systems
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST IR 7693, Specifications for Asset Identification 1.1
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-126 Rev. 2, The Technical Specification for the Security Content Automation Protocol (SCAP)
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NSA, A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS) Ver. 1.1
- RFC 2263, SNMPv3 Applications

Back to Hardware and Software Inventory

Configuration Management References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- Interim DoDI 5000.02, Operation of the Defense Acquisition System
- E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- MIL-HDBK-61A(SE), Military Handbook: Configuration Management Guidance
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), [Classified]
- NIST SP 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program
- NIST SP 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-126 Rev. 2, The Technical Specification for the Security Content Automation Protocol (SCAP)
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NSA, Enterprise Security Management (ESM) Annex for Secure Configuration Management (SCM) [Classified]
- NSA, Security Configuration Guide: Application Whitelisting
- NSA, Security Configuration Guide: Limiting Workstation-to-Workstation Communication

- NSA, Security Configuration Guide: Secure Baseline Configuration
- NSA, Security Configuration Guide: Take Advantage of Software Improvements
- TechAmerica Standard ANSI/EIA-649-B, Configuration Management Standard

Back to Configuration Management

Data Protection References

- CNSSI-1001, National Instruction for Classified Information Spillage
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material
- CNSSP-18, National Policy on Classified Information Spillage
- CNSSP-21, National Information Assurance Policy on Enterprise Architectures for National Security Systems
- DHS Management Directive 11045, Protection of Classified National Security Information: Accountability, Control, and Storage
- DoD 5200.1-R, Information Security Program
- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) Ch. 1
- DoD Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media
- DoDD 8000.01, Management of the DoD Information Enterprise
- DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information
- DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899
- Executive Order 13526, Classified National Security Information
- ICPM 2007-500-3, Intelligence Information Sharing
- Intelligence Community Information Assurance Architecture, Version 1.1 (final draft) [Classified]
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security
- NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-77, Guide to IPsec VPNs
- NIST SP 800-88 Rev. 1 (Draft), Guidelines for Media Sanitization
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access
- NIST SP 800-121 Rev. 1, Guide to Bluetooth Security
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLAN)
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information

Back to Data Protection

Identity Management References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- DoDD 1000.25, DoD Personnel Identity Protection (PIP) Program
- DoDD 8320.03, Unique Identification (UID) Standards for a Net-Centric DoD
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0
- FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors
- Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity [Classified]
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-63-2, Electronic Authentication Guideline
- NIST SP 800-76-1, Biometric Data Specification for Personal Identity Verification
- NIST SP 800-103 (Draft), An Ontology of Identity Credentials Part 1: Background and Formulation

Back to Identity Management

Attribute Management References

- CJCSI 6212.01F, Net Ready Key Performance Parameter (NR KPP)
- CNSSP-24, Policy on Assured Information Sharing (AIS) for National Security Systems (NSS)
- Department of Defense Discovery Metadata Specification
- DoD 5015.02-STD, Electronic Records Management Software Applications Design Criteria Standard
- DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing
- DoDD 5015.2, DoD Records Management Program
- DoDD 8320.02, Data Sharing in a Net-Centric Department of Defense
- DoDD 8320.03, Unique Identification (UID) Standards for a Net-Centric DoD
- DoDM 5200.01 Vol. 1, DoD Information Security Program: Overview, Classification, and Declassification
- DoDM 5200.01 Vol. 3, DoD Information Security Program: Protection of Classified Information
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0
- IC/DoD Unified Authorization and Attribute Service (UAAS) Authorization Attribute Set [Classified]
- ICD 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community
- ICD 710, Classification Management and Control Markings System
- ICPG 500.2, Attribute-Based Authorization and Access Management
- ICPM 2007-500-3, Intelligence Information Sharing
- ICPM 2008-500-1, Information Sharing Data Standards for Intelligence [Classified]
- ICS 500-10, Intelligence Community Standard for Information Security Marking Metadata
- ICS 500-2, Intelligence Community Standard for Information Resource Metadata
- ICS 500-21, Tagging of Intelligence and Intelligence-Related Information

- ICS 500-3, Intelligence Community Standard for Publication Metadata
- ICS 500-5, Intelligence Community Standard for Source Reference Citation Metadata
- Intelligence Community (IC) Design Patterns, Identity and Access Management (IdAM) Design Patterns
- Implementation Profile for Information Resource Metadata (HTML Encoding)
- Implementation Profile for Information Resource Metadata (XML Encoding)
- Implementation Profile for Information Security Marking Metadata (XML Encoding)
- Implementation Profile of Intelligence Publications (XML Encoding)
- National Information Exchange Model (NIEM) Ver. 3.0
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- NSA, Enterprise Security Management (ESM) Annex for Attribute Management [Classified]
- NSA, Enterprise Security Management (ESM) Annex for IA Metadata Management [Classified]
- NSA, Enterprise Security Management (ESM) Annex for Privilege Management [Classified]
- NSA, Security Configuration Guide: Control Administrative Privileges

Back to Attribute Management

Credential Management References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- DoDD 1000.25, DoD Personnel Identity Protection (PIP) Program
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0
- Homeland Security Presidential Directive(HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity [Classified]
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST, National Checklist Program (NCP)
- NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information
- NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-63-2, Electronic Authentication Guideline
- NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- NSA, Enterprise Security Management (ESM) Annex for Credential Management [Classified]
- NSA, Security Configuration Guides
- OMB M-04-04 Memorandum to the Heads of All Departments and Agencies, E-Authentication Guidance for Federal Agencies

Back to Credential Management

Logical Access Control References

- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Ver. 2.0
- Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- ICPG 500.2, Attribute-Based Authorization and Access Management
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, 118 Stat. 3638
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NSA, Enterprise Security Management (ESM) Annex for Authentication [Classified]
- NSA, Enterprise Security Management (ESM) Annex for Privilege Management [Classified]

Back to Logical Access Control

Security Evaluations References

- CERT, Current Malware Threats and Mitigation Strategies
- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- NIST SP 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- PPD 20, U.S. Cyber Operations Policy [Classified]

Back to Security Evaluations

Physical Enterprise Monitoring References

- CJCSI 3213.01D, Joint Operations Security
- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSI-7000, TEMPEST Countermeasures for Facilities [Classified]
- DHS Management Directive 11035, Industrial Security Program
- DHS Management Directive 11052, Internal Security Program
- Director of Central Intelligence Directive (DCID) 6/1
- DoD 5200.1-R, Information Security Program

- DoD 5200.2-R, Personnel Security Program Ch. 3
- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) Ch. 1
- DoD WHS Administrative Instruction No. 23, Personnel Security Program and Civilian Personnel Suitability Investigation Program
- DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program
- DoDM 5105.21 Vol. 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities
- Executive Order 12968, (Amended in part by Executive Order 13467), Access to Classified Information
- ICD 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community
- ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
- ICD 705, Sensitive Compartmented Information Facilities
- ICPG 704.1, Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
- ICPG 704.2, Personnel Security Adjudicative Guidelines for Determining eligibility for access to Sensitive Compartmented Information and other Controlled Access Program Information
- ICPG 704.3, Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information, and Appeals Processes
- ICPG 704.4, Reciprocity of Personnel Security Clearance and Access Determinations
- ICPG 704.5, Intelligence Community Personnel Security Database Scattered Castles
- ICPM 2007-500-3, Intelligence Information Sharing
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NSTISSAM Level I, Compromising Emanations Laboratory Test Standard [Classified]
- NSTISSAM Level II, Laboratory Test Standard for Protected Facility Equipment [Classified]
- NSTISSAM Level III, Laboratory Test Standard for Tactical Mobile Equipment/Systems [Classified]
- NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements Electromagnetics [Classified]
- NSTISS TEMPEST/1-93, Compromising Emanations Field Test Requirements, Electromagnetics [Classified]
- NSTISS TEMPEST/1-95, Shielded Enclosures [Classified]
- NSTISS TEMPEST/2-91, Compromising Emanations Analysis Handbook [Classified]
- NSTISS TEMPEST/2-92, Procedures for TEMEST Zoning [Classified]

Back to Physical Enterprise Monitoring

Intrusion Detection and Prevention References

- AMSG 799B, NATO Zoning Procedures [Classified]

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CJCSM 6510.01B, Cyber Incident Handling Program
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSP-300, National Policy on Control of Compromising Emanations [Classified]
- DISA, Desktop Application Antispyware General – Ver. 4, Rel. 1
- DISA, Enclave STIG- Ver. 4, Rel. 4
- DISA, Intrusion Detection and Prevention Systems (IDPS) SRG Ver. 1
- DoD S-5240.05-M-1, The Conduct of Technical Surveillance Countermeasures Vol. 1 [Classified]
- DoD S-5240.05-M-2, The Conduct of Technical Surveillance Countermeasures Vol. 2 [Classified]
- DoDD 5250.01, Management of Intelligence Mission Data (IMD) in DoD Acquisition
- DoDD O-5240.02, Counterintelligence [Classified]
- DoDD O-8530.1, Computer Network Defense (CND)
- DoDI 5240.05, Technical Surveillance Countermeasures (TSCM)
- DoDI 5240.16, Counterintelligence Functional Services (CIFS)
- DoDI 8410.02, NetOps for the Global Information Grid (GIG)
- DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies
- DoDI 8500.01, Cybersecurity
- ICD 702, Technical Surveillance Countermeasures
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), [Classified]
- NATO SDIP-29,Installation of Electrical Equipment for Processing of Classified Information [Classified]
- NIST SP 800-36, Guide to Selecting Information Technology Security Products
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-94 Rev. 1 (Draft), Guide to Intrusion Detection and Prevention Systems (IDPS)
- NSA, Security Configuration Guide: Anti-Exploitation
- NSA, Security Configuration Guide: Antivirus File Reputation Services
- NSA, Security Configuration Guide: Host Intrusion Prevention (HIPS) Systems

Back to Intrusion Detection and Prevention

Network Enterprise Monitoring References

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CJCSM 6510.01B, Cyber Incident Handling Program
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSP-24, Policy on Assured Information Sharing (AIS) for National Security Systems (NSS)
- DHS 4300A, Sensitive Systems Handbook, Version 7.2.1
- DHS 4300A, Sensitive Systems Policy Directive, Version 8.0

- DNI Memorandum E/S 00765, Concept of Operations and Plan for Implementation of the Comprehensive National Cybersecurity Initiative to Connect Current Cyber Centers [Classified]
- DoDI 8500.01, Cybersecurity
- DoDD O-8530.1, Computer Network Defense (CND)
- DoDI 8410.02, NetOps for the Global Information Grid (GIG)
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
- ICD 502, Integrated Defense of the Intelligence Community Information Environment
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST IR 7800 (Draft), Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-92, Guide to Computer Security Log Management
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- US CERT, Traffic Light Protocol

Back to Network Enterprise Monitoring

Cyber Incident Response References

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CJCSM 6510.01B, Cyber Incident Handling Program
- CNSS-048-07, National Information Assurance (IA) Approach to Incident Management (IM)
- CNSS-079-07, Frequently Ask Questions (FAQ) on Incidents and Spills
- CNSSI-1001, National Instruction on Classified Information Spillage
- CNSSI-1253, Security Categorization and Control Selection for National Security Systems
- CNSSP-18, National Policy on Classified Information Spillage
- DNI Memorandum E/S 00765, Concept of Operations and Plan for Implementation of the Comprehensive National Cybersecurity Initiative to Connect Current Cyber Centers [Classified]
- DoD 8580.02-R, DoD Health Information Security Regulation
- DoDI 8500.01, Cybersecurity
- DoDD O-8530.1, Computer Network Defense (CND)
- DoDI 8110.1, Multinational Information Sharing Networks Implementation
- DoDI 8410.02, NetOps for the Global Information Grid (GIG)
- Intelligence Community Policy for Reporting Security Incidents and Outages on Intelligence Community Information Systems
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations

- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-86, Guide to Integrating Forensic Techniques Into Incident Response
- White House, National Strategy for Information Sharing and Safeguarding

Back to Cyber Incident Response

Contingency and Continuity Management References

- CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
- CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Classified Material
- CNSSI-1253, Security Categorization for Control Selection for National Security Systems
- DHS, Code of Federal Regulation, Title 6, Part 7: Classified National Security Information
- DHS, National Emergency Communications Plan
- DoD 5200.08-R, Physical Security Program
- DoDD 1400.31, DoD Civilian Work Force Contingency and Emergency Planning and Execution
- DoDD 3020.26, Department of Defense Continuity Programs
- DoDD 3020.44, Defense Crisis Management
- DoDI 3020.42, Defense Continuity Plan Development
- Executive Order 13526, Classified National Security Information
- Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 (P.L. 107-347-Title III)
- FEMA, Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements
- FEMA, Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process
- FEMA, National Continuity Policy Implementation Plan (NCPIP)
- FEMA, National Disaster Recovery Framework
- Homeland Security Presidential Directive (HSPD) 7: Critical Infrastructure Identification, Prioritization, and Protection
- National Security Presidential Directive 51/Homeland Security Presidential Directive 20 (NSPD-51/HSPD-20), National Continuity Policy
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]) [Classified]
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Back to Contingency and Continuity Management

Appendix B: Topical Index

Capability Abbreviation Key

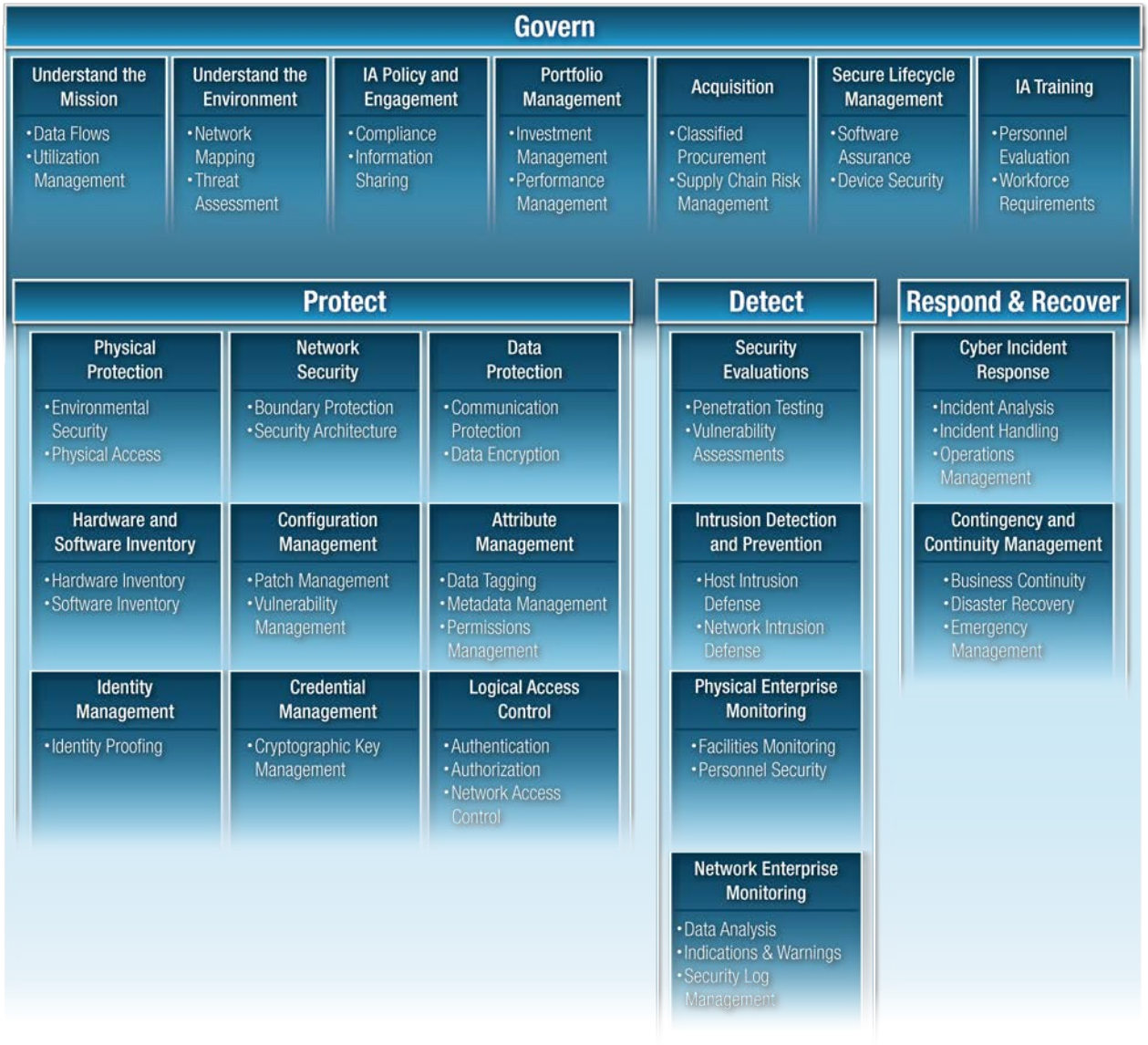
Capability Name	Abbreviation	Capability Name	Abbreviation
Acquisition	ACQ	**Intrusion Detection & Prevention**	IDP
Attribute Management	ATM	**Logical Access Control**	LAC
Configuration Management	CFM	**Network Enterprise Monitoring**	NEM
Contingency and Continuity Management	CCM	**Network Security**	NES
Credential Management	CDM	**Physical Enterprise Monitoring**	PEM
Cyber Incident Response	INR	**Physical Protection**	PHP
Data Protection	DPR	**Portfolio Management**	PMA
Hardware and Software Inventory	HSI	**Secure Lifecycle Management**	SLM
Identity Management	IDM	**Security Evaluations**	SEV
Information Assurance Policy and Engagement	IPE	**Understand the Environment**	UNE
Information Assurance Training	IAT	**Understand the Mission**	UNM

Table 1: Capability Abbreviation Key

A | B | C | D | E | H | I | L | M | N | O | P | R | S | T | V

Appendix C: Framework Topical View

This view offers a graphical depiction of key topics addressed within each of the 22 CGS capabilities. This view is not exhaustive, but provides a quick reference of capability highlights.



Appendix D: CGS v1.1 to v2.0 Capability Mapping

CGS v2.0 Capabilities*	CGS v1.1 Capabilities†
Understand the Mission	Understand Mission Flows, Understand Data Flows, Utilization and Performance Management
Understand the Environment	Network Boundary and Interfaces, Network Mapping, Understand the Physical Environment, Threat Assessment
IA Policy and Engagement	IA Policies, Procedures and Standards, Digital Policy Management, IA Awareness, Organizations and Authorities
Portfolio Management	Portfolio Management, Finance
Acquisition	Acquisition
Secure Lifecycle Management	Development, Deployment, Decommission
IA Training	IA Training
Physical Protection	Physical and Environmental Protections
Network Security	Port Security, Architecture Reviews, Network Boundary Protections
Hardware and Software Inventory	Hardware Device Inventory, Software Inventory
Configuration Management	Configuration Management, System Protection, Operations and Maintenance
Data Protection	Data Protection, Communication Protection
Identity Management	Identity Management
Attribute Management	Attribute Management, Metadata Management
Credential Management	Credential Management, Key Management
Logical Access Control	Access Management, Network Access Control
Security Evaluations	Network Security Evaluations, Vulnerability Assessment
Physical Enterprise Monitoring	Physical Enterprise Monitoring, Physical Hunting, Personnel Enterprise Monitoring, Personnel Security
Intrusion Detection and Prevention	Signature Repository, Network Intrusion Detection, Host Intrusion Detection, Network Hunting, Network Intrusion Prevention, Host Intrusion Prevention
Network Enterprise Monitoring	Network Enterprise Monitoring, Enterprise Audit Management
Cyber Incident Response	Incident Response, Incident Analysis
Contingency and Continuity Management	Contingency Planning

**Some Capability concepts are represented in multiple v2.0 capabilities; only primary relationships represented.*

†The "Manage Risk" cybersecurity function has been removed from CGS v2.0. Readers are encouraged to review the NIST Risk Management Framework described in NIST Special Publications 800-30/37/39.

Appendix E: CGS v2.0 Relationship to CNSSI 1253 Security Controls

This is not a prescriptive or exhaustive list of relevant security controls for IA capabilities. This list represents one recommended approach in relating CGS capabilities to NSS security controls.

CGS v2.0 Capabilities	NIST SP 800-53 Rev. 4 / CNSSI 1253 Controls
Understand the Mission	PM-11, RA-2, SC-6
Understand the Environment	CM-8, RA-2, RA-3, SC-35
IA Policy and Engagement	AC-8, AC-9, AC-22, PL-9, PS-6, SC-37, SI-5, PM-1, PM-2, PM-12, PM-15, PM-16, AP-1, AP-2, AR-6, DM-1, IP-4, TR-1, TR-2, TR-3, UL-2
Portfolio Management	AR-2, PM-3, PM-4, PM-6, PM-7, PM-9, PM-10, RA-1, SA-2
Acquisition	AR-3, MA-6, PS-7, SA-1, SA-4, SA-9, SA-12, SA-19
Secure Lifecycle Management	AR-7, CA-6, MA-1, PL-1, PL-2, PL-7, PL-8, SA-3, SA-5, SA-8, SA-10, SA-11, SA-13, SA-14, SA-15, SA-17, SA-20, SA-22, SI-10
IA Training	AR-5, AT-1, AT-2, AT-3, AT-4, IR-2, PL-4, PM-13, PM-14, SA-16, SC-38
Physical Protection	MA-2, MA-5, MP-4, MP-5, MP-6, PE-1, PE-2, PE-3, PE-4, PE-5, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18, PE-19, PM-8, PS-5, SA-18, SC-32
Network Security	CA-3, SC-7, SC-19, SC-20, SC-21, SC-22, SC-26, SC-29, SC-31, SC-32, SI-8, SI-15
Hardware and Software Inventory	CM-8, CM-10, PE-20, PM-5, SC-27, SE-1
Configuration Management	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, CM-11, CP-12, MA-3, MA-4, MP-7, SC-2, SC-3, SC-18, SC-24, SC-25, SC-34, SC-39, SC-42, SC-43, SI-1, SI-2, SI-6, SI-7, SI-11, SI-16, SI-17
Data Protection	AC-23, AR-1, CP-9, DI-1, DI-2, DM-1, DM-2, DM-3, IA-6, IA-7, IP-1, IP-3, MP-1, SC-1, SC-8, SC-13, SC-28, SC-30, SC-40, SC-41, SE-1, SI-12, UL-1
Identity Management	AC-2, IA-4
Attribute Management	AC-2, AC-5, AC-6, AC-16, MP-3, MP-8, SC-16
Credential Management	IA-5, SC-12, SC-17
Logical Access Control	AC-1, AC-3, AC-4, AC-7, AC-10, AC-11, AC-12, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, AC-24, AC-25, CA-9, IA-1, IA-2, IA-3, IA-8, IA-9, IA-10, IA-11, IP-2, MP-2, PS-5, SC-4, SC-10, SC-11, SC-15, SC-23
Security Evaluations	CA-1, CA-2, CA-5, CA-8, RA-5
Physical Enterprise Monitoring	AR-8, MA-2, PE-6, PE-8, PE-16, PS-1, PS-2, PS-3, PS-4, PS-8, RA-6, SA-21, SC-2
Intrusion Detection and Prevention	SC-5, SC-44, SI-3, SI-14
Network Enterprise Monitoring	AR-4, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, AU-15, AU-16, CA-7, SC-2, SI-4
Cyber Incident Response	IR-1, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, IR-9, IR-10
Contingency and Continuity Management	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-10, C-11, CP-13, PE-17, SC-36, SI-13

Appendix F: Glossary

A | B | C | D | E | F | G | I | K | L | M | N | O | P | R | S | T | U | V | W

A

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. [CNSSI-4009]

Access Control: The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). [CNSSI-4009]

Access Control Mechanism: Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. [CNSSI-4009]

Accountability: Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. [CNSSI-4009]

Alert: Notification that a specific attack has been directed at an organization's information systems. [CNSSI-4009]

Application: Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. [CNSSI-4009]

Asset: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. [CNSSI-4009]

Assurance: Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. [CNSSI-4009]

Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [CNSSI-4009]

Attack Signature: A characteristic byte pattern used in malicious code or an indicator, or set of indicators that allows the identification of malicious network activities. [CNSSI-4009]

Attribute Based Access Control (ABAC): Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. [CNSSI-4009]

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. [CNSSI-4009]

Audit Log: A chronological record of system activities. Includes records of system accesses and operations performed in a given period. [CNSSI-4009]

Audit Reduction Tools: Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. [CNSSI-4009]

Audit Trail: A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. [CNSSI-4009]

Authentication: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. [CNSSI-4009]

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges. [CNSSI-4009]

Availability: The property of being accessible and useable upon demand by an authorized entity. [CNSSI-4009]

Awareness (Information Security): Activities which seek to focus an individual's attention on an (information security) issue or set of issues. [NIST SP 800-50]

B

Baseline: Hardware, software, databases, and relevant documentation for an information system at a given point in time. [CNSSI-4009]

Binding: Process of associating two or more related elements of information. [CNSSI-4009]

Blue Team:

1. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).
2. The term Blue Team is also used for defining a group of individuals that conducts operational network vulnerability evaluations and provides mitigation techniques to customers who need an

independent technical review of their network security posture. A Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment's current state of security readiness. Based on its findings and expertise, a Blue Team provides recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or to ensure that the customer's networks are as secure as possible before having a Red Team test the systems. [see CNSSI-4009; Blue Team]

Boundary: Physical or logical perimeter of a system. [CNSSI-4009]

Boundary Protection: Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). [CNSSI-4009]

Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. [CNSSI-4009]

C

Cascading: Downward flow of information through a range of security levels greater than the accreditation range of a system network or component. [CNSSI-4009]

Certificate: A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date). In the Information Assurance community certificate usually implies public key certificate. [see CNSSI-4009; Certificate]

Certification Authority (CA): 1. For Certification and Accreditation (C&A) (C&A Assessment): Official responsible for performing the comprehensive evaluation of the security features of an information system and determining the degree to which it meets its security requirements. 2. For Public Key Infrastructure (PKI): A trusted third party that issues digital certificates and verifies the identity of the holder of the digital certificate. [CNSSI-4009]

Chain of Custody: A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. [CNSSI-4009]

Clearance: Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a

secret clearance, to secret and confidential material; and a confidential clearance, to confidential material. [CNSSI-4009]

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [CNSSI-4009]

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST SP 800-53]

Contamination: Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. [CNSSI-4009]

Contingency Plan: Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or Disaster Recovery Plan for major disruptions. [CNSSI-4009]

Continuous Monitoring: The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating Information Assurance (IA) relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise. [CNSSI-4009]

Credential Service Provider (CSP): A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities and verifiers that it operates. A CSP may be an independent third party or may issue credentials for its own use. [CNSSI-4009]

Critical Infrastructure: System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [CNSSI-4009]

Cyber Incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See *Incident*. [CNSSI-4009]

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks. [CNSSI-4009]

D

Defense-in-Depth: Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [CNSSI-4009]

Demilitarized Zone (DMZ): Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. [CNSSI-4009]

Digital Signature: Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay. [CNSSI-4009]

Disaster Recovery Plan: Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See *Contingency Plan*. [CNSSI-4009]

Disruption: An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). [CNSSI-4009]

Domain: An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See also *Security Domain*. [CNSSI-4009]

E

Enclave: Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. [CNSSI-4009]

Enclave Boundary: Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a Wide Area Network (WAN). [CNSSI-4009]

Encryption: The process of changing plaintext into ciphertext for the purpose of security or privacy. [CNSSI-4009]

(e)nterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. [CNSSI-4009]

(E)nterprise: A system or collection of agencies or enterprises (i.e., NSA would be an enterprise, while the Intelligence Community, including NSA, would be an enterprise); colloquially known as "big E" enterprise. [Common Usage]

Entity: A user or a non-person device or service. [see CNSSI-4009, Authentication]

Environment: Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. [CNSSI-4009]

Event: Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. [CNSSI-4009]

F

Failover: The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. [CNSSI-4009]

Firewall: A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. [CNSSI-4009]

G

Gateway: Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. [CNSSI-4009]

Goals: Guidance for security control implementation in the form of high-level policies and requirements, laws, regulations, and guidelines obtained from agency strategic and performance plans. [NIST SP 800-55]

I

Identification: An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others. [CNSSI-4009]

Identifier: A data object—often, a printable, non-blank character string—that definitively represents a specific identity of a system entity, distinguishing that identity from all others. [CNSSI-4009]

Identity: The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. [CNSSI-4009]

Identity Registration: The process of making a person's identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system. [CNSSI-4009]

Impact Level: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [CNSSI-4009]

Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CNSSI-4009]

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s). [CNSSI-4009]

Information Assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [CNSSI-4009]

Information System (IS): A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [CNSSI-4009]

Inside(r) Threat: An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. [CNSSI-4009]

Integrity: The property whereby an entity has not been modified in an unauthorized manner. NIST SP 800-53: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity. [CNSSI-4009]

Interface: Common boundary between independent systems or modules where interactions take place. [CNSSI-4009]

Intrusion: Unauthorized act of bypassing the security mechanisms of a system. [CNSSI-4009]

Intrusion Detection Systems (IDS): Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside organizations) and misuse (attacks from within organizations). [CNSSI-4009]

Intrusion Detection Systems (IDS), (Host-Based): IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack,

because they can directly access and monitor the data files and system processes usually targeted by attacks. [CNSSI-4009]

Intrusion Detection Systems (IDS), (Network-Based): IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment. [CNSSI-4009]

Intrusion Prevention Systems (IPS): System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. [CNSSI-4009]

K

Key: A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. [CNSSI-4009]

L

Least Privilege: The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. [CNSSI-4009]

M

Malware: Includes malicious code, malicious applets, and malicious logic. [see CNSSI-4009; Malware]

Media: Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. [CNSSI-4009]

Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [CNSSI-4009]

N

National Security Information (NSI): Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [see CNSSI-4009; Classified National Security Information]

Need to Know: A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms "need to know" and "least privilege" express the same idea. Need to know is generally applied to people, while least privilege is generally applied to processes. [CNSSI-4009]

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. [CNSSI-4009]

Network Security: See *Information Assurance*. [CNSSI-4009]

O

Object: Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains. [CNSSI-4009]

Objectives: See *Goals*. [NIST SP 800-55]

P

Penetration: See *Intrusion*. [CNSSI-4009]

Perimeter: (*L) Encompasses all those components of the system that are to be accredited by the DAA, and excludes separately accredited systems to which the system is connected. [CNSSI-4009]

Personally Identifiable Information (PII): 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. [CNSSI-4009]

Potential Impact: The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals. [CNSSI-4009]

Privacy Impact Assessment (PIA): An analysis of how information is handled 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [CNSSI-4009]

Protocol: Set of rules and formats, semantic and syntactic, permitting information systems to exchange information. [CNSSI-4009]

Public Key: A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign. [CNSSI-4009]

Public Key Infrastructure (PKI): The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. [CNSSI-4009]

R

Records: The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). [CNSSI-4009]

Red Team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. A Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and what works for defenders (i.e., a Blue Team) in an operational environment. [see CNSSI-4009; Red Team]

Registration: The process through which a party applies to become a subscriber of a CSP and a Registration Authority validates the identity of that party on behalf of the CSP. [CNSSI-4009]

Remediation: The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application. [NIST 800-40 Version 2]

Remote Access: Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). NIST 800-53: Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). [CNSSI-4009]

Removable Media: Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device, that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar Universal Serial Bus (USB) storage devices. [CNSSI-4009]

Resilience: Ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions. [DHS Risk Lexicon]

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise

from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [CNSSI-4009]

Risk Management Framework (RMF): A structured approach used to oversee and manage risk for an enterprise. [CNSSI-4009]

Role: A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. [CNSSI-4009]

S

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. [CNSSI-4009]

Sandboxing: A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. [CNSSI-4009]

Secure State: Condition in which no subject can access any object in an unauthorized manner. [CNSSI-4009]

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. [CNSSI-4009]

Security Categorization: The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See also security category. [NIST SP 800-53]

Security Control: A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. [NIST SP 800-53]

Security Posture: The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. [CNSSI-4009]

Security Safeguards: Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [CNSSI-4009]

Sensitive Compartmented Information Facility (SCIF): Accredited area, room, or group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed. [CNSSI-4009]

Sensitive Information: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235)). [CNSSI-4009]

Service Level Agreement: Defines the specific responsibilities of the service provider and sets the customer expectations. [CNSSI-4009]

Signature: See *Attack Signature*. [CNSSI-4009]

Situational Awareness: Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future. [CNSSI-4009]

Spillage: Security incident that results in the transfer of classified or Controlled Unclassified Information (CUI) onto an information system not accredited (i.e., authorized) for the appropriate security level. [CNSSI-4009]

Subject: An active entity (generally an individual, process, or device) that causes information to flow among objects or changes the system state. See also *Object*. [CNSSI-4009]

Subscriber: A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol. [CNSSI-4009]

System Owner: Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. [CNSSI-4009]

T

Tampering: An intentional event resulting in modification of a system, its intended behavior, or data. [CNSSI-4009]

Technical Surveillance Countermeasures (TSCM): Techniques and measures to detect, neutralize, and/or exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information. [DoDI-5240.05]

TEMPEST: A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. [CNSSI-4009]

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSSI-4009]

Token: Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. [CNSSI-4009]

U

Unauthorized Access: Any access that violates the stated security policy. [CNSSI-4009]

Unauthorized Disclosure: An event involving the exposure of information to entities not authorized access to the information. [CNSSI-4009]

Unclassified: Information that has not been determined pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified. [CNSSI-4009]

User: Individual, or (system) process acting on behalf of an individual, authorized to access an information system. [CNSSI-4009]

V

Virtual Private Network (VPN): Protected information system link utilizing tunneling, security controls (see *Information Assurance*), and endpoint address translation giving the impression of a dedicated line. [CNSSI-4009]

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself via email programs to other computers, or even erase everything on a hard disk. [see CNSSI-4009; Virus]

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [CNSSI-4009]

Vulnerability Assessment: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [CNSSI-4009]

W

Whitelisting: The process used to identify: (i) software programs that are authorized to execute on an information system or (ii) authorized Universal Resource Locators (URL)/websites. [NIST SP 800-53]

Appendix G: Acronyms

A | B | C | D | E | F | G | H | I | J | M | N | O | P | R | S | T | U | V | W

A

A&A: Assessment and Authorization

ABAC: Attribute-Based Access Control

AIS: Assured Information Sharing

AO: Authorizing Officials

APT: Advanced Persistent Threat

B

BCP: Business Continuity Plan

C

C&A: Certification and Accreditation

CBM+: Conditions Based Management Plus

CCB: Configuration Control Board

CD: Compact Disk

CGS: Community Gold Standard

CIP: Critical Infrastructure Protection

CISO: Chief Information Security Officer

CJCSI: Chairman of the Joint Chiefs of Staff Instruction

CNCI: Comprehensive National Cybersecurity Initiative

CND: Computer Network Defense

CNSS: Committee on National Security Systems

CNSSI: Committee on National Security Systems Instruction

COMSEC: Communications Security

CONOPS: Concept of Operations

COOP: Continuity of Operations

CPIC: Capital Planning and Investment Control Process

CPTED: Crime Prevention Through Environmental Design

CPU: Central Processing Unit

CRB: Configuration Review Board

CSfC: Commercial Solutions for Classified

CSP: Credential Service Provider

CSS: Central Security Service

CUI: Controlled Unclassified Information

D

DCID: Director of Central Intelligence Directive

DCIP: Defense Critical Infrastructure Program

DDoS: Distributed Denial of Service

DHS: Department of Homeland Security

DIRNSA: Director of the National Security Agency

DDoS: Distributed Denial of Service

DMZ: Demilitarized Zone

DNI: Director of National Intelligence

DNS: Domain Name System/Service

DoD: Department of Defense

DoS: Denial of Service

DRP: Disaster Recovery Plan

E

EO: Executive Order

ESM: Enterprise Seccurity Management

F

FCD: Federal Continuity Directive

FICAM: Federal Identity, Credential, and Access Management

FIPS: Federal Information Processing Standard

FISMA: Federal Information Security Management Act

FOCI: Foreign Ownership, Control, or Influence

FSO: Facility Security Officer

G

GIG: Global Information Grid

GOTS: Government off-the-shelf

H

HIDS: Host Intrusion Detection Systems

HIPS: Host Intrusion Prevention Systems

HR: Human Resources

HSPD: Homeland Security Presidential Directive

HVAC: Heating, Ventilation, and Air Conditioning

I

I&W: Indications and Warnings

IA: Information Assurance

IANA: Internet Assigned Numbers Authority

IC: Intelligence Community

IC-ID: Intelligence Community-Digital Identifier

ICD: Intelligence Community Directive

ICPG: Intelligence Community Policy Guidance

ICS: Industrial Control System

ICT: Information and Communication Technology

IdAM: Identity and Access Management

IDP: Intrusion Detection & Prevention

IDPS: Intrusion Detection & Prevention Systems

IDS: Intrusion Detection Systems

INCOSE: International Council on System Engineering

IPS: Intrusion Prevention Systems

IPsec: Internet Protocol Security

IRTPA: Intelligence Reform and Terrorism Prevention Act

IS: Information System

ISA: Interconnection Security Agreement

ISCM: Information Security Continuous Monitoring

ISCP: Information System Contingency Plan

IT: Information Technology

J

JCIDS: Joint Capabilities Integration Development System

L

LAC: Logical Access Control

M

MAC: Message Authentication Code

MNP: Manageable Network Plan

MOU: Memorandum of Understanding

N

NCPIP: National Continuity Policy Implementation Plan

NIAP: National Information Assurance Partnership

NIDS: Network Intrusion Detection System

NIEM: National Information Exchange Model

NISPOM: National Industrial Security Program Operating Manual

NIST: National Institute of Standards and Technology

NSA: National Security Agency

NSI: National Security Information

NSPD: National Security Presidential Directive

NSS: National Security System

O

ODNI: Office of the Director of National Intelligence

OEP: Occupant Emergency Plan

OMB: Office of Management and Budget

OOB: Out-of-band

OPSEC: Operations Security

OS: Operating System

P

PIA: Privacy Impact Assessment

PII: Personally Identifiable Information

PIP: Personnel Identity Protection

PIV: Personal Identity Verification

PK: Public Key

PKI: Public Key Infrastructure

PPSM: Ports, Protocols, and Services Management

R

RAM: Random-Access Memory

RAS: Remote Access Server

RMF: Risk Management Framework

S

SCADA: Supervisor Control and Data Acquisition

SCAP: Security Content Automation Protocol

SCI: Sensitive Compartmented Information

SCIF: Sensitive Compartmented Information Facility

SCM: Secure Configuration Management

SCRM: Supply Chain Risk Management

SLA: Service Level Agreement

SME: Subject Matter Expert

SRG: Security Requirements Guide

SSE: System Security Engineer

STIG: Security Technical Implementation Guide

T

TSCM: Technical Surveillance Countermeasure

TT&E: Training, Test, and Evaluation

TTL: Time to Live

TTP: Tactics, Techniques, and Procedures

U

UAAS: Unified Authorization and Attribute Service

UML: Unified Modeling Language

URL: Universal Resource Locator

USB: Universal Serial Bus

V

VLAN: Virtual Local Area Network

VM: Virtual Machines

VPN: Virtual Private Network

W

WAN: Wide Area Network

WLAN: Wireless Local Area Network