THE SECRETARY OF THE NAVY

SECNAV M-5239.1
November 2005

Department of the Navy Information Assurance Program

Information Assurance Manual




Published By
The Department of the Navy Chief Information Officer

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

FOREWORD

Information Assurance (IA) is a cornerstone of the Department of the Navy (DON) transformation to a secure interoperable, net-centric Naval Information Management/Information Technology Enterprise. The security and superiority of DON information, systems, and personnel is key to our maritime dominance and national security. We take a Defense in Depth (DiD) approach to IA, layering IA principles and controls that apply to people, processes, and technology. The path to a net-centric environment is rife with opportunities and risks. To retain an agile IA posture, DON integrates IA controls throughout all facets of the Enterprise. We must all accept the challenges presented in a net-centric, interconnected environment, especially that risk assumed by one system is incurred by all systems.

This Manual implements the policy set forth in Secretary of the Navy Instruction (SECNAVINST) 5239.3A, Subject: "Department of the Navy Information Assurance Policy" and is issued under the authority of SECNAVINST 5430.7N, Subject: "Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy." This Manual is intended to serve as a high-level introduction to information assurance and IA principles. It discusses common IA controls and associated requirements and reviews the Department of Defense strategy for implementing those controls. Future manuals in the SECNAV Manual (SECNAVMAN) 5239 series will address other topics such as IA roles and responsibilities, basic IA practices and procedures, and IA incident reporting and response, etc.

This Manual is effective immediately; it is mandatory and applicable to all DON activities, installations, commands, units, and personnel, and DON owned or controlled information systems. Nothing in this manual shall alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information and special access programs for intelligence.

The entire SECNAV IA Manual series may be accessed through the Department of the Navy, Navy Electronic Directives System website: http://neds.daps.dla.mil/.

D. M. Wennergren
Department of the Navy
Chief Information Officer

TABLE OF CONTENTS

1. CHAPTER 1 – INTRODUCTION

1.1. PURPOSE

This Manual:

1.1.1. Introduces the Department of the Navy (DON) Information Assurance Program, its concepts, and their application within the DON. Other manuals in the series will provide more detailed guidance on specific IA-related topics.

1.1.2. Describes the DON Information Assurance Program. The purpose of the DON IA Program is to protect information to support the DON mission as described in the DON Information Management and Information Technology (IM/IT) Strategic Plan, to "deliver secure, interoperable, and integrated information management and information technology to the Marine and Sailor to support the full spectrum of warfighting and warfighting support missions." The major elements of the DON IA Program are: to promulgate IA policies and procedures to manage risk to DON IT assets, promote implementation of IA throughout the life cycle of all DON IT assets, and to integrate IA controls throughout the daily activities of the DON.

1.1.3. Replaces DON IA Publication 5239-01, dated May 2000, and should be reviewed in its entirety.

1.2. APPLICABILITY

1.2.1. This manual is mandatory and applies to all DON activities, installations, commands, units, and personnel, and to information collected or maintained by or on behalf of the Department of the Navy and Information Systems used or operated by the Department of the Navy, by a contractor of the Department of the Navy processing DON information, or other organizations on behalf of the Department of the Navy. Military, civilian, contractor, and foreign national personnel who have access to DON-owned or controlled information systems are also subject to the provisions herein. This manual applies only to classified collateral, and/or sensitive unclassified, or unclassified information systems and networks. This publication does not apply to Special Compartmented Information, Cryptographic, Cryptologic, Special Access Program, Single Integrated Operation Plan-Extremely Sensitive Information, or North Atlantic Treaty Organization information. Those systems are under the purview of their respective authorities. However, this manual mentions these types of information only to complete definitions or provide examples.

1.2.2. This manual is consistent with Federal and Department of Defense (DoD) IA policies. In the case of a conflict, directives and instructions set forth by higher authority take precedence. Implementing authorities at the Marine Corps and Navy shall identify conflicting policy and issues of precedence to the Office of the DON Chief Information Officer (DON CIO) for resolution.

2. CHAPTER 2 – IA PRINCIPLES, ATTRIBUTES, AND APPROACHES

2.1. PRINCIPLES

2.1.1. The DON CIO is responsible for developing and promulgating IA strategy and policy, coordinating IA within the Department and with other DoD components, measuring and evaluating Service and system level IA performance, and reporting to the Secretary of the Navy on the effectiveness of DON IA activities. The DON CIO shall carry out for the Secretary of the Navy the information assurance responsibilities assigned in *The Federal Information Security Management Act of 2002 (FISMA)* to the Head of each Federal Agency. DON CIO reports directly to the Secretary of the Navy and has the responsibility to ensure compliance with applicable Information Assurance requirements including the development and maintenance of a Department-wide IA Program.[1] The Navy Deputy Chief Information Officer for Policy and Integration (DON Deputy CIO (Policy and Integration)) is designated as the Department of the Navy Senior Information Assurance Officer (DON Senior IA Officer).

2.1.2. DON CIO focuses its efforts on the development of IA policy, strategy, tools, and oversight. The goal of IA is to protect and defend information and information systems. Information Assurance is an operational requirement throughout DON and is an essential contributor to the warfighting mission and system interoperability.

2.1.3. The DON Information Management and Information Technology vision is to provide a joint, net-centric environment that delivers knowledge dominance to the Naval warfighting team. Achieving that vision requires ensuring that the warfighter has the full and best use of world-leading information technology assets. This is achieved through the pursuit of general IA principles, executed through DoD and DON-specific approaches.

2.1.4. IA is a critical supporting capability for Information Operations as a primary warfare area. Information Operations is defined as actions taken to affect adversary information and information systems while defending one's own information and information systems. IA impacts all five core capabilities of Information Operations: Electronic Warfare, Computer Network Operations, Military Deception, Operations Security, and Psychological Operations. An Information Operations operational planner must ensure that activities are prioritized and synchronized with IA in order to achieve stated goals and objectives.

2.1.5. Information and information systems shall be properly managed and protected as required by law, regulation, policy, or treaty. IA is a composite of the principles addressed in this section.

2.2. ATTRIBUTES

2.2.1. IA shall be achieved through the cost-effective, risk-balanced application of controls in a manner that promotes confidentiality, integrity, availability, non-repudiation, and authentication of information. The first three attributes are widely applicable to systems and are the basis for DoD-wide system characterization and subsequent assignment of appropriate IA

[1] SECNAVINST 5430.7N

controls. Non-repudiation and authentication are often included with the three fundamentals to emphasize their importance to DoD.

2.2.1.1. Confidentiality is assurance that information is not disclosed to unauthorized persons, processes, or devices. It includes both the protection of operational information and the protection of IA-related system information such as password or configuration files.

2.2.1.2. Integrity is assurance that information is not modified by unauthorized parties or in an unauthorized manner. Integrity supports the assurance that information is not accidentally or maliciously manipulated, altered, or corrupted. Additionally, integrity implies the ability to detect when information has been altered.

2.2.1.3. Availability is assurance of timely, reliable access to data and information systems by authorized users. Availability-focused IA controls protect against degraded capabilities and denial of service conditions.

2.2.1.4. Non-repudiation is assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

2.2.1.5. Authentication is assurance of the identity of an e-mail message sender or receiver. Authentication supports the validation of e-mail messages and information system access requests.

2.3. APPROACHES TO IA

2.3.1. DON IA is achieved through joint efforts within DON and across DoD. Understanding the common DoD approaches to IA ensures better DON implementation.

2.3.1.1. Joint Vision 2020. This DoD strategy focuses on the continuing transformation of America's Armed Forces. The primary purpose of those forces has been and will be to fight and win the Nation's wars. The overall goal of the transformation described in this document is the creation of a force that is dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict. The continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control.

2.3.1.2. The Global Information Grid. Joint Vision 2020 envisioned the concept of a Global Information Grid (GIG) to provide the Net-Centric DoD environment required to achieve information superiority. The GIG supports all DoD, National Security, and related Intelligence Community mission and functions in war and in peace. The GIG—a seamless, common-user, information infrastructure—will be the foundation for information superiority by providing the enterprise-wide information services for the DoD's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems (C4ISR) and e-Business systems. The GIG includes all owned and leased communications and computing

systems and services, software, data, security services, and other associated services necessary to achieve information superiority. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). Further, the GIG provides interfaces to coalition, allied, and non-DoD users and systems. GIG IA provides the capabilities that enable information superiority in every military operation, and is inherent to net-centric capabilities that support the full range of warfighter, intelligence, and business operations. DON Information Technology (IT) and IA efforts are oriented towards securely achieving the vision of the GIG.

2.3.1.2.1. FORCEnet. FORCEnet is the U.S. Navy (USN) and U.S. Marine Corps (USMC) initiative to achieve Net-Centric Operations and Joint Transformation by providing robust information sharing and collaboration capabilities across the Naval / Joint force. FORCEnet supports joint interoperability requirements of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, *Joint Capabilities Integration and Development System*. FORCEnet provides a transitional approach to requirements definition, cross-domain solutions, and command and control. FORCEnet technical requirements match key Joint, Net-Centric, and GIG technical guideposts. FORCEnet will enable the delivery of distributed combat systems connected through the network. It is not a single process, but a collection of processes such as requirements generation, architecture and design standards, innovation and experimentation, human system engineering, certification and compliance, and others, all created under a common vision and with common authority in the USN and USMC, aimed at delivering this capability.

2.3.1.2.2. Navy Marine Corps Intranet. The Navy Marine Corps Intranet (NMCI) is both a strategy and a network. As a strategy, NMCI supports USN and USMC leverage of a new and technically up-to-date enterprise network and promotes enhanced network security. As a network, it provides a common, secure, enterprise infrastructure capable of supporting new enterprise-wide applications. The IA benefits of NMCI include central management of the network, configuration management, and improved systems availability. Most legacy networks will migrate to NMCI, the single DON Enterprise network. The consolidation of legacy networks into NMCI will reduce the number of vulnerabilities to and increase the IA posture of the DON enterprise.

2.3.1.3. Defense-in-Depth. DiD is the DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA controls within and among IT assets; and the selection of IA solutions based on their relative level of robustness. The practice of Computer Network Defense (CND) embodies incident detection and response, a critical part of defense-in-depth. CND synchronizes the technical, operational, and intelligence assessments of the nature of a computer attack in order to defend against it. As part of DiD, IA controls should be selected to mitigate both external and insider threats.

2.3.1.4. DoD IA Strategic Plan. The DoD IA Strategic Plan represents a collaborative, enterprise-wide effort to identify and organize the major goals and objectives of DoD-wide IA efforts. Each goal is associated with specific IA activities and goal leaders direct goal-related efforts. The major goals of the strategy include:

- Goal One - Protect Information;

- Goal Two - Defend Systems and Networks;
- Goal Three - Provide Integrated IA Situational Awareness/IA Command and Control;
- Goal Four - Transform and Enable IA Capabilities; and,
- Goal Five - Create an IA-empowered Workforce.

2.3.1.5. Risk Management. Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. In a networked environment, a risk to one system is a risk to all systems; therefore, effective risk management reduces risk assumed by all systems to an acceptable level for operational use. FISMA directs the Head of each Federal Agency to provide IA "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained…; and information systems used or operated…"[2] System owners are expected to manage risk but it is understood that risk cannot be fully avoided. Commands confront varying environments and changing operational requirements. Therefore, Commanders of DON organizations, in support of appropriate Designated Approving Authorities (DAAs), shall apply risk management principles to determine how to best attain the required level of protection. Employing risk management may result in command decisions to adopt specific security measures above and beyond the DoD and DON baseline, given the relative costs and available resources.[3]

2.3.2. As a standard approach to IA, all DON information and information systems shall be safeguarded through the application of IA controls per DoD Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation* and SECNAVINST 5239.3A.

2.3.2.1. IA controls are applied to manage risks to confidentiality, integrity, availability, authentication, and non-repudiation based upon mission criticality and classification or sensitivity level of information processed, stored, and/or transmitted.

2.3.2.2. Federal regulations and guidance organize IA controls into classes and families. Each family contains controls related by function. Federal regulations require the application of baseline IA controls organized in this class and family structure. This document is aligned with that structure.

2.3.2.2.1. The management class of IA controls addresses topics that may be characterized as managerial. They are techniques and concerns that are normally directed or addressed by leadership. They focus on the management of IA and the management of risk.

2.3.2.2.2. The operational class of IA controls focus on activities that are implemented and executed by people as opposed to systems. These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and rely upon management activities as well as technical controls.

---

[2] Federal Information Security Management Act of 2002 (FISMA)
[3] SECNAVINST 5510.36

2.3.2.2.3. The technical class of IA controls focuses on IA controls that are set up by people but executed by systems. These controls depend upon the proper functioning of the systems to be effective. Implementation of technical controls requires significant operational considerations and should be consistent with the management of IA within the organization.

2.4. ROLES AND RESPONSIBILITIES

DON IA roles and responsibilities are set forth in SECNAVINST 5239.3A and SECNAVINST 5430.7N. Additional key roles are described and assigned in DoD Directive (DoDD) 8500.1, *Information Assurance (IA)* and DoDI 8500.2. A high-level summary of key IA roles follows. An upcoming SECNAV IA Manual will provide a more detailed discussion of DON IA roles and responsibilities.

2.4.1. DON CIO. The DON CIO is responsible for developing and promulgating IA strategy and policy, coordinating IA within the Department and with DoD components, measuring and evaluating Service and system level IA performance, and reporting to the Secretary of the Navy on the effectiveness of DON IA activities. The Navy Deputy Chief Information Officer for Policy and Integration (DON Deputy CIO (Policy and Integration)) is designated as the Department of the Navy Senior Information Assurance Officer (DON Senior IA Officer). The DON Senior IA Officer has the responsibilities and performs the functions of the "senior agency information security officer" referenced in FISMA.

2.4.2. DON Deputy CIOs. The DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) shall, subject to the authority of the DON CIO, implement and enforce policies, standards, and procedures to ensure that DON complies with applicable statutes, regulations, and directives.

2.4.3. Chief of Naval Operations. The Chief of Naval Operations (CNO) is responsible for developing and implementing IA-related programs and controls, ensuring that IA is incorporated throughout the system development lifecycle, assigning designated approval authorities (DAAs), providing enterprise-wide vulnerability mitigation solutions, and providing an incident reporting and response capability.

2.4.4. Commandant of the Marine Corps. The Commandant is responsible for developing and implementing IA-related programs and controls, ensuring that IA is incorporated throughout the system development lifecycle, assigning DAAs, providing enterprise-wide vulnerability mitigation solutions, and providing an incident reporting and response capability.

2.4.5. Designated Approving Authority. The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. DAAs accredit IT system security postures throughout the system development lifecycle and in accordance with risk-management principles.

2.4.6. Certification Authority. The Certification Authority (CA) is the official responsible for performing the comprehensive evaluation of the technical and non-technical security features and safeguards of an IT system, application, or network. This evaluation is made in support of the accreditation process, to establish the extent that a particular design and implementation meets information assurance requirements. The CA is responsible for making a technical

judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and issuing a certification statement for the system. The CA is responsible for managing the certification process.

2.4.7. Program Manager. The Program Manager (PM) is the person who owns the business process and controls the funding for the system. The PM is the individual with overall responsibility for the system/application.

2.4.8. Command Information Officers. All Navy Echelon II Commands and all Marine Corps Major Subordinate Commands shall have a command Information Officer (IO) billet. Navy Echelon II command IOs report to the DON Deputy CIO (Navy) for tactical matters and to their commanding officer for administrative matters. Marine command IOs report to both the DON Deputy CIO (Marine Corp) and their Major Subordinate Commander.[4]

2.4.9. IA Manager. The Information Assurance Manager (IAM) is responsible for the information assurance program within a command, site, system, or enclave. The IAM is responsible to the local IA command authority and DAA for ensuring the security of an IT system, and that it is approved, operated, and maintained throughout its life cycle in accordance with IT system security certification and accreditation documentation. Additionally, this individual is responsible for creating the site accreditation package. The IAM functions as the command's focal point for IA matters on behalf of, and principal advisor to, the DAA.

2.4.10. IA Officers. IA Officers (IAOs) are responsible to an IAM for ensuring the appropriate operational IA posture is maintained for a command, organization, site, system, or enclave. IAOs assist in creating accreditation packages. They implement and enforce system-level IA controls in accordance with program and policy guidance.

2.4.11. Commanding Officers/Officers-in-Charge. Leadership support at all levels is the most important part of a command's IA program. In their role as local IA authorities Commanding Officers/Officers-in-Charge (COs/OICs) are directly responsible for identifying vulnerabilities in their operational environments and implementing the appropriate countermeasures. COs/OICs are responsible for ensuring that personnel under their command are trained and abide by IA policy. Commanders of DON organizations shall ensure that all IT assets they oversee and operate are accredited and operated in accordance with the accreditation documentation.

2.4.12. Privileged Users. Individuals who have access to system control, monitoring, or administration functions (e.g., system administrator, IAO, system programmers, etc.) are Privileged Users. Privileged Users are responsible for providing IA safeguards and assurances to the data they control as well as their personal authentication mechanisms.

---

[4] DON memorandum to CNO and CMC, "Designation of the Department of the Navy Deputy Chief Information Officer (NAVY) and the Department of the Navy Deputy Chief Information Officer (MARINE CORPS)," 22 Aug 2005.

2.4.13. Users. Individuals or system processes authorized to access an information system. Users are responsible for the protection of data they create and compliance with IA policy requirements.

3. CHAPTER 3 – MANAGEMENT CONTROLS

3.1. INTRODUCTION

3.1.1. DON IA management controls focus on the direction of IA-related activities (policy), the acquisition of systems and services, and the certification and accreditation (C&A) of information systems.

3.2. POLICY MANAGEMENT

3.2.1. Department of the Navy IA policies are generated and promulgated by the DON CIO (and the DON Senior IA Officer as a focal point within DON CIO) and provide DON-specific interpretations of laws, regulations, and executive policy. They also address requirements set forth by DoD and component organizations. They are general statements of organizational intent and provide specific IA roles and responsibilities for members of the DON.

3.2.1.1. USMC IA implementation guidance is generated and promulgated by the DON Deputy CIO (Marine Corps).

3.2.1.2. USN IA implementation guidance is generated and promulgated by the DON Deputy CIO (Navy).

3.2.2. Effective IA implementation relies on consistent, clearly documented operating procedures for both system configuration and operational use.

3.2.3. Procedures shall define deployment of the system, system configuration, day-to-day operations for both the system administrator and user, as well as how to respond to real or perceived attempts to violate system security.

3.2.4. All DON information systems and networks shall include written standard operating procedures, which are routinely updated and tailored to reflect changes in the operational environment.

3.3. SYSTEM AND SERVICES ACQUISITION

3.3.1. Cost-effective IA measures shall be incorporated in each acquisition program in accordance with DoDD 8580.1, *Information Assurance (IA) in the Acquisition Defense System*.

3.3.1.1. IA concepts shall be a visible element of all investment portfolios incorporating DoD-owned or controlled information systems, to include outsourced business processes supported by private sector information systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives.

3.3.1.2. Data shall be collected to support reporting and IA management activities across the investment life cycle.[6]

3.3.1.3. Explicitly identify and integrate funding for IA technologies and programs into IT investment and budgeting plans.

3.3.1.4. Establish consistent methodologies for determining information security costs for all systems and networks.

3.3.1.5. System acquisition may not proceed prior to registration with the DON system inventory.

3.3.1.6. System developers shall design or acquire information systems according to the Ports, Protocols and Services Assurance Category Assignments List and shall ensure newly developed, acquired or modified systems be assessed for operational risk by the Ports, Protocols and Services Configuration Control Board per DoDI 8551.1, *Ports, Protocols, and Services Management*.

3.3.1.7. The National Information Assurance Partnership (NIAP) is a U.S. Government initiative originated to meet the security testing needs of both IT consumers and producers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under the *Computer Security Act of 1987* (Public Law (PL) 100-235). The partnership combines the extensive IT security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems. DON organizations acquiring IA products must acquire those that are NIAP-evaluated. A current list of validated products may be viewed at http://niap.nist.gov/. If a DON organization requires an IA product for which a NIAP evaluation does not exist, use the DoD C&A process to provide evidence to the DAA of the risk associated with using the product. However, DON organizations should only acquire IA products without a NIAP evaluation in the most exceptional cases.

3.3.2. Life Cycle Support

3.3.2.1. Implement sound security procedures early in system design to increase the effectiveness of other security mechanisms. Incorporate appropriate security features at the individual system level and consider the vulnerabilities that may surface when operating with other systems over shared communication links. Consider the inherent risk of operating less secure systems inside a secure enclave.

3.3.2.2. Each system shall include risk assessment and risk management programs throughout the system's life cycle.

3.3.2.3. To the extent possible, legacy systems shall employ system security standards that support relevant security policies and procedures within a secure enclave. Modifications to legacy systems shall prioritize incorporation of common security procedures

[6] DoDD 8500.1, Information Assurance (IA)

and products to improve their overall security postures. Legacy systems with weak security implementations shall be placed outside the secure enclave or in a separate demilitarized zone (DMZ) if they pose significant security risks to other information resources protected within the enclave. Ultimately, most legacy networks will migrate to the single DON Enterprise network, NMCI.

3.3.3. Acquisitions

3.3.3.1. Information Assurance Strategies ensure that IA planning is started at the beginning and continues throughout an IT program's acquisition life cycle. They demonstrate that system developers have appropriate awareness of IA policies and procedures and that C&A activities are progressing. DoD policies and guidance for acquisition are found in DoDI 5000.2, *Operation of the Defense Acquisition System,* and DoDI 8580.1. The DON Information Assurance Strategy Guidance is available on the DON CIO website: http://www.doncio.navy.mil (search on "IA Strategy").

3.3.3.2. IA requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems. These requirements apply to all IT systems (note that this is inclusive of weapon and C4ISR systems).

3.3.4. Outsourced Information System Services

3.3.4.1. Review contracts to ensure that information assurance is appropriately addressed in the contracting language.

3.3.4.2. Require appropriate safeguards to protect outsourced systems and networks from unauthorized access throughout all phases of a contract. Monitor performance to ensure compliance with IA requirements.

3.3.4.3. Contract personnel may not be assigned to perform inherently governmental IA functions.[7] For example, contract personnel may not make final certification or accreditation decisions.

3.4. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT

3.4.1. Certification and Accreditation. The C&A process leads to an informed system accreditation decision based on risk-management principles. Accreditation may be granted by DAAs only after systems are identified and categorized, IA controls are assigned and implemented, and control implementations are validated.

3.4.1.1. All DON information systems (as defined in DoDD 8500.1) shall be certified and accredited for operation.

[7] SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy

3.4.1.2. Information systems developed or procured by a program office or local authority shall be accredited at the system level prior to deployment, as well as at the site level as part of the overall site accreditation.

3.4.1.3. DON C&A shall be conducted in accordance with DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process* and DoD 8510.1-M, *Department of Defense Information Technology Security Certification and Accreditation Process Application Manual*. These documents present the standard DoD approach for: identifying, implementing, and validating IA Controls; authorizing the operation of DoD information systems; and managing IA posture across DoD information systems. The process ensures compliance with various Federal reporting requirements and flexibility in a changing technical and threat environment.

3.4.2. Identify and Categorize Systems. The provision of IA is dependent on the accurate and timely identification and categorization of systems; understanding which assets require protection and the level of protection appropriate for each asset is necessary for the development of a comprehensive and effective IA program. All DON information systems shall be identified and reported to the DON system inventory. Categorization addresses a system's classification level and mission assurance category as described in DoDI 8500.2.

3.4.2.1. Services shall annually certify that all mission critical, mission essential, and mission support systems are included in the DoD's system inventory or that systems are separately included in the Intelligence Community's system inventory. Descriptions of "mission critical" and "mission essential" are described in DoDI 5000.2, Enclosure 4. A definition of "Mission Support is located in Appendix B.

3.4.2.2. Each inventory entry shall be updated at least quarterly[8] and shall include several mandatory elements, including: date of most recent security control testing, listing of system interconnections, and system mission assurance categories and classification levels. Detailed information about mission assurance categories may be found in DoDI 8500.2. Detailed information about classification levels may be found in SECNAVINST 5510.36, *Department of the Navy Information Security Program Regulation*.

3.4.3. Assign, Implement, and Validate IA Controls. Every DON information system shall include risk assessment and risk management programs. When assigning IA controls from DoDI 8500.2, consider the mission assurance category and classification level of a system. Also consider the specific risks to a system and address general and localized threats and vulnerabilities (risk assessment). Implementation of IA controls varies with operating environment and shall be documented as a portion of the C&A package (risk management). Validation techniques will vary between controls; DoD C&A policy provides specific guidance on selecting and implementing IA control validation techniques (risk management).

3.4.4. Plan of Action and Milestones. The Plan of Action and Milestones (POA&M) is a Federally-mandated[9] management tool for tracking IA weaknesses and weakness mitigation

[8] Mandate established under FISMA. Deadlines are December 1, March 1, June 1, and September 1.
[9] Mandate established under FISMA.

activities. POA&Ms identify discrepancies between implementation results and C&A specifications.

3.4.5. Make Certification Determination. Certification represents the comprehensive evaluation of a system's IA control implementation to establish the extent to which the implementation meets a set of specified security requirements. Certification decisions are based on an assessment of the actual validation results.

3.4.6. Make Accreditation Determination. Accreditation is a formal declaration by the DAA that an information system is approved to operate in a prescribed operational configuration using a defined set of IA controls. Accreditation decisions are risk-based and shall be based on a balance of mission or business need, protection of personal privacy, protection of information being processed, and protection of the information environment. Accreditation decisions are documented with a written Approval to Operate, Interim Approval to Operate, or disapproval. The DAA may revoke accreditation and connectivity for systems and networks when it is determined that appropriate IA controls are not implemented correctly.

3.4.7. Maintain Approval to Operate and Conduct Reviews. Computers and the environments they operate in are dynamic. System technology and users, data and information in the systems, risks associated with the system and, therefore, security requirements are ever-changing. Design, execute, and maintain a Lifecycle Implementation Plan that specifies the C&A schedule for all systems. Reevaluate system security postures at least annually or when there are significant modifications that change the security posture or accreditation status..

3.5. SYSTEM INTERCONNECTIONS

3.5.1. Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources* requires "written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems." DON information systems satisfy this requirement through compliance with the connection approval procedures established in CJCSI 6211.02B, *Defense Information System Network: Policy, Responsibilities and Processes*.

3.5.2. Written agreements between Government networks that are under the purviews of different DAAs detailing proof of accreditation, acceptance of risk, and related responsibilities shall be in place prior to interconnection between networks. Assessing benefits and risks of internetworking, as compared with the costs to mitigate and control risks, is required as part of the overall vulnerability analysis. Decisions to maintain connections to other networks should be made with awareness of the lack of control over the security safeguards in use by other network infrastructures.

3.5.3. Dynamic interaction among accredited software systems that have been designed to interact is not considered a security relevant event. This includes authorized messaging with non-DoD information systems, e.g., electronic commerce/electronic data interchange transactions with an information system belonging to another department or agency.

3.5.4. DON connections to the Defense Information Infrastructure, including the Non-Classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router

Network (SIPRNet), shall be coordinated in accordance with established Defense Information Systems Agency (DISA) requirements. Appropriate protections shall be employed in a DiD approach to protect the associated data and systems. Commanders of DON organizations shall obtain formal authorization to interconnect information systems in accordance with DoDI 8500.2.

3.5.4.1. DON systems that connect directly to non-DoD infrastructures such as the Internet shall apply appropriate security technologies, to specifically include a firewall, to protect information technology resources from unauthorized external activities. Do not design or connect without the approval of the appropriate DAA. Such systems shall conform to requirements set forth in DoDI 8551.1, *Ports, Protocols, and Services Management*.

3.5.5. Cross Domain Solutions. A Cross Domain Solution provides the ability to manually and/or automatically access and or transfer information between two or more differing security domains. Interconnections between DoD information systems of different security domains or with other U.S. Government systems of different security domains shall be employed only to meet compelling operational requirements, not operational convenience. Service-level validation as well as Service and formal Defense Information Systems Network (DISN) DAA authorization are required prior to making connections. Details of the Navy Cross Domain Solution process and sample documents including request forms and checklist can be obtained from https://infosec.navy.mil/, and Marines are directed to use this site also.

3.6. OVERSIGHT AND COMPLIANCE

3.6.1. The *Federal Information Security Management Act of 2002 (FISMA)* is a part of the *E-Government Act of 2002* (PL 107-347). FISMA places requirements on government agencies and their components, with the goal of improving the security of federal information and information systems.

3.6.2. FISMA requires the Head of each Federal Agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.

3.6.3. FISMA requires each federal agency to report to Congress annually, addressing the adequacy and effectiveness of information security policies, procedures, and practices. In addition to the annual report, FISMA requires each agency to conduct an annual independent evaluation of the IA program and practices to determine their effectiveness. The annual DON FISMA Report is submitted to the DoD Office of the Assistant Secretary of Defense (Networks and Information Integration), which sends a composite FISMA report to OMB and Congress.

3.6.4. The annual FISMA report changes each year. Generally, it summarizes the data in the DON IT Registry, including C&A status of systems and networks, dates of annual reviews, and dates of annual testing of security controls and contingency plans. It also includes personnel training statistics. These statistics play an important part of Congress' annual "grading" Federal agency security programs.

3.6.5. DON Program Managers/System Managers, DON Command Information Officers, and Functional Area Managers are responsible for updating FISMA data in the DON IT Registry, which is the database for DON FISMA reporting.

4. CHAPTER 4 – OPERATIONAL CONTROLS

4.1. INTRODUCTION

4.1.1. DON IA operational controls focus on activities that are implemented and executed by people as opposed to systems. These controls are put in place to improve the security of a particular system or group of systems. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

4.2. PERSONNEL SECURITY

4.2.1. Introduction

4.2.1.1. Personnel security controls evaluate the military, civilian, and contractor personnel who develop, use, operate, administer, maintain, defend, and retire DoD or DON Information Systems. These controls support assurance that the right people have access to the right information and information systems.

4.2.1.2. DON shall have a workforce that is sufficiently educated and trained to assure the security of government networks and information. DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, establishes IA training, certification, and workforce management policy for DoD.

4.2.1.3. DoDD 8500.1 defines information technology position categories applicable to unclassified DoD information systems. It provides a designator that indicates the level of IT access required to execute the responsibilities of the position, based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. The position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor, or a foreign national.

4.2.1.4. SECNAVINST 5510.30A, *Department of the Navy Personnel Security Program*, established the DON Personnel Security Program to authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties, including IT duties, to those persons whose loyalty, reliability and trustworthiness are such that entrusting the persons with classified information or assigning the persons to sensitive duties is clearly consistent with the interests of national security. The criteria for designating DON IT-I, IT-II and IT-III positions, and the investigative and adjudicative standards for assignment are provided in SECNAVINST 5510.30A.

4.2.2. Access Control. An individual's access to DON information and resources is contingent upon having the need-to-know, holding the appropriate security clearances, and authorization by the cognizant DON Commanding Officer. Need-to-know is defined as the

necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties.[10]

4.2.3. Foreign Nationals

4.2.3.1. "Foreign nationals" refers to all individuals who are not citizens or nationals of the U.S. This may include some U.S. military personnel, DoD civilian employees, and contractors.

4.2.3.2. Access to systems or information by foreign nationals or representatives of foreign entities shall be limited, but may be permitted under controlled conditions. Authorization for access to DON IT systems depends on meeting criteria for need to know, possession of appropriate level of security determination, and compliance with applicable DoD, DON, and the U.S. Department of State policies.

4.2.3.3. Where foreign national access is required, each system shall have policies and procedures to ensure that access is authorized only to information approved for release to that foreign national's government, and for controlled unclassified information authorized for release in accordance with the International Traffic in Arms Regulations and the Export Administration Regulations.

4.2.3.4. Foreign nationals shall be identified as such in all network communications, including e-mail addresses, display names, and electronic signatures.

4.2.3.5. SECNAVINST 5510.34A, *Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives*, is the primary reference regarding the disclosure of DON military information to foreign governments and international organizations.

4.2.3.6. Requirements for permitting foreign national access to systems or information are specified by DoDD 8500.1; Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, *Defense-in-Depth: Information Assurance and Computer Network Defense*; SECNAVINST 5510.30A; and SECNAVINST 5510.36.

4.2.3.7. DAAs and IAMs shall be U.S. citizens. DAAs shall be civilian or military employees of the U. S. Government, while IAMs shall be civilian, military, or contract employees of the U. S. Government.

4.2.3.8. IAOs and personnel with privileged access may be contractors or foreign nationals, provided requirements of DoDI 8500.2 and SECNAVINST 5510.30A are met. For foreign nationals, requirements include submission of a complete waiver package per SECNAVINST 5510.30A.

4.2.4. Privileged Access. A privileged user is an authorized user who has access to system control, monitoring, or administration functions.[11] Privileged access to DON systems

[10] DoDD 8500.1

[11] DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 2003, section E2.1.44

should only be held by personnel whose current job duties require that level of access. SECNAVINST 5510.30A specifies requirements for privileged access to DON systems.

4.2.5. IA Workforce Identification, Tracking, and Reporting

4.2.5.1. IA duties may be performed full-time or part-time, as additional/embedded duties, by a DON employee (civilian or military) or by a support contractor. All IA workforce personnel (military, civilian, contractor, and foreign/other nationals in each of those groups) shall be identified, tracked, and managed so that IA positions are staffed with personnel trained and certified by category, level, and function.[12]

4.2.5.2. Personnel Identification and Tracking

4.2.5.2.1. DoDI 8500.2 and SECNAVINST 5510.30A state that DAAs and IAMs shall be U.S. citizens. DAAs shall be civilian or military employees of the U. S. Government, while IAMs may be civilian, military, or contractor employees. See DoDI 8500.2 and SECNAVINST 5510.30A for more information.

4.2.5.2.2. Personnel performing IA privileged user or management functions, regardless of job series or military specialty, shall be appropriately identified in applicable Naval personnel databases.

4.2.5.2.3. The status of IA personnel certifications and certification status shall be identified, documented, and tracked in Naval personnel databases.

4.2.5.2.4. Contractor personnel performing IA functions shall have their IA certification category and level documented in the Defense Eligibility Enrollment Reporting System.

4.2.5.3. Workforce Systems

4.2.5.3.1. All IA-related positions are assigned in writing, including a statement of IA responsibilities, and appointees to positions shall receive appropriate IA training.[13]

4.2.5.3.2. All civilian positions with IA functions, regardless of Office of Personnel Management series or job title, will be identified as IA workforce in the Defense Civilian Personnel Data System.

4.2.5.3.3. All military billets with IA responsibilities, whether full time, part time, or as a collateral duty, shall be identified in USN or USMC workforce databases.

4.2.5.4. IA Workforce Reporting

[12] DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, 15 August 2004
[13] DoDI 8500.2, section 5.8.2

4.2.5.4.1. IA training shall be monitored and reported as an element of mission readiness and as a management review item. The status of awareness and training provision and certifications shall be reported to DON CIO as an element of mission readiness.

4.2.5.4.2. Reporting requirements are applicable to all personnel performing IA functions, inclusive of contractors and foreign nationals.

4.3. PHYSICAL AND ENVIRONMENTAL PROTECTION

4.3.1. Physical Security is the action taken to protect DON information technology resources (e.g., installations, infrastructure, personnel, equipment, electronic media, and documents) from damage, loss, theft, or unauthorized physical access.

4.3.2. Commanders of DON organizations are responsible for ensuring the physical security posture is accurately assessed and security resources are appropriate to protect DON information and resources in accordance with SECNAVINST 5510.34 and SECNAVINST 5510.36.

4.4. CONTINGENCY PLANNING

4.4.1. All DON units shall be prepared to recover from disasters and continue operations in the event of the non-availability of information systems and resources or denial of service conditions. Contingency plans shall be developed, evaluated, and annually tested to prepare for emergency response, backup operations, and post-disaster recovery. At a minimum, contingency planning shall address reconstitution for the loss of processing, storage, or transmitting of information.

4.4.2. System and network design shall incorporate redundancy and data backup in accordance with the level of IA controls for the system's mission assurance category (MAC) level. For some systems or networks, this will require a remote site capable of providing network operations using routine system backups stored offsite in preparation for a disaster. NIST Special Publication 800-34, *Contingency Planning for Information Technology Systems,* provides guidance on developing contingency plans, including disaster recovery.

4.4.3. The DON continuity of operations (COOP) program provides the means to continue DON mission essential operations during national security emergencies and events requiring all or part of the DON to be relocated or reconstituted. Program details are described in SECNAVINST 3030.4A, *Department of the Navy Continuity of Operations (DON COOP) Program*.

4.5. CONFIGURATION MANAGEMENT

4.5.1. Configuration management identifies, controls, accounts for, and audits all changes to a site or information system during its design, development, and operational lifecycle. Proper configuration management is essential to the maintenance of system accreditation status. For each change or modification to an information system or site configuration, assess the security impact of the change against the accreditation conditions issued by the DAA.

4.5.2. Various federal departments and agencies publish baseline security requirements for commonly deployed IT hardware and software. Key resources include:

NSA Security Configuration Guides address a wide variety of open source and proprietary software.
http://www.nsa.gov/snac/.

DoD Security Technical Implementation Guides include configuration standards for IA and IA-enabled devices and systems, security checklists, and security readiness review scripts for testing products for compliance with standards.
http://iase.disa.mil/stigs/index.html.

NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, provides checklists of settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government.
http://csrc.nist.gov/checklists/index.html.

4.6. MALICIOUS CODE PROTECTION

4.6.1. Malicious code refers to any type of computer software, standalone or embedded, designed to perform some type of unauthorized or undesirable activity. This includes viruses, worms, spyware, Trojan horses, and other executable files and scripts that intentionally or unintentionally perform unauthorized activities or act in a malicious manner.[14]

4.6.2. The most critical countermeasure to malicious code is the installation and maintenance of anti-virus software. This software is available to all DoD components at no cost and is downloadable from the DoD IA Portal and the DON IA website.[15]

4.7. INTRUSION DETECTION TOOLS AND TECHNIQUES

4.7.1. Network management tools are used to detect, isolate, and react to intrusions, disruption of services, or events that threaten the security of DON information technology resources. Intrusion detection is performed by personnel actively monitoring the outputs of these tools.

4.7.2. The Navy Computer Incident Response Team (NAVCIRT) and the Marine Corps Network Operations and Security Center (MCNOSC) monitor networks for these types of events. More information on DON incident response will be published in a forthcoming manual.

4.8. SECURITY ALERTS AND ADVISORIES

4.8.1. A vulnerability is a weakness in an information system that may lead to an undesirable reduction in confidentiality, integrity, availability, non-repudiation, and/or

[14] Source: http://www.cert.mil/antivirus/malcode.htm
[15] Source: http://iase.disa.mil/ or https://infosec.navy.mil/.

authentication of information. Vulnerabilities are identified throughout the system development lifecycle through demonstration, inspection, and/or analysis. Operational systems shall be subjected to vulnerability scanning.

4.8.2. The IA Vulnerability Management (IAVM) process generates alerts that are issued by DoD to direct enterprise-wide response to specific software vulnerabilities. IAVM actions shall be addressed and compliance reported within the timeframe allotted by DoD.

4.8.2.1. The IAVM program applies to any asset on any DON owned or controlled information system network.

4.8.2.2. IAVM notifications originate at DoD and are disseminated through NAVCIRT and MCNOSC via record message traffic.

4.8.2.3. There are three types of IAVM notifications:

4.8.2.3.1. IA Vulnerability Alerts (IAVA) address severe network vulnerabilities resulting in immediate and potentially severe threats to DON systems and information. Corrective action is of the highest priority due to the severity of the vulnerability risk.

4.8.2.3.2. IA Vulnerability Bulletins (IAVB) address new vulnerabilities that do not pose an immediate risk to DON systems, but are significant enough that noncompliance with the corrective action could escalate the risk.

4.8.2.3.3. Technical Advisories (TA) address new vulnerabilities that are generally categorized as low risk to DON systems.

4.8.3. NAVCIRT issues periodic advisories summarizing and highlighting computer incidents or addressing immediate threats. NAVCIRT issues Computer Task Orders, Advisories, and Alerts. MCNOSC issues Operational Directives and Advisories.

4.8.4. The Information Operations Condition (INFOCON) system is a commander's alert system that establishes a uniform process for posturing and defending against malicious activity targeted against DoD information systems and networks.

4.8.4.1. The five INFOCON levels include: Normal, Alpha, Bravo, Charlie, and Delta. These are defined in DoDD O-8530.1, *Computer Network Defense*.

4.8.4.2. The Commander, United States Strategic Command (STRATCOM) establishes the INFOCON level for the DoD. Changes of INFOCON level are sent from STRATCOM to NAVCIRT and MCNOSC, which forward them to all USN and USMC Commands.

4.8.4.3. Commanders at all levels of the Department of Defense are authorized to elevate INFOCONs for information systems and networks within their area of authority to levels higher than the DoD level.

4.8.4.4. An increase in INFOCON requires timely notification. For further guidance regarding the INFOCON system, see DoDD O-8530.1, CJCSM 6510.01, and STRATCOM.

4.9. VALIDATION ACTIVITIES

4.9.1. Assistance is available to assess and improve the IA posture, by identifying vulnerabilities in an operational environment and validating a site's overall security posture and degree of system integration.

4.9.2. Validation may occur locally. Requests for on-line surveys, IA assist visits, and Red Team support may be made to NAVCIRT or MCNOSC via appropriate command. Assistance is also available to support vulnerability identification and mitigation via appropriate Service commands.

4.9.2.1. Blue Team Operations. A Blue Team operation uses a team specifically constructed for the Inter-Deployment Training Cycle charged with assisting in the protection of the targeted assets and conducting training to local personnel. The Blue Team provides special technical expertise to system/security administrators and managers to assist command personnel in defensive actions. Blue Team trusted agents provide assistance in identifying Red Team attacks and serve as safety observers to ensure that safety is not compromised.

4.9.2.2. Red Team Operations. A Red Team operation is an independent and threat based effort by an interdisciplinary, simulated opposing force, which after proper safeguards are established, uses both active and passive capabilities on a formal, time-bounded tasking to expose and exploit IA vulnerabilities of friendly forces. Red Team operations may be employed to validate existing IA protections and to exercise standard operating procedures and tactics to evaluate vulnerabilities.

4.9.2.3. Information Assurance Assist Visits. The Computer Network Vulnerability Assist is a three-phase exercise designed to provide assistance in the identification and subsequent safeguarding of information system vulnerabilities. In Phase One, Configuration Management and Vulnerability Assessment, the Blue Team ensures configuration is current. In Phase Two, Risk Assessment and Active Computer Network Defense, internal training, risk assessment, and management updates occur. In Phase Three, Red Team Assessment, the exercise Blue Team tests the skills learned from the previous phases in order to evaluate their network protection strategy and capabilities. There are three teams or “cells” at work during this phase, Red (attackers), Blue (defenders, serve as trusted agents) and White (safety observers and exercise coordinators).

4.10. MEDIA PROTECTION

4.10.1. Protect all electronic media (e.g., compact disks, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information from unauthorized access.

4.10.2. Control access to such materials, and ensure that they are properly labeled, stored, destroyed, and disposed of in accordance with the rules for the data they contain. This includes all sensitive unclassified data not approved for public release. This also includes special handling instructions for U.S. classified and NATO marking and release requirements.

4.10.3. SECNAVINST 5510.36 defines the DON Information Security Program policies, including media marking requirements.

4.11. INCIDENT DETECTION AND RESPONSE

4.11.1. An event is an observable occurrence, not yet assessed, that may affect the performance of a system. Examples of events include a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail, or a firewall blocking a connection attempt.

4.11.2. Incidents are adverse events with a negative consequence. Examples of incidents include the unauthorized use of another user's account, the unauthorized use of system privileges, and the execution of malicious code that destroys data, and data manipulation such as web defacements. There are two types of incidents pertinent to this document.

4.11.2.1. An IA incident is an assessed event having actual or potentially adverse effects on an information system.

4.11.2.2. A Communications Security (COMSEC) incident is an assessed event that potentially jeopardizes the security of COMSEC material or the secure electronic transmission of national security information or information governed by Title 10 U.S.C. Section 2315.

4.11.3. Sites shall have a structured ability to audit, detect, isolate, react, and promptly report incidents.

4.11.4. USMC personnel shall report potential IA incidents to the MCNOSC via their chain of command. USN personnel shall report events and incidents to NAVCIRT via their chain of command.

4.11.5. Incident Response Guidance.

4.11.5.1. CJCSI 6510.01 provides instruction on IA incident response and reporting requirements.

4.11.5.2. SECNAVINST 5510.36 describes the DON Information Security Program (ISP). The ISP instruction provides DON policy and incident reporting requirements.

4.11.5.3. Note that not all computer incidents will result in a reportable loss or compromise of classified information. When an incident does occur, be cognizant of DON dual reporting requirements.

4.12. AWARENESS AND TRAINING

4.12.1. DON shall establish, resource, and implement IA training and certification programs for all Naval personnel – military and civilian – in accordance with SECNAVINST 5239.3A. These programs shall train, educate, certify, and professionalize personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and retire DoD information systems.[16]

4.12.2. Initial IA Awareness training shall be provided to all military, civilian, and contractor personnel as a condition of access to DON information systems in any system lifecycle phase.

4.12.3. IA professionals shall complete specialized position-specific training as required. Training should emphasize achieving appropriate IA certifications.

[16] DoDI 8500.2, Section 5.7.7

5. CHAPTER 5 – TECHNICAL CONTROLS

5.1. INTRODUCTION

5.1.1. The technical class of IA controls focuses on IA controls established by people but executed by systems. To be effective, these controls are dependent upon the proper functioning of the systems. Implementation of technical controls requires significant operational considerations and should be consistent with the management of IA within the organization.

5.2. USER IDENTIFICATION AND AUTHENTICATION

5.2.1. Identification and authentication refers to the technical means by which information systems verify the legitimacy of a request for access by a person or another system. An identity is an assertion that the user is person X. Authentication provides proof to support that assertion. There are three types of proof supporting authentication:

5.2.1.1. Something you know – A secret, such as a password or a personal identification number.

5.2.1.2. Something you have – A recognized object, such as a DoD Common Access Card or a Public Key Infrastructure (PKI) certificate.

5.2.1.3. Something you are – A unique attribute of the user, such as a fingerprint or iris scan.

5.2.2. All DON information systems must require at least one of the three methods above to identify a user for the purpose of access in addition to need-to-know and security clearance requirements. DAAs will ensure that the identifying mechanism is appropriate for the system criticality. For example, access to a MAC I system with classified information should require at least two of the three identification mechanisms.

5.3. PUBLIC KEY INFRASTRUCTURE

5.3.1. Public Key Infrastructure is an enabling technology that enhances information systems security, promotes secure electronic commerce, and supports the automation of many current paper-based manual processes. Public key cryptography offers DON IT environments the best available technology for secure transmission of unclassified data across public and private wide area networks. It provides a high degree of assurance of data confidentiality, integrity, authentication, and user identification among users of public key enabled information systems, including network login, e-mail, web-based information services, and electronic commerce transactions.

5.3.2. DON information systems including networks, e-mail, and web servers shall be enabled to use DoD PKI certificates to support authentication, access control, digital signature, and encryption. PKI requirements for DoD and DON information systems and applications can be found in DoDI 8520.2, *Public Key Infrastructure and Public Key Enabling*.

5.4. AUTHENTICATOR MANAGEMENT

5.4.1. An authenticator is the means used to confirm the identity of a station, originator, or individual.

5.4.2. The Common Access Card (CAC) is the DoD's cyber and physical identification card for all active duty Uniformed Services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD networks and e-mail services. The CAC is organization independent and interoperable across all DoD Departments and Agencies including the DON.

5.4.3. The CAC is the primary token for generation, storage, and use of DoD PKI certificates.

5.4.4. Authenticators shall be protected commensurate with the classification or sensitivity of the information accessed; they shall not be shared, and they shall not be embedded in access scripts or stored on function keys.

5.4.5. Passwords shall be encrypted both for storage and for transmission. Password criteria are specified in CJCSM 6510.01.

5.5. ACCESS CONTROL POLICY AND PROCEDURES

5.5.1. Access Controls are used to ensure the confidentiality, integrity, and availability of data and information systems by limiting access to authorized personnel. Access to all DoD information systems shall be based on a demonstrated need-to-know and granted in accordance with SECNAVINST 5510.30A requirements for position designation, personnel security investigation, and adjudication.

5.6. ACCOUNT MANAGEMENT

5.6.1. Account management ensures that valid user accounts are associated with active, authorized personnel. While applicable to all types of accounts, account management for privileged user accounts is critical. System administrators shall monitor user account inactivity and establish procedures for investigating, deactivating, and eliminating accounts that do not show activity over time.

5.7. BOUNDARY DEFENSE

5.7.1. In DON networks, a DMZ, also know as a "screened subnet," exists logically between the public domain (Internet) and the DISN. This boundary condition can be physical or virtual. One option for creating this dedicated network segment is to operate a dedicated network segment with a firewall installed at both ends, thus better protecting the internal network during external information exchange and providing external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. Both firewalls will have different rule sets according to the specific access controls for the attached networks and the interior firewall will be more restrictive than the exterior firewall. A DMZ may also include an intrusion detection system sensor to alert the appropriate personnel of suspicious

and/or malicious network traffic. In order to defend the internal network, services that are accessed from external networks, such as e-mail and web servers, must be placed in a DMZ.

5.7.2. Deploy firewalls, intrusion detection systems, and other NIAP or NSA-approved security solutions to provide exterior protection to networks. Boundary defenses shall be commensurate with the criticality and sensitivity of the systems in the network and appropriate to the operating environment.

5.7.3. Intranet and extranet web services shall be protected with appropriate access controls. Afloat commands shall only use Internet web-hosting services provided by a centralized network operations center.

APPENDIX A – REFERENCES

View http://iase.disa.mil/policy.html for a list of all IA-related laws, regulations, and policies.

Laws

Federal Information Security Management Act of 2002, Title III of E-Government Act of 2002 (PL 107-347), 17 Dec 2002

The Computer Security Act of 1987 (PL 100-235), 11 June 1987

Title X, United States Code, Chapter V, Armed Forces, 20 Oct 2000

Executive Branch Regulations

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

Department of Defense Directives and Instructions

IA Generally

DoDD 8500.1, *Information Assurance (IA)*, 24 Oct 2002

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 2003

CJCSI 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005

CJCSI 6211.02B, *Defense Information System Network (DISN): Policy, Responsibilities and Processes*, 31 July 2003

Acquisition

DoDI 5000.2, *Operation of the Defense Acquisition System*, 12 May 2003

DoDD 8580.1, *Information Assurance (IA) in the Acquisition Defense System*, 9 July 2004

Certification and Accreditation

DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP),* 30 December 1997

DoDI 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, 31 July 2000

Computer Network Defense

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 10 August 2004

CJCSI 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND)*, 15 June 2004

DoDD 0-8530.1, *Computer Network Defense (CND)*, 8 January 2001

Ports and Protocols

DoDI 8551.1, *Ports, Protocols, and Services Management (PPSM)*, 13 Aug 2004

PKI

DoDI 8520.2, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, 1 April 2004

Workforce Development

DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, 15 August 2004

DoD Strategic Documentation

Joint Vision 2020, June 2000

DoD IA Strategic Plan Version 1.1, January 2004

Department of the Navy Instructions

SECNAVINST 3030.4A, *Department of the Navy Continuity Of Operations (DON COOP) Program*, 27 July 2004

SECNAVINST 5239.3A, *Department of the Navy Information Assurance Policy*, 20 December 2004

SECNAVINST 5430.7N, *Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy*, 11 January 2005

SECNAVINST 5510.30A, *Department of the Navy Personnel Security Program*, 19 June 2000

SECNAVINST 5510.34A, *Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives*, 8 October 2004

SECNAVINST 5510.36, *Department of the Navy Information Security Program Regulation*, 17 March 1999

Other References

CNSS Instruction No. 4009, *National Information Assurance (IA) Glossary*, May 2003.

DON memorandum to CNO and CMC, "Designation of the Department of the Navy Deputy Chief Information Officer (NAVY) and the Department of the Navy Deputy Chief Information Officer (MARINE CORPS)," 22 Aug 2005.

Website References

Secretary of the Navy/Assistant for Administration Under Secretary of the Navy Publications website: https://www.navsopubs.hq.navy.mil.

Department of the Navy Electronic Directives System: http://neds.daps.dla.mil/.

DON CIO website: http://www.doncio.navy.mil.

USMC C4 Information Assurance website: https://hqdod.hqmc.usmc.mil/IA.asp

USN Information Assurance website: https://infosec.navy.mil/.

NSA National Information Assurance Partnership: http://niap.nist.gov/.

The DoD IA Portal: http://iase.disa.mil/eta/index.html.

The DoD IA Portal Policies list: http://iase.disa.mil/policy.html.

NIST Computer Security Resource Center: http://csrc.nist.gov/.

APPENDIX B – DEFINITIONS

The following definitions are critical to understanding IA. A comprehensive set of IA definitions is available from the Committee on National Security Systems Instruction Number 4009, *National Information Assurance (IA) Glossary* at http://www.cnss.gov/.

Accreditation	Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Authentication	Authentication is assurance of the identity of a message sender or receiver. Authentication is the security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Authenticator	The means used to confirm the identity of a station, originator, or individual.
Availability	Availability is assurance of timely, reliable access to data and information systems by authorized users. Availability-focused IA controls protect against degraded capabilities and denial of service conditions.
Certification	Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.
Class (Control)	IA controls are organized into three classes: management, operational, and technical.
Computer Network Attack	Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.
Confidentiality	Confidentiality is assurance that information is not disclosed to unauthorized persons, processes, or devices. It includes both the protection of operational information and the protection of IA-related system information such as password or configuration files.

Controls	The management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Controls also provide authentication and non-repudiation of communications.
Demilitarized Zone	A "screened subnet" that exists logically between the public domain (Internet) and the DISN. This boundary condition can be physical or virtual and is intended to isolate less secure systems and networks.
Enclave	Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.
Family (Control)	Within each IA control class, individual controls are grouped into families. A family consists of two or more controls designed to accomplish a similar purpose such as Certification and Accreditation or Contingency Planning.
Incident	Assessed occurrence having actual or potentially adverse effects on an information system. (COMSEC) Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or information governed by 10 U.S.C. Section 2315.
Information Assurance	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.
Information Operations	Actions taken to affect adversary information and information systems, while defending one's own information and information systems. Information Operations require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of command and control with intelligence support. Information Operations are conducted through the integration of many capabilities and related activities.

Information System	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.
Integrity	Integrity is assurance that information is not modified by unauthorized parties or in an unauthorized manner. Integrity supports the assurance that information is not accidentally or maliciously manipulated, altered, or corrupted. Additionally, integrity implies the ability to detect when information has been altered.
Legacy System	An existing system that is designated for closure when the capability is absorbed by an interim or core system or if the capability is no longer required. No modifications or enhancements are made to legacy systems.[17]
Management Controls	The management class of IA controls addresses topics that may be characterized as managerial. They are techniques and concerns that are normally directed or addressed by leadership. They focus on the management of IA and the management of risk.
Mission Assurance Category	Applicable to all DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity.
Mission Critical (System)	A system the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations.
Mission Essential (System)	A system that is basic and necessary for the accomplishment of the organizational mission.
Mission Support (System)	A system handling information that is important to the support of deployed and contingency forces. It must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified, but is more likely to be sensitive or unclassified).

[17] http://www.dod.mil/bmmp

Net-centricity	Net-centricity is the realization of a networked environment (including infrastructure, systems, processes, and people) that enables a completely different approach to warfighting and business operations. It compels a shift to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data. This extends beyond the traditional focus on standardized, predefined, point-to-point interfaces.
Non-repudiation	Non-repudiation is assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.
Operational Controls	The operational class of IA controls focus on activities that are implemented and executed by people as opposed to systems. These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and rely upon management activities as well as technical controls.
Risk	Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
Technical Controls	The technical class of IA controls focus on IA controls that are set up by people but executed by systems. To be effective, these controls are dependent upon the proper functioning of the systems. Implementation of technical controls requires significant operational considerations and should be consistent with the management of IA within the organization.
Threat	Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

APPENDIX C – ABBREVIATIONS AND/OR ACRONYMS

C&A	Certification and Accreditation
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CA	Certification Authority
CAC	Common Access Card
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CIO	Chief Information Officer
CND	Computer Network Defense
CO	Commanding Officer
COMSEC	Communications Security
DAA	Designated Approving Authority
DiD	Defense-in-Depth
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DON	Department of the Navy
DON CIO	DON Chief Information Officer
FISMA	Federal Information Security Management Act of 2002
GIG	Global Information Grid
IA	Information Assurance
IAM	IA Manager
IAO	IA Officer
IAVM	IA Vulnerability Management
INFOCON	Information Operations Condition
IO	Information Officer
ISP	Information Security Program
IT	Information Technology
MAC	Mission Assurance Category
MCNOSC	Marine Corps Network Operations Security Center
NAVCIRT	Navy Computer Incident Response Team
NIAP	National Information Assurance Partnership
NIPRNet	Non-secure Classified Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NSA	National Security Agency
OIC	Officer in Charge
OMB	Office of Management and Budget

PKI	Public Key Infrastructure
PL	Public Law
PM	Program Manager
POA&M	Plan of Action and Milestones
SECNAV	Secretary of the Navy
SECNAVINST	SECNAV Instruction
SECNAVMAN	SECNAV Manual
SIPRNet	Secure Internet Protocol Routing Network
STRATCOM	Strategic Command
USMC	US Marine Corps
USN	US Navy