DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
914 CHARLES MORRIS CT SE
WASHINGTON NAVY YARD DC 20398-5540

REFER TO:

COMSCINST 5239.3A
N6
14 October 2003

COMSC INSTRUCTION 5239.3A

Subj: MILITARY SEALIFT COMMAND INFORMATION ASSURANCE PROGRAM

Ref:
(a) SECNAVINST 5239.3, Department of the Navy (DON) Information Security Program, July 14, 1995
(b) OPNAVINST 5239.1B, DON IA Program, November 9, 1999
(c) NSTISSP No. 11, National Information Assurance Acquisition Policy, January 2000
(d) NSTISSI No. 4009, National Information Systems Security Glossary, September 2000
(e) Department of Defense (DoD) Directive O-8530.1, Computer Network Defense, January 8, 2001
(f) DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP), December 30, 1997
(g) through (oo) see enclosure (3)

Encl:
(1) Military Sealift Command Information Assurance Policy
(2) Military Sealift Command Information Assurance Implementation
(3) References, continued

1. Purpose. To establish the Military Sealift Command (MSC) Information Assurance (IA) Program. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMSCINST 5239.3.

3. Policy. All commands within MSC shall comply with the policies and guidance in this instruction. These policies are derived from national, DoD, DON and MSC requirements. Nothing in this instruction should be understood to contravene national, DoD or DON requirements, although MSC may impose stricter requirements than the higher level requirements. MSC IA policy is set forth in enclosure (1) and MSC IA implementation is set forth in enclosure (2). Guidance used in preparing this instruction is found in references (a) through (oo).

4. Action. MSC Program Managers, Functional Directors and Special Assistants will review enclosures (1) and (2) and ensure staff compliance. The Director, Command, Control, Communication and Computer (C4) Systems (N6) is delegated authority to sponsor all networks and information technology (IT) systems and administer enclosures (1) and (2) and to ensure compliance with cited references. Specific responsibilities are detailed in enclosure (2), which refers to delegated authority where applicable.

5. IA Roles and Responsibilities

a. Commander, MSC (COMSC). COMSC has the ultimate responsibility for IA for all MSC IT systems and enclaves and delegates the Designated Approving Authority (DAA) duties in writing to an individual at an appropriate level in the organization.

b. Designated Approving Authority. The DAA is the primary decision-maker for IA matters in MSC and is responsible for deciding whether or not to grant IT systems and enclaves approval to operate based on satisfactory implementation of acceptable IA controls. The DAA is responsible for ensuring that IA requirements are included throughout the life cycle of IT assets. The DAA or his designee is responsible for appointing Information System Security Managers (ISSMs) and the Information Assurance Program Manager (IAPM).

c. Information Assurance Program Manager. The IAPM is responsible for developing, implementing and managing the IA program and the IA organization; this includes staffing, funding and execution. The IAPM is responsible for maintaining this instruction and supporting the DAA, as required, with regard to MSC IA incidents and compliance with IA policy.

d. Information Systems Security Managers. ISSMs are responsible for all activity related to IA and for ensuring that all necessary IA tasks and functions are performed, with regard to personnel, systems or resources under their purview. This is accomplished by performing, directing, coordinating, administering and overseeing various activities and personnel, including appointing, in writing, as many Information Systems Security Officers (ISSOs), Network Security Officers (NSOs) and System Administrators, as needed.

e. Information Systems Security Officers/Network Security Officers. ISSOs and NSOs are responsible for ensuring that users under their purview comply with the IA program requirements and procedures on behalf of the ISSM. They are responsible for ensuring that all IA controls are appropriately implemented on systems and networks under their purview and that these controls are working properly to meet the IA requirements.

f. System/Network Administrators. System Administrators and Network Administrators are responsible for ensuring that all components of IT systems or networks for which they have been assigned functional responsibility are operating effectively and securely according to MSC, DON and DoD policies and procedures.

g. Facility Security Managers. Facility Security Managers are responsible for ensuring the physical security of IT facilities and IT assets under their purview. They coordinate IA-relevant facility issues with the appropriate ISSM and assist with the IA program, as appropriate.

h. Managers and Supervisors. Managers and Supervisors are responsible for ensuring that appropriate IA safeguards are used to adequately protect MSC data and IT assets under their purview. They must commit resources for IA requirements, and ensure that users under their purview comply with IA requirements.

i. User. A User is anyone, including all of the aforementioned roles, using IT assets. A User is responsible for complying with MSC, DON, and DoD IA policies and procedures for the secure operation and authorized use of MSC IT assets, per this instruction.

6. Effective Date. This instruction is effective immediately.

//S//
D. A. LOEWER
Vice Commander

Distribution:
COMSCINST 5215.5
List I (Case A, B, C)

Military Sealift Command Information Assurance Policy

Enclosure (1)

TABLE OF CONTENTS

1.0 IA POLICY INTRODUCTION

1.1 Purpose

This document promulgates Department of Defense (DoD), Department of the Navy (DON), and Military Sealift Command (MSC) Information Assurance (IA) policies, defines the scope and objectives of these policies and assigns responsibilities accordingly, to be used by MSC Headquarters, Area Commands, field offices and ships.

1.2 Scope

a. This document applies to:

(1) All MSC locations.

(2) All MSC-sponsored contractors and commercial partners who own, procure, use, operate or maintain IT systems at government or contractor owned facilities.

(3) All IT systems and resources designed, developed, procured or managed by MSC activities or by their contractors.

(4) IT systems operated on behalf of MSC, but not owned by MSC (e.g., U.S. Transportation Command (USTRANSCOM), Navy Marine Corps Intranet (NMCI)).

b. This document applies to all elements and categories of an IT system, including automated information system applications, enclaves, outsourced IT-based processes and platform IT interconnections. As required, specific activities are managed under separate instruction or notice (e.g., Classified Processing, teleworking, IT systems acquisitions).

c. This document requires that protective measures are applied to IT systems and enclaves based on their assigned mission assurance category. All IT systems and enclaves must be assigned a mission assurance category associated with the importance of the information they contain relative to the achievement of MSC goals and objectives.[1] The three mission categories are as follows.

(1) Mission Assurance Category I: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness.

[1] DoD Directive 8500.1 October 24, 2002, DoD Instruction 8500.bb (Draft), February 1, 2002.

(2) Mission Assurance Category II: Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.

(3) Mission Assurance Category III: Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities.

1.3 Background

MSC has prepared this policy document to integrate current IA concepts and capabilities in recognition that protection of MSC information and IT systems is key to mission accomplishment and the protection of lives, property and technology. This IA document ensures that responsive and cost effective IA measures will be employed throughout MSC to secure its boundaries and assure that IT systems are operated within an acceptable level of risk.

1.4 Objectives

a. To establish MSC IA policies that address the aspects of IA as promulgated by references (a) through (oo).

b. To ensure that MSC information processed, stored or transmitted is adequately protected with respect to the level of concern for confidentiality, integrity and availability.

c. To guide appropriate implementation of safeguards with respect to level of robustness necessary to protect MSC IT systems and information.

d. To integrate technical and non-technical processes of various security disciplines and guiding principles into one comprehensive and concise IA program.

e. To integrate IA with other MSC programs (e.g., life cycle management).

f. To standardize IA across MSC.

g. To align MSC IA activities with other DoD and DON organizations with whom MSC shares IA responsibility.

1.5 Document Organization

a. The front piece of this document contains the Instruction the Information Assurance Program. Enclosure (1) contains MSC IA policy applicable to all MSC IT and connections outside. Enclosure (2) contains MSC IA implementation. Enclosure (2) is divided into two portions, the first is implementation applicable to all IT systems and the second portion is additional implementation for classified systems.

b. Most terms used in this document are to be understood as defined in NSTISSI 4009.[2] Terms that are not defined in NSTISSI 4009 are defined in Section Four of enclosure (2). In electronic versions of this document, where possible, referenced documents will be linked to copies of the actual reference.

[2] NSTISSI No. 4009, National Information Systems Security Glossary, September 2000.

2.0 IA POLICY

a. IA is the set of activities that protect and defend information and IT systems by ensuring their availability, integrity and confidentiality. This includes providing for restoration of IT systems by incorporating protection, detection and reaction capabilities in a layered approach, often referred to as defense-in-depth. To determine the appropriate measures to be used to defend the information and IT systems MSC shall use the Information Systems Security Engineering (ISSE) process, as described in DoD 8500,[3] and the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).[4] The ISSE is an engineering process that captures and refines information protection requirements and ensures their integration into IT acquisition processes and ongoing management through purposeful security design or configuration. The DITSCAP is a management process for evaluating systems and providing a means for determining the amount of risk at which a system may operate.

b. Utilizing this defense-in-depth approach, the following policies shall be implemented by all MSC enclaves and IT systems. Controls for the following policies will be found in enclosure (2).

2.1 General Policies

a. All MSC information and resources shall be appropriately safeguarded at all times, to support defense-in-depth across MSC, DON and DoD. Safeguards shall be applied so that information and IT system resources maintain the appropriate level of protection for confidentiality, integrity and availability based upon:

(1) Mission criticality;

(2) Classification or sensitivity level of information entered, processed, stored or transmitted;

(3) Documented threats and vulnerabilities; and

(4) Cost effectiveness.

b. Compliance with the policies in this instruction shall be enforced. Violations of these policies shall be subject to disciplinary action, including criminal prosecution and administrative sanction.

[3] DoD Directive 8500.1 October 24, 2002, DoD Instruction 8500.bb (Draft), February 1, 2002.

[4] DoD Instruction 5200.40, DITSCAP December 30, 1997.

c. The operational view of the IA architecture shall be implemented by clearly delineating IA roles and responsibilities at all organizational and IT system levels in policy and practice.

d. The safeguards for a given system shall be appropriate for the most sensitive information stored in it. The safeguarding of information and IT systems shall be accomplished through the employment of multi-disciplined defensive layers, as well as sound administrative and operational practices.

e. IA shall be a visible element of all IT-dependent and IT-related investment portfolios, and shall be reviewed and managed relative to the return on investment, contributions to mission outcomes and contributions toward the achievement of strategic goals and objectives in accordance with public laws, Executive Orders, National Security Directives and DoD and DON directives and standards. Data shall be collected to support reporting and IA management activities throughout the investment life cycle.

f. Interoperability and integration of IA solutions within or supporting MSC shall be achieved through adherence to an IA architecture that is consistent with DoD, Joint Chiefs of Staff and DON technical standards framework and a defense-in-depth approach.

g. MSC shall follow national, DoD and DON policies for operating and protecting IT systems.

2.2 Risk Management

Risk shall be continuously assessed, analyzed and reviewed. All MSC personnel shall practice sound risk management. Risks shall be mitigated to the maximum extent possible, and only those residual risks that exist after due consideration has been given, based on current technology and cost/benefit analyses, will be accepted. All interconnections of MSC IT systems shall be managed to continuously minimize community risk by ensuring that the IA posture of one IT system is not undermined by vulnerabilities of interconnected IT systems.

2.3 Certification and Accreditation

a. All MSC IT systems and enclaves shall be certified and accredited in accordance with the DITSCAP.[5] Certification is the evaluation of the technical and non-technical IA features of an IT 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 IA requirements.

[5] DoD Instruction 5200.40, DITSCAP December 30, 1997.

b. Accreditation is the formal management authorization for operation of a specific implementation of an IT system, network, or computer resource based on the results of a security certification and risk analysis. It is the formal declaration by the DAA that subject IT systems are approved to operate in a particular security environment meeting a prescribed set of security requirements at an acceptable level of risk. At a minimum, the accreditation status of MSC IT systems shall be reviewed every 3 years. Changes that could affect the security posture of an IT system, such as the introduction of new systems, new connections and changes to the level of data processed, or configuration changes, may be cause for review of the accreditation status or issuance of an Interim Authority to Operate.

2.4 Defense-In-Depth

In order to protect sensitive and critical information and IT systems and enclaves, MSC follows defense-in-depth. Defense-in-depth is an integrated and multi-layered approach to protecting IT systems. Defense-in-depth uses several forms of defense against an intruder, recognizing that it is not possible to rely on any single defensive mechanism to secure IT systems and enclaves. Measures are intended to reinforce one another and enable MSC to quickly and effectively respond to an attack or breach of security.

2.4.1 Networks and Infrastructure

To ensure availability, MSC local and wide area communication networks need to be protected against attacks such as denial of service. To ensure confidentiality and integrity, the information transmitted over these networks and the characteristics of the traffic flow need to be protected against unintentional disclosure or exploitation. MSC shall employ controls that safeguard the communication networks and the information transmitted over these networks.

2.4.1.1 Network Security

Information systems and enclaves shall be configured with the most restrictive security rules and, at a minimum, must comply with MSC, DoD, DON and USTRANSCOM guidance with respect to managing ports, protocols and services. Network security controls shall be employed to protect confidentiality, integrity and accessibility of transmitted information between or outside MSC enclaves.

2.4.1.2 Communications Security

Communications Security (COMSEC) policies establish requirements designed to deny unauthorized access to information during transmission. COMSEC requirements vary according to the classification level of data and are designed to prevent the derivation of valuable information from other aspects of communications (traffic flow and message analysis) and to enhance the authentication of communications. MSC shall enforce COMSEC techniques to the extent necessary to deny information to unauthorized personnel and to effectively defend against interception, traffic analysis and imitative deception.

2.4.1.3 Connection Approval Process

MSC enclaves or other external organizations or systems, in order to connect to the MSC networks, shall be compliant with the MSC Enterprise Connection Approval Process.[6]

2.4.2 Enclave Boundaries

To resist active network attacks, enclave boundaries shall provide strong boundary defense such as traffic filtering and control and intrusion detection. MSC enclaves shall employ perimeter defense technologies (e.g., firewalls, IDS, DMZ, proxy servers, email/ Internet content screening filters and filtering routers) and host-based IA controls that are in concert with enclave perimeter protections.

2.4.3 Computing Environments

MSC shall protect the computing environment by employing controls to secure access, safeguard the confidentiality and integrity of data, securely configure and manage the computing environment, and defend against subversive acts of people and systems, both internal and external. Controls shall be implemented to protect system software. A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities shall be in place.

2.5 Key Management

MSC shall use a key management infrastructure based on DoD and DON public key infrastructure (PKI) policies and procedures.[7] PKI shall be incorporated into new IA-enabled acquisitions when possible.

[6] Memorandum 5230, MSC Enterprise Connection Approval Process, July 22, 2002.

[7] Public Key Infrastructure Roadmap, October 17, 2001, ITSG, X.509 Certificate Policy for the United States Department of Defense, Version. 5.2, November 13, 2000, DEPSECDEF Memorandum, subject: DoD PKI, August 12, 2000. Additional information can be found at the PKI Program Management Office Website.

2.6 Life Cycle Management

MSC IA requirements shall be identified and included in the design, acquisition, installation, operation, upgrade or replacement of all IT or IT-dependent systems in accordance with applicable national, DoD and DON instructions. All MSC enclaves shall consider IA policies throughout the life cycle of an IT system from beginning of concept development through design, development, operation, and maintenance until replacement or disposal.

2.6.1 Acquisition

IA objectives and requirements shall be included in the development or acquisition of all IT assets and services in accordance with national, DoD and DON policy and guidance.[8]

2.6.2 Configuration Management

Configuration management procedures shall be used to identify, control, and audit all changes made to enclaves or IT systems throughout their entire lifecycle. Configuration management shall be used to maintain an appropriate IA posture, based on the enclave or system's accreditation.

2.6.3 Continuity of Operations

All MSC enclaves shall employ administrative and operational procedures along with technical IT system measures to ensure continuity of operations. Data backups shall be scheduled, performed, stored, protected, and tested according to the criticality of the data. A contingency plan shall be developed for every mission essential and mission critical IT system within MSC.

2.6.4 Maintenance

Maintenance support shall be available to ensure that systems are operated in a manner that appropriately supports MSC. All persons who access a system to perform maintenance shall have the appropriate clearance to access the highest level of information on the system or shall be monitored by someone with technical expertise to detect unauthorized system modifications.

[8] e.g., NSTISSP No. 11, National Information Assurance Acquisition Policy, January 2000, Public Law 106-398, Title X, Subtitle G, Government Information Security Reform Act (GISRA), October 30, 2000, and Title 48, CFR Federal Acquisitions Regulations.

2.6.5 Disposal and Data Remanence

All documents, equipment and media shall be cleaned or destroyed, when released from MSC control or when released for use at a lower level of classification.

2.7 IA Infrastructure Disciplines

IA shall be enforced using an appropriate combination of personnel, IT, administrative and physical means that are validated through testing and are fully documented.

2.7.1 Personnel Security

Personnel security measures shall be used to have a well-trained and aware user population with access limited to data and systems based on clearance and need-to-know.

2.7.1.1 Clearance and Need-to-know

All IT system users who require access to IT systems and data shall possess the requisite clearance and need-to-know for the system.

2.7.1.2 IA Training and Awareness

All MSC IT users shall undergo IA training upon assignment with periodic refresher training to occur at least annually. Training compliance shall be tracked.

2.7.2 Administrative Security

Administrative security measures shall be enforced to control and monitor the access and use of data and IT systems and may be used to supplement technical measures when technical measures are infeasible or ineffective.

2.7.2.1 Logical Access

Logical access controls shall be implemented to ensure that only authorized users with the appropriate clearance and need-to-know can gain access to IT systems. Access procedures shall enforce the principles of separation of duties and “least privilege.”

2.7.2.2 Session Controls

Session controls shall be employed to restrict access based on inactivity and multiple logon attempts. Users shall be warned that they are entering a government information system, and are provided with the appropriate privacy and security statements to include statements informing them that they are subject to monitoring, recoding and auditing. Mechanisms and procedures shall be employed to monitor all IT systems and enclaves and to react to unauthorized activity.

2.7.2.3 Auditing

Auditing shall be in place to ensure that each person who accesses a system is accountable for their actions. Audit records shall be sufficiently detailed to reconstruct events that lead to a security violation, malfunction or other adverse event, and determine its cause and scope. These records must be protected and reviewed as appropriate for the level of concern for the system.

2.7.2.4 Security Violations, Incidents and Response

All incidents shall be documented, reported and responded to in order to mitigate any potential vulnerability and to respond to malicious acts.

2.7.3 Physical Security

Physical security controls appropriate for the levels of sensitivity and criticality shall be used to protect all IT-related assets including: hardware, software, communication lines, IT system output and facilities housing IT assets. All personnel shall have the appropriate need-to-know and clearances in order to be granted physical access to any IT assets.

2.7.3.1 Environmental Protection

Environmental controls including humidity, temperature and lighting shall protect personnel and equipment based on the operational needs of the site. Fire detection and suppression equipment shall be installed that meets the operational needs of the site.

2.7.3.2 Critical Utilities and Supplies

Critical supplies, including hardware, software and firmware, and utilities shall be protected to ensure an adequate level of operation based on the level of concern. This could include such things as maintenance or spare parts, uninterrupted power supplies and arrangements for alternative communication lines.

2.7.3.3 Physical Access to IT Assets

Computing facilities and systems shall be protected physically to restrict access to individuals with the appropriate clearance and need-to-know.

2.7.3.4 Marking and Labeling

All information, data storage devices and hardware that stores, processes, transmits or displays data in any form or format that is not approved for public release shall comply with DON and DoD policy and guidance for marking and labeling.[9]

2.7.4 Security Documentation and Testing

Security documentation shall be developed and protected based on the level of concern for the information contained in the documentation. Security testing shall be carried out to ensure that IT systems and infrastructure components are appropriately configured and are being used according to policy.

2.7.4.1 System Security Authorization Agreement

A System Security Authorization Agreement (SSAA) shall be prepared or developed and maintained for all MSC IT systems and enclaves describing the technical, administrative, and procedural IA program and policies that govern the system or enclave, and identifies its IA personnel and specific IA requirements and objectives, e.g., requirements for data handling or dissemination, system redundancy and backup or emergency response.

2.7.4.2 Other Security Documentation

Other security documentation shall be created, managed and protected based on DoD, DON and MSC needs and requirements.

2.7.4.3 *S*ecurity Testing

MSC shall regularly and systematically assess the IA posture of critical utilities, information systems, enclaves and supporting infrastructures through combinations of self-assessments, independent assessments and audits, formal testing and certification activities, system and network vulnerability or penetration testing and IA program reviews. A comprehensive set of procedures shall be implemented that tests all patches, upgrades, configuration changes and new DoD information systems prior to deployment or operation.

[9] DoD Regulation 5200.1-R, SECNAVINST 5510.36, DON IS Program Regulation, March 17, 1999.

2.7.5 Miscellaneous Provisions

The following IA policies pertain to daily operations that all MSC enclaves will encounter and may, if not addressed properly, introduce vulnerabilities into MSC.

2.7.5.1 Personal Electronic Devices

Personal electronic devices shall be prohibited without the authorized approval of the DAA. If approved, PEDs shall be operated securely within the limits of DAA approval.

2.7.5.2 Non-Governmental IT Assets

The use of non-governmental owned IT assets is prohibited without the authorized approval of the ISSM.

2.7.5.3 Web Servers

Web servers shall be configured to comply with DoD, DON and MSC guidance. Information shall be reviewed before being placed on web servers.

2.7.5.4 Remote Access

Remote access shall be appropriately encouraged, in accordance with national, DoD and DON guidance on telework, but in all cases it shall managed to ensure the session confidentiality.[10]

2.7.5.5 Mobile Code

In accordance with established MSC, DON and DoD procedures, mobile code shall be restricted based on its potential to cause damage if used maliciously. A mobile code registration and approval process to prevent the use of unacceptable mobile code within the IT system or enclave shall be implemented.

2.7.5.6 Virus Protection

All servers, workstations and mobile computing devices shall implement virus protection that includes a capability for automatic updates, content checking for e-mail with attachments and to check data arriving by FTP and HTTP. Virus detection signatures shall be updated at least weekly.

[10] DoD Telework Policy.

2.7.5.7 Acceptable Use

Access to the Internet and e-mail systems shall be for official use and authorized purposes only. Use shall be with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

2.8 Program and Budget

A discrete line item for IA shall be established in programming and budget documentation. All IA investments within MSC shall be continuously aligned to the mission and business needs identified through the enterprise IA architecture, and coordinated across related acquisition programs and operational domains. IA shall be traced as a programmatic entity by MSC and visibility extended into MSC's budget execution. Strategic IA goals and annual IA objectives shall be established in accordance with the Information Management Strategic Plan and funding and progress toward those objectives shall be tracked, reported and validated.

Military Sealift Command Information Assurance Implementation

Enclosure (2)

TABLE OF CONTENTS

Section One

Introduction

The following, the MSC IA Implementation, is intended to further define the MSC IA policies from enclosure (1). It provides guidance for particular controls for the implementation of policy and relates particular roles with specific responsibilities under each policy. Supplemental guidance may replace or further refine specific provisions with the issuance of other MSC notices or instructions.

In Section One, responsibilities are generally defined for IA roles in MSC. In Section Two, controls are given for the implementation of IA policies in all IT systems and enclaves, including the particular roles and their responsibilities for each policy. These are the minimum controls that shall be applied for all MSC systems and enclaves. This section tracks by the number the policies from enclosure (1). In Section Three, additional guidance is given for classified systems. All classified systems must meet the controls in Sections Two and Three. When there is a conflict between the controls in the two sections, the stricter control shall be applied.

Most terms used in this document are based on the definitions in NSTISSI 4009. Terms that are not defined in NSTISSI 4009 are defined in Section Four. In electronic versions of this document, when possible, referenced documents will be linked to copies of the actual reference. Section Five is a list of abbreviations and acronyms.

1.0 IA ROLES AND RESPONSIBILITIES

The roles and responsibilities for IA are defined generally here. Specific responsibilities for each role will be indicated at the end of each policy in Sections Two and Three of this enclosure.

1.2 Commander, Military Sealift Command

COMSC has the ultimate responsibility for IA for all MSC IT systems and enclaves and for delegating the DAA duties in writing to an individual at an appropriate level in the organization.

1.3 Designated Approving Authority

The DAA is the primary decision-maker for IA matters in the MSC and is responsible for ensuring that all IT systems are certified and accredited in accordance with the DITSCAP, DoD Instruction 5200.40.[11] Additionally, the DAA is responsible for determining whether to grant MSC IT systems and enclaves approval to operate based on implementation of acceptable IA controls, either through accreditation or the CAP.[12] The DAA is responsible for ensuring that IA requirements are included throughout the life cycle of IT assets, and for appointing the IAPM and the ISSMs. The DAA is also responsible for keeping the COMSC apprised of the status of the IA program on a regular basis.

1.4 Information Assurance Program Manager

The IAPM is responsible for developing, implementing and managing the IA program and the IA organization; this includes staffing, directing, funding and executing. The IAPM reviews and decides whether to approve new acquisitions and improvements of IA assets. The IAPM is responsible for maintaining this instruction and supporting the DAA, as required, with regard to MSC security incidents and compliance with IA policies. The IAPM is the point of contact for IA matters and represents MSC's IA interests to agencies and organizations external to MSC. The IAPM may also serve in the capacity of an ISSM.

[11] DoD Instruction 5200.40, DITSCAP, December 30, 1997.

[12] Memorandum 5230, MSC CAP, July 22, 2002.

1.5 Information Systems Security Managers

ISSMs are responsible for all activities related to IA and ensure that all necessary tasks and functions are performed for the systems and enclaves operating under their authority. They execute the IA program, under the guidance of the IAPM, to ensure compliance with all relevant policies. They ensure that all tasks are performed as required for certification and accreditation and for maintaining the security baseline. They develop and present IA training and develop and distribute IA awareness material and bulletins. They track compliance with IA awareness and training. ISSMs are also responsible for appointing and overseeing as many ISSOs, NSOs and System and Network Administrators, as needed. For additional information, see the ISSM Guidebook.[13]

1.6 Information Systems Security Officer/Network Security Officer

ISSOs and NSOs, under the direction of the ISSM, are responsible for ensuring that all IA controls are appropriately implemented and are working properly to meet the IA requirements of the systems or networks under their purview. They are responsible for ensuring that risk assessments are performed. They ensure IA auditing and monitoring are performed and analyzed. They ensure that users comply with the IA program's requirements and procedures and act as the primary contact for users. For additional information, see the ISSO Guidebook.[14]

1.7 Systems Administrators/Network Administrator

System Administrators and Network Administrators, under the direction of the ISSM, are responsible for ensuring that all components of IT systems or networks under their purview are operating effectively and securely in accordance with the System Security Authorization Agreement (SSAA) and MSC, DON and DoD policies and procedures. This includes configuration and management of systems and accounts, auditing and monitoring and system testing. They must be trained and certified in accordance with applicable requirements.

1.8 Facility Security Managers

Facility Security Managers are responsible for ensuring the physical security of IT facilities and IT assets under their purview. They coordinate IA-relevant facility issues with the appropriate ISSM/ISSO and assist with the IA program, as appropriate.

[13] NAVSO P-5239-04, ISSM Guidebook, September 1995.

[14] NAVSO P-5239-07, ISSO Guidebook, February 1996.

1.9 Managers and Supervisors

Managers and supervisors are responsible for ensuring that appropriate IA safeguards are used to adequately protect MSC data and IT assets under their purview. They ensure that they and their employees have the appropriate clearance and need to know in order to access IT systems and are aware of and observe all IA policies and procedures. They ensure that proposed acquisitions of hardware, software, communications, applications and equipment satisfy IA requirements and offer the best return on investment. Managers and supervisors shall seek accreditation or approval to operate from the DAA for all IT systems under their purview.

1.10 User

A User is anyone using IT assets, including all of the aforementioned roles. A User is responsible for complying with MSC, DON and DoD IA policies and procedures, accreditation instructions and a user agreement, if applicable. They must maintain a level of IA awareness commensurate with their job duties. They are responsible for protecting IT systems and information from improper disclosure and reporting any compromise or suspected compromise to the ISSO. They must access only that data, control information, software, hardware and firmware for which they are authorized and which is necessary to perform their duties.

Section Two

IA Policy

2.0 IA CONTROLS

a. MSC's IA strategy encompasses layered solutions that incorporate personnel, technical and operational controls in a defense-in-depth approach. These controls are derived from MSC IA requirements. To determine IA requirements for IT systems and enclaves, MSC shall use the ISSE process and the DITSCAP. The ISSE captures and refines information protection requirements and ensures their integration into IT acquisition processes and ongoing management through purposeful security design or configuration. MSC's IA policies utilize a baseline of IA controls of varying levels of robustness. Robustness is derived from level of concern for confidentiality, integrity and availability. The level of concern is determined by examining the Mission assurance category, data classification (sensitivity) and need-to-know. Therefore, it is MSC policy that all MSC IT systems implement IA controls that satisfy the level of concern (i.e., high, medium or basic) using corresponding criteria for high, medium or basic levels of robustness. Robustness describes the strength of an IA control and may also indicate a level of design assurance for a technical IA solution. Technical or non-technical (operational and personnel) controls may be used to achieve protection requirements dictated by the level of concern.

b. The DITSCAP captures ISSE requirements and other IA decisions. It is the management process for evaluating systems and providing a means for determining the amount of risk at which a system may operate.

c. The following controls shall be implemented by all MSC enclaves for all systems. Policies from which these controls are derived are to be found in enclosure (1).

2.1 General

As IT systems will vary greatly throughout MSC, it is important that as early as possible in the life cycle of IT-dependent programs, information owners establish the Mission assurance category, security classification, sensitivity level and need-to-know of information and IT systems. Information owners must also establish the permissible uses of information and systems and the associated mission or business rules of use, and ensure that the distinction between information that is operationally sensitive and information that can be made available to the public.

a. Action

(1) MSC enclaves shall implement IA controls, such as boundary defense, incident detection and response or PKI, based on the IA requirements they inherit from the IT systems they use. MSC enclaves shall assume the highest Mission assurance category and security classification of the IT systems used.

(2) MSC shall defend all systems and enclaves following all appropriate DoD, DON and MSC policies, guidance and instruction.[15] If there are conflicting requirements the most stringent shall be followed.

(3) All MSC IT systems and enclaves shall be assigned a Mission assurance category directly associated with the criticality and sensitivity of the information they contain relative to the achievement of MSC goals and objectives.

(4) Information systems shall employ ISSE in order to ensure that information protection is built into the overall system. As part of the ISSE, IT systems shall ensure interoperability with and maximum use of the common IA solutions provided by the hosting enclaves. Early in the system development life cycle, program managers shall inform enclave managers of system IA requirements, and enclave managers shall add any capabilities to the enclave necessary to support the system.

(5) Violations of these policies shall be subject to disciplinary action, including criminal prosecution and administrative sanction.

b. Roles and Responsibilities

(1) The DAA ensures that IA policies are defined for all IT assets.

(2) The IAPM interprets DoD and DON IA policy for implementation in MSC.

(3) The Enterprise ISSM ensures IA policy is uniformly implemented throughout the MSC.

(4) Site ISSMs ensure that IA policy is implemented for all IT assets under their purview.

[15] See, for example, SECNAVINST 5239.3, DON Information Security Program, July 14, 1995, OPNAVINST 5239.1B, DON IA Program, November 9, 1999, DoD Directive 8500.aa (Draft) as of 1 Feb 02, Instruction 8500.bb (Draft) as of 1 Feb 02, DoD Directive O-8530.1, Computer Network Defense, January 8, 2001. The Naval Office IA Publication series provide specific guidance and direction on the implementation of IA instruction for the Navy. The IA Publications are available at http://infosec.navy.mil

(5) The ISSOs/NSOs and System/Network Administrators are responsible for the implementation of IA on all IT systems in MSC.

(6) Managers and supervisors shall:

(a) Ensure that their employees are aware of and follow the policies and guidance in this instruction.

(b) Establish the permissible uses of information and systems from a functional security perspective along with the business rules of use, and ensure that there is distinction between information that is operationally sensitive and information that can be made available to the public.

(c) Assign a Mission assurance category based on the criticality and sensitivity of the information they contain for all IT systems and enclaves under their purview.

(7) Users are responsible for complying with all IA policies and procedures.

2.2 Risk Management

All MSC personnel shall perform risk management. Risk management shall be performed to identify threats and vulnerabilities, identify and apply mitigating countermeasures and review and test the effectiveness of the countermeasures throughout MSC, both within and between enclaves. The purpose is to reduce risk to an acceptable level using IA controls that are cost effective and conducive to MSC's mission. Risk management includes risk assessment, countermeasure selection, Security Test and Evaluation, contingency planning and system review. Risk assessments are performed to evaluate the threats, vulnerabilities and current safeguards related to the subject of the assessment. An ST&E must be performed on all IT systems or enclaves in order to gather sufficient technical information to support the DAA's decision whether or not to accredit or issue authority to operate.

a. Action

(1) Risk assessments shall be performed for all MSC IT systems and enclaves to evaluate all software, hardware, firmware and the environment in which they operate in accordance with the Risk Assessment Guidebook[16] or with another method approved by the ISSM or DAA.

[16] NAVSO P-5239-16, Risk Assessment Guidebook, September 1995.

(2) A risk assessment shall be performed on each system or enclave, at a minimum, every 3 years. In support of accreditation, risk assessments must be periodically reviewed and modified to accommodate the changing threats environment. Changes shall be reviewed to assess their affect on the accreditation status of the IT system.

(3) Risk shall be considered in all proposed configuration changes.

b. Roles and Responsibilities

(1) The DAA shall:

(a) Base accreditation decisions on the result of the risk management activities.

(b) Determine the acceptable level of risk for operating a system within MSC.

(c) Approve the risk assessment methodologies to be used.

(2) The IAPM shall:

(a) Ensure that risk management tasks are performed for all IT systems.

(b) Make recommendations to the DAA regarding accreditation based on the amount of residual risk on an IT system or enclave.

(3) ISSMs shall:

(a) Ensure that risk assessment is performed on all IT systems under their purview.

(b) Determine the risk assessment methodology to be used.

(c) Ensure that the assessment identifies the threats, vulnerabilities and controls.

(d) Review risk assessment to ensure methodology was properly followed, risk and risk levels were identified, countermeasures are appropriate and residual risk was identified.

(e) Ensure that the ST&E requirements to support an accreditation are satisfied.

(f) Keep current on potential threats and changes in technology and conditions that may have an impact on IA on systems or enclaves under their purview.

(g) Report to the IAPM any information that would significantly impact the IA posture of MSC systems.

(h) Review proposed configuration changes for risk.

(i) Ensure that any planned changes are assessed for their impact on security.

(4) ISSOs/NSOs shall:

(a) Perform risk assessments.

(b) Recommend countermeasures based on the level of risk and cost effectiveness.

(c) Review and modify risk assessments to accommodate changes to the system.

(d) Assist the ISSM in the planning and execution of the ST&E.

(e) Maintain a copy of the most recent ST&E.

(5) System/Network Administrators shall ensure that any changes to the IT systems are reviewed for their impact on risk.

(6) Users shall do all actions required to ensure that no additional risks are introduced into an MSC IT system or enclave.

2.3 Certification and Accreditation

All IT systems will be certified and accredited in accordance with DITSCAP.[17] Certification and accreditation is an ongoing process that must be continued throughout the life-cycle of the system or enclave. After accreditation, activities must be employed to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Certification and accreditation of MSC systems and enclaves must be supported by a risk assessment.

[17] DoD Instruction 5200.40 DITSCAP, December 30, 1997.

a. Action

(1) All systems and enclaves shall be accredited using the DITSCAP and in accordance with the baseline controls as determined by the ISSE.

(2) Certification of IT systems or enclaves shall be performed and documented by competent personnel in accordance with specified criteria, standards and guidelines.

(3) Certification must be supported by an ST&E. An ST&E test plan and procedures shall exist that requires testing, analysis, and documentation of the IT system or enclave as defined in the SSAA to confirm that they have no undesired effect(s) on the information being processed, that they perform as intended, and that the system or enclave is operating in accordance with the provisions and standards established in the SSAA.

(4) Accredited systems shall be monitored and employ security management, change management and periodic compliance validation to ensure that residual risk is kept at an acceptable level.

(5) The accreditation statement must identify the required confidentiality, integrity and availability services and constraints under which the system can operate including data sensitivity, user authorization, physical and system configuration.

(6) Once accredited, reaccredidation must be performed every 3 years or when any change is made that could affect the security posture of the system.

b. Roles and Responsibilities

(1) The DAA shall make a decision whether or not to accredit and reaccredit systems, or grant authority to operate based on the certification and accreditation documentation.

(2) The IAPM shall act as the certifying authority for all MSC IT assets, unless otherwise delegated to an ISSM.

(3) ISSMs shall:

(a) Ensure that the ST&E is executed appropriately.

(b) Ensure that all activities required to certify, accredit and reaccredit an IT system or enclave are executed.

(4) ISSOs/NSOs and System/Network Administrators shall provide support to the ISSMs and DAA throughout the certification and accreditation processes.

(5) Program Managers shall:

(a) Ensure that certification and accreditation are funded for their IT systems.

(b) Ensure that certification and accreditation are carried out on all IT systems under their purview and they shall not operate systems without prior approval to operate or prior accreditation.

2.4 Defense-In-Depth

MSC shall implement defense-in-depth for networks and infrastructure, enclave boundaries and computing environments.[18]

2.4.1 Networks and Infrastructure

MSC networks and infrastructure must be protected from attacks which could compromise the availability, confidentiality, or integrity of information and systems. To do this, all MSC enclaves shall employ controls to include network and communication security, and they shall follow the MSC Enterprise CAP.

2.4.1.1 Network Security

All MSC enclaves shall employ network security measures to protect networks and services from unauthorized modification, destruction, or disclosure. Network IA ensures that the network performs its critical functions correctly and there are no harmful side-effects.

a. Action

(1) Enclaves shall provide sufficient resources and redundancy to ensure that a single failure of a component or path will not result in isolation.

(2) MSC shall employ controls that safeguard its networks and the information transmitted over these networks and implement tools for automatically monitoring the integrity of the IT components and information.

[18] DON Chief Information Officer Information Technology Infrastructure Architecture (ITIA), DON CIO Information Technology Standards Guidance (ITSG).

(3) Network safeguards shall be configured securely according to DoD security technical implementation guides (STIGs) and security recommendation guides (SRGs) when available.[19]

(4) Interoperability and integration of IA solutions within or supporting MSC shall be achieved through adherence to an IA architecture that is consistent with DoD, Joint Chiefs of Staff and DON technical standards framework and a defense-in-depth approach.

b. Roles and Responsibilities

(1) The IAPM shall:

(a) Advocate funding for IA controls to adequately protect, preserve, and defend MSC networks and infrastructure.

(b) Ensure that the technical framework supports secure interoperability within and between MSC enclaves and external organizations.

(c) Review IA controls to ensure that they adequately address MSC IA requirements.

(2) ISSMs shall:

(a) Validate that network and infrastructure components and host IT systems are appropriately configured according to DoD STIGs and SRGs.

(b) Ensure that enclaves conform to the approved technical framework.

(c) Oversee interoperability testing.

(d) Ensure compliance with Information Assurance Vulnerability Alert (IAVA) and VCTS.

(e) Ensure that all systems and network components are covered by a standard operating procedure.

(3) ISSOs/NSOs shall:

(a) Monitor to ensure that the networks and components are appropriately configured in accordance with STIGs and SRGs.

[19] NAVSO P-5239-13, Vol. II, NSA SRGs.

(b) Perform interoperability testing.

(4) System/Network Administrators shall:

(a) Implement and configure controls to ensure the safety of networks and infrastructure.

(b) Assist the ISSOs/NSOs with the interoperability testing, as necessary.

(c) Implement IAVAs.

(d) Ensure systems are included in VCTS.

(5) Users shall follow Acceptable Use policy as described in Section 2.7.5.7.

2.4.1.2 Communications Security

Communications Security (COMSEC) techniques shall be applied to the extent necessary to deny information to unauthorized personnel and to effectively defend against interception, traffic analysis and imitative deception. Secure identification and authentication methods shall be used to protect the communication session.

a. Action

(1) Sensitive-but-unclassified (SBU) data must be protected in transmission by an approved technique[20] unless a waiver is granted under procedures established by the IAPM. NSA-approved techniques that may be used separately, or in various combinations, to protect the transmission of SBU include the following.

(a) Encryption: Encryption is the preferred technique for protecting transmitted SBU data.[21]

(b) Unencrypted Cable Circuits: Although encryption is preferred, unencrypted cable circuits of copper or fiber optics may be used. The degree of protection depends on the type of cable used. Unencrypted cable circuits can be employed to transmit SBU information if the cables are used only within the geographic boundaries of the United States or, if overseas, within areas totally under U.S. control, and if adequate measures are implemented such that circuits are maintained on cable and not converted to unencrypted radio transmission.

[20] NIST FIPS PUB 140-2, Security Requirements For Cryptographic Modules, October 10, 2001.

[21] Cryptographic Module Validation Program

(c) Protected Services: Commercial telecommunications companies offer services that are endorsed to protect the transmission of SBU information.

(2) All file transfers and e-mail shall be scanned for classified spillage and used consistently with policies herein. Integrity checking mechanisms, such as parity checks, cyclical redundancy checks and covert channel mechanism checks, shall be implemented for incoming and outgoing files.

(3) Voice over IP traffic (VoIP) to and from individually configured workstation IP telephony clients is prohibited within MSC networks. Both inbound and outbound individually configured VoIP traffic shall be blocked at the enclave perimeter.

(4) Implementation of specific non-repudiation capabilities such as digital signatures must exist if mission accomplishment requires non-repudiation. NIST FIPS validated cryptography shall be used for encryption, key exchange, digital signature and hash.[22]

(5) All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided.

b. Roles and Responsibilities

(1) The DAA shall:

(a) Ensure that COMSEC policies are enforced.

(b) Review and decide whether or not to approve waiver requests for use of non-NSA-approved techniques for protecting SBU data in transmission.

(2) The IAPM shall:

(a) Ensure that COMSEC security policies are developed and implemented.

(b) Develop procedures for evaluating and approving requests for waivers from using NSA approved techniques for protecting transmitted SBU information.

(c) Advise the DAA on whether or not to approve waiver request for use of non-NSA-approved techniques for protecting SBU data in transmission.

[22] NIST FIPS PUB 140-2, Security Requirements For Cryptographic Modules, October 10, 2001

(3) ISSMs shall:

(a) Review systems and enclaves to ensure appropriate COMSEC controls are utilized.

(b) Be responsible for identifying auditable events that may be used for exploiting known covert storage channels and documenting the bandwidths of known covert storage channels which are not detectable by auditing, and reporting this information to the IAPM.

(c) Be responsible for submitting waiver requests to the IAPM, as necessary.

(4) ISSOs/NSOs shall:

(a) Monitor systems and networks to ensure that COMSEC controls are in place.

(b) Ensure that transmitted files and e-mails are scanned and have been checked for integrity.

(5) System/Network Administrators shall configure systems and network components to implement COMSEC controls.

(6) Program Managers shall ensure that their systems make use of and are interoperable with COMSEC controls.

(7) Users shall use their digital certificates or other mechanisms for non-repudiation for systems requiring non-repudiation.

2.4.1.3 Connection Approval Process

MSC enclaves or other external organizations or systems shall be compliant with the MSC Enterprise CAP in order to connect to the MSC network.[23]

a. Action

(1) All interconnections and connections to external systems of MSC IT systems shall undergo the MSC CAP to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.

[23] Memorandum 5230, MSC CAP, July 22, 2002.

(2) Connection approvals shall be granted for an appropriate period of time according to the MSC CAP.

b. Roles and Responsibilities

(1) The DAA shall review the connection request and make a determination whether to approve the request or require additional information or changes be made.

(2) ISSMs shall:

(a) Collect initial IA information (any current supporting documentation).

(b) Complete information requirements.

(c) Ensure supporting documentation is current.

(d) Submit Connection Request to DAA.

(e) Correct any deficiencies in accordance with MSC DAA explanation, if applicable.

(f) Review approved connections every three years to ensure they continue to meet the CAP requirements.

(3) The ISSOs/NSOs shall support the Site ISSM in the CAP, as required.

2.4.2 Enclave Boundary Controls

Strong boundary defenses such as traffic filtering and control and intrusion detection to protect against network attacks shall be employed by all MSC enclaves.

a. Action

(1) For all IT systems that do not process sensitive or classified information, boundary defense mechanisms, including firewalls and network Intrusion Detection System (IDS), shall be deployed at the enclave boundary to the Wide Area Network (WAN). Internet access shall be permitted only from a Demilitarized Zone (DMZ) that is isolated from other MSC systems by physical or technical means.

(2) For all IT systems that process sensitive information, boundary defense mechanisms, including firewalls and network IDS, shall be deployed and configured appropriately at the enclave boundary to the WAN, and at layered or internal enclave boundaries as required.[24] All Internet access shall be proxied through Internet access points.

(3) Each MSC regional area command or field activity shall install and maintain a network IDS and designate a network administrator and a configuration manager. The IDS must be outside any local firewalls at the enclave perimeter so that it can detect all malicious activity. IDS shall be monitored.

(4) Boundary safeguards shall be configured as securely as possible based on operational needs. This includes blocking all services, ports, and protocols that are not required, auditing traffic, securing perimeter devices (e.g., routers, switches, guards) both physically and logically.

(5) MSC virtual private networks (VPN) shall be configured to comply with the SPAWAR Minimum Protection Profile and other DoD, DON and MSC policies and standards.[25]

(6) Domain Name System (DNS) shall be operated and managed securely. All MSC locations with DNS servers shall have a split DNS service. The external DNS server must reside on the bastion host or on another host in the DMZ. It must not include any information about anything within the protected enclave. It can show information about machines in the DMZ that people outside the enclave must access. The external DNS server must deny recursive queries. Internal DNS servers process DNS queries that come from inside the enclave. The internal functions of the authoritative DNS server for local zones must be on a different system from the caching recursive server for remote DNS zones. Any internal server that accepts recursive queries must limit recursive access to authorized network clients.

(7) All e-mail and other transmitted data shall be scanned to prevent classified spillage.

b. Roles and Responsibilities

(1) ISSMs shall:

[24] NAVSO P-5239-13, Vol. II, May 2000 (DRAFT), App. B, ITSG, Navy-Marine Corps NIPRNet Enclave Protection Policy, November 30, 2001.

[25] SPAWAR Technical Memorandum, “VPN devices and applications used in the US Navy unclassified networks” February 2, 2000.

(a) Ensure that any security violations and incidents are pursued appropriately.

(b) Review the enclave boundary policies and procedures to ensure that they meet current standards for protecting the enclave.

(c) Review boundary controls to ensure they are appropriately implemented.

(2) ISSOs/NSOs shall:

(a) Ensure that e-mail is scanned for classified spillage and shall report any violations to the ISSM.

(b) Monitor boundary safeguards and network devices to ensure that they are configured to provide the appropriate level of security.

(3) System/Network Administrators shall:

(a) Implement and configure enclave boundary safeguards according to the security classification and Mission assurance category of the system or enclave.

(b) Review and monitor IDS logs and report findings to the ISSM in accordance with incident response procedures.

(c) Ensure that filters used for email, http and ftp scanning remain current.

(d) Configure and manage VPNs and DNS according to current policy and standards.

(4) Users shall comply with all e-mail procedures to prevent classified spillage.

2.4.3 Computing Environments

MSC shall use controls to secure access, safeguard the confidentiality and integrity of data, protect system software, securely configure and manage the computing environment and defend against subversive acts of trusted people and systems, both internal and external.

a. Action

(1) All systems shall be compliant with pertinent SRGs or STIGs and the latest DoD, DON and USTRANSCOM IA requirements.[26]

(2) All enclaves and systems shall be configured in accordance with MSC DoD and DON Information Operations Condition (INFOCON), Force Protection Condition (FPCON) guidance.

(3) All enclaves and systems shall comply with the latest IAVAs and shall track this compliance.

(4) All software used on MSC IT systems must be approved prior to installation and operation. MSC IT systems must include an identified set of executable software that is authorized for that system. Such software must be protected from unauthorized modification to the maximum extent possible by the hardware and software mechanisms of the system.

(5) Software shall be used in accordance with all copyright laws.[27] Freeware, shareware or privately owned software shall not be used unless approved by the ISSM.

(6) Systems shall be configured to remain in a secure state. IT systems shall be tested periodically to ensure the integrity of the system state. Recovery procedures and technical system features shall be developed and enforced to ensure that recovery is done in a secure and verifiable manner. Circumstances that can cause a non-secure recovery shall be documented and appropriate mitigating procedures shall be put in place.

(7) No information, including encrypted representations of information, produced by a prior subject's action shall be available to any subject that obtains access to an object that has been released back to the system.

(8) Host-based IDS must be deployed for major applications, to include network management assets such as routers, switches and DNS for all systems that process Mission assurance category I and II information.

(9) When data at rest is encrypted, it shall only be encrypted using encryption algorithms approved by the DON.[28]

[26] NAVSO P-5239-13, Vol. II, NSA SRGs, Information Systems Security Handbook for Program Mangers, USTC, March 2002.

[27] United States Code 17, section 504 and 506, and United States Code 18-2319

[28] ITSG.

b. Roles and Responsibilities

(1) The IAPM shall:

(a) Track IAVA compliance.

(b) Report IAVA compliance to DON, USTRANSCOM and others as required.

(c) Ensure that MSC implements INFOCON and FPCON procedures.

(d) Ensure that IT systems are continuously reviewed and monitored for incorporating improved IA practices.

(e) Develop and implement a process for software development change control.

(2) ISSMs shall:

(a) Monitor systems and enclaves to ensure that they are using appropriate IA controls, including complying with the current INFOCON and FPCON.

(b) Ensure that systems are appropriately configured according to the STIGs and SRGs to meet all IA requirements.

(c) Shall approve all software prior to installation on any system.

(d) Monitor IAVA compliance and submit compliance information to the IAPM.

(3) ISSOs/NSOs shall:

(a) Limit and review application programmer privileges based on the criticality of the systems.

(b) Ensure that IDS systems are configured and monitored on major applications.

(4) System/Network Administrators shall:

(a) Ensure that IT networks and systems are configured in compliance with pertinent STIGs and SRGs to comply with all IA policies and procedures, including current FPCON and INFOCON status and IAVAs.

(b) Not install software before receiving IA guidance or approval from the ISSM.

(c) Implement and appropriately configure IA controls to ensure the security of the computing environment.

(d) Configure and test systems to ensure that they remain in a secure state at all times.

(e) Configure systems that require encryption for data at rest to use DON approved encryption techniques.

(5) Users shall:

(a) Abide by the controls in the computing environment.

(b) Abide by the Acceptable Use Policy.

(c) Report any security incidents to the ISSM or IAPM as required.

2.5 Key Management

The key management infrastructure (KMI) provides a common unified process for the secure creation, distribution and management of the cryptographic products such as public keys and traditional symmetric keys that enable security services for the network, enclave and computing environment. MSC shall implement a KMI based on DoD, DON and MSC PKI policies and procedures. [29]

a. Action

(1) The use of PKI certificates and biometrics for positive access control shall be in accordance with published DoD and DON policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible.

(2) Where interoperable PKI is required for the exchange of unclassified information with its vendors and contractors, MSC shall only accept PKI certificates obtained from a DoD-approved External Certificate Authority, or other approved mechanisms in accordance with DoD PKI policy.

[29] Public Key Infrastructure Roadmap, October 17, 2001, ITSG, X.509 Certificate Policy for the United States Department of Defense, Version. 5.2, November 13, 2000, DEPSECDEF Memorandum, subject: DoD PKI, August 12, 2000. Additional information can be found at the PKI Program Management Office Website.

(3) For IT systems processing Mission assurance category III information, symmetric keys shall be produced, controlled and distributed using NIST-approved key management technology and processes.[30] For systems processing Mission assurance category I and II information, symmetric keys shall be produced, controlled and distributed using NSA approved key management technology and processes.[31] Asymmetric Keys shall be produced, controlled and distributed using DoD PKI Class 4 Certificates and hardware security tokens that protect the user's private key. For systems processing classified information, symmetric and asymmetric keys shall be produced, controlled and distributed using NSA-approved key management technology and processes.

(4) For Mission assurance category III systems, identification and authentication shall be accomplished using the DoD PKI Class 3 token or a commercial Secure Socket Layer application when possible. For Mission assurance category I and II systems, identification and authentication shall be accomplished using the DoD PKI Class 4 token or an NSA-certified product when possible.[32]

b. Roles and Responsibilities

(1) The IAPM shall ensure that PKI is appropriately implemented according to DoD and DON policies in new acquisitions and upgrades, wherever possible.

(2) ISSMs shall monitor and review systems to ensure that they are complaint with PKI policies and procedures.

(3) System/Network Administrators shall configure systems to implement PKI systems controls.

(4) Program Managers shall acquire PKI enabled IA assets when possible.

(5) Users shall abide by all PKI controls.

(6) PKI roles (e.g., Local Registration Authority and Trusted Agents) and their responsibilities are detailed in the MSC PKI Roadmap.[33]

[30] FIPS Pub. 140-2, October 10, 2001.

[31] Trusted Product Evaluation Program.

[32] Trusted Product Evaluation Program

[33] Public Key Infrastructure Roadmap, October 17, 2001

2.6 Life Cycle Management

Information assurance processes shall be implemented throughout the life-cycle of all IT systems from development, acquisition, use, modification, maintenance, through disposition.

2.6.1 Acquisition

IA shall be identified and included in the design, acquisition, installation, operation, upgrade or replacement of all IT systems.[34] Acquisition or outsourcing of IA services such as incident monitoring, analysis and response, operation of IA services shall be supported by a formal risk analysis.

a. Action

(1) Priority shall be given to products evaluated by either the International Common Criteria/NIAP Evaluation and Validation Program, or the FIPS validation program.[35] If an approved U.S. Government protection profile exists for a particular product type and no validated products exist, acquisition documentation must contain requirements for evaluation and validation of the product to the approved protection profile. If no U.S. Government protection profile exists for a particular product type, then acquisition documentation will require vendors to provide a security target that describes the security attributes of their product and have that product evaluated or under contract to be evaluated by a NIAP-certified laboratory.

(2) The acquisition of all COTS/GOTS IA and IA-enabled IT products shall be evaluated for compliance with national and DoD policies.[36]

(3) Outsourcing of dedicated IA services is discouraged. It must be supported by a formal risk analysis and must explicitly address government, service provider and MSC end user IA roles and responsibilities prior to approval.

b. Roles and Responsibilities

(1) The DAA shall determine whether or not to approve outsourcing of IA services.

[34] See, e.g., NSTISSP No. 11, National Information Assurance Acquisition Policy, January 2000, Public Law 106-398, Title X, Subtitle G, Government Information Security Reform Act (GISRA), October 30, 2000, and Title 48, CFR Federal Acquisitions Regulations.

[35] International Common Criteria/NIAP Evaluation and Validation Program, NIST validation program.

[36] NSTISSIP No. 11.

(2) The IAPM shall:

(a) In accordance with NIAP, approve only those products and services which have been evaluated by the NSA, or in accordance with NSA-approved processes.

(b) Make a recommendation to the DAA with regard to outsourcing of IA services.

(c) Conduct a risk analysis for all outsourced IA services.

(3) ISSMs shall:

(a) Monitor IT acquisition for security impact to ensure compliance with IA regulations and requirements.

(b) Ensure that any proposed acquisition meets IA requirements.

(4) Program Managers shall:

(a) Include IA in procurement requests.

(b) Route procurement requests to the IAPM for review.

2.6.2 Configuration Management

Configuration management (CM) practices shall be followed to ensure that changes to any IT system or enclave do not diminish the security posture of any portion of MSC.[37] The CM practices shall implement a full range of processes to insure that changes are identified, tested, approved and audited appropriately.

a. Action

(1) All changes to MSC hardware and software shall be reviewed according MSC policy.

(2) Automatic monitoring shall be used to confirm that system and enclave hardware and software inventories and configurations are compliant with approved settings.

[37] See, the MSC Configuration Management Web Site.

(3) Testing of configuration changes shall not be performed in a live environment unless authorized by the DAA.

(4) All software shall have current licenses.

(5) A current and comprehensive baseline inventory of all software and hardware along with documented configuration required to support operations shall be maintained and protected. On-line libraries of software and hardware inventories are encouraged.

(6) System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.

(7) A backup copy of the hardware and software inventory shall be stored in a fire-rated container or otherwise not collocated with the original.

b. Roles and Responsibilities

(1) The DAA shall:

(a) Develop policies and procedures for controlling changes to IT systems and enclaves.

(b) Determine whether or not to approve CM changes based on the results of security testing.

(2) The IAPM shall:

(a) Promulgate and manage the CM process.

(b) Review and determine whether or not to approve the system library procedures.

(3) ISSMs shall:

(a) Provide input to CM activities to ensure that implemented changes do not compromise the security of the system or enclave.

(b) Review the status reports and determine what actions need to be taken, if any, to maintain an appropriate security posture.

(c) Review testing of changes to ensure comply with IA requirements.

(d) Develop and promulgate the system library procedures to ensure that system libraries are managed and maintained appropriately.

(4) ISSOs/NSOs shall:

(a) Assist the ISSM in providing input to, or actively participating in, CM activities to ensure that implemented changes do not compromise the security of IT systems or enclaves.

(b) Test systems to ensure that they conform to approved configurations.

(c) Monitor systems to ensure that all changes to systems are made according to the policy.

(d) Monitor the system and review the baseline to ensure that software and hardware components have not changed, been relocated or otherwise been tampered with in any way that may alter IA posture.

(e) Provide a status report, highlighting changes, to the ISSM that summarizes the nature (estimated IA impact, if any) of changes along with a copy of the inventory list.

(f) Perform security testing of proposed changes.

(g) Maintain secure backup copies of hardware and software inventories.

(h) Update library when changes are made.

(i) Review software licenses to ensure that they are current.

(5) Facilities Security Managers shall be responsible for ensuring the safety of the hardware and software inventories.

(6) System/Network Administrators shall:

(a) Ensure that all changes are approved through the CM process.

(b) Develop the baseline inventory of software and hardware.

(c) Assist in the performance of security testing for proposed changes.

(d) Follow system library procedures as directed by the ISSOs/NSOs.

(7) Program Managers shall ensure that changes to configurations to all IT systems under their purview go through the appropriate CM process.

(8) Users shall abide by all system library management controls.

2.6.3 Continuity of Operations

All MSC enclaves shall employ procedures and technical IT system measures to ensure continuity of operations. Data backups shall be scheduled, performed, stored, protected and tested according to the criticality of the data. A contingency plan shall be developed for every mission essential IT system within MSC. The details of contingency plans may vary depending on the criticality of the IT system. A disaster recovery plan, appropriate to the level of criticality, shall be created, maintained and tested.

2.6.3.1 Identification of Critical Functions

Critical functions for the continued operation of essential systems shall be identified. These functions may change over time and shall be reevaluated in order to make sure that the most critical systems are addressed for continued operation.

a. Action

(1) Mission and business critical functions shall be identified for priority restoration planning for all IT systems.

(2) For Mission assurance category I and II systems, all assets supporting critical functions shall be identified.

(3) Critical functions shall be reevaluated annually.

b. Roles and Responsibilities

(1) The DAA shall determine whether or not to approve the selection and prioritization of critical functions.

(2) The IAPM shall review the selection and prioritization of critical functions.

(3) ISSMs shall:

(a) Ensure that critical functions and systems are identified and included in the contingency plan.

(b) Review the plans yearly to make sure they reflect the current status of the IT systems.

(4) ISSOs/NSOs shall assist the ISSMs in the selection, prioritization and yearly review of critical systems.

(5) Program Managers shall participate in the prioritization of critical functions.

2.6.3.2 Contingency and Disaster Recovery Plans

A contingency plan is a plan of action designed to reduce to an acceptable level the consequences of any loss of IT resources or capabilities. The purpose of a contingency plan is to mitigate the damaging consequences of unexpected and undesirable events of any magnitude, not just major catastrophes. While plans must include the possibility of catastrophically destructive occurrences, they must also account for less-than-cataclysmic events, which also seriously impede data processing functions. Disaster recovery plans provide for the ability to recover from a disaster in order to return to the normal operation of the organization. Enclaves shall prepare a disaster recovery plan for all mission critical IT systems. Contingency plans and disaster recovery plans are living documents that shall reflect the realities of change in the workplace. This requires that the plans are reviewed and tested regularly.

a. Action

(1) A contingency plan shall be created for every mission essential IT system.

(2) A contingency plan shall include actions that must be taken; if normal use of the operating environment is impaired or disrupted; if an application or user is denied information or service; and if the information system suddenly has to expand its capacity to accommodate a national emergency or some other critical event.

(3) A disaster recovery plan shall provide for the resumption of full operations within 5 days of an event resulting in the cessation or degradation of full operations for Mission assurance category III IT systems.

(4) A disaster recovery plan shall provide for the resumption of full operations within 24 hours of an event resulting in the cessation or degradation of full operations for Mission assurance category II IT systems.

(5) A disaster recovery plan shall provide for the smooth transfer of all operations to an alternate site for the duration of an event with little or no loss of operational continuity for Mission assurance category I IT systems.

(6) Contingency and disaster recovery plans shall be tested annually for systems processing Mission assurance category II and III information.

(7) Contingency and disaster recovery plans or significant portions thereof shall be tested semi-annually for systems processing Mission assurance category I information.

b. Roles and Responsibilities

(1) The DAA shall:

(a) Make the final determination, based on the analysis performed by IAPM or the ISSM, whether a system requires a contingency plan.

(b) Determine whether or not to approve contingency plans.

(c) Determine whether or not to approve the disaster recovery plans.

(d) Review the test results and recommendations and decide whether or not to reaffirm approval of the plans.

(2) The IAPM shall review the contingency and disaster recovery test results and recommend corrective measures.

(3) ISSMs shall:

(a) Assess all IT systems under their purview to recommend to the DAA if a contingency plan is required.

(b) Prepare, document and evaluate contingency plans for all mission essential IT systems.

(c) Prepare, document and evaluate disaster recovery plans.

(d) Review and test all contingency plans on a schedule commensurate with the Mission assurance category of the system.

(e) Maintain a copy of the most current disaster recovery and contingency plans for the systems/enclaves under their purview.

(4) ISSOs/NSOs shall assist the ISSMs in the preparation, documentation, testing and evaluating of disaster recovery plans and contingency plans.

(5) Program Managers shall maintain contingency and disaster recovery plans for IT systems under their purview.

(6) System/Network Administrators and Users shall know their roles in carrying out the plans.

2.6.3.3 Alternate Site Designation

Contingency plans shall identify an alternate site for operations and the site shall be prepared based on the criticality of the systems. Boundary defenses at alternate sites shall provide no less than the level of security at the primary site.

a. Action

(1) An alternate site shall be identified that will permit the resumption of partial operations for systems processing Mission assurance category III information and will permit the resumption of full operations for systems processing Mission assurance category I and II information.

(2) Enclave boundary defense at the alternate site shall provide IA measures equivalent to the primary site for systems processing Mission assurance category II and III information and IA measures configured identically to that of the primary site for systems processing Mission assurance category I information.

b. Roles and Responsibilities

(1) The DAA shall review and determine whether to approve the alternate site designations based on the site's ability to carry out the mission of the organization while maintaining an adequate level of security.

(2) The IAPM shall review the alternate site to ensure that it meets IA requirements.

(3) ISSMs shall:

(a) Identify an alternate site for operation.

(b) Ensure that it is readied to the appropriate level for the Mission assurance category of the system.

(4) ISSOs/NSOs shall assist the ISSM in readying the alternate site.

(5) Facility Security Managers shall evaluate the alternate facilities to ensure that the physical IA controls meet the same IA requirements as at the primary site.

2.6.3.4 Backups

Backups shall be performed and maintained in a manner that ensures systems can be restored to a level of operation commensurate with the criticality of the system.

a. Action

(1) Data backup shall be performed as follows:

(a) At least weekly for systems processing Mission assurance category III information.

(b) Daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its Mission assurance category and/or classification for systems processing Mission assurance category II information.

(c) By maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation for systems processing Mission assurance category I information.

(2) Complete restoration of information from backup media shall be tested at least annually for systems processing Mission assurance category III information.

(3) Complete restoration of information from backup media shall be tested at least semi-annually for systems processing Mission assurance category II information.

(4) Complete restoration of information from backup media shall be tested at least quarterly for systems processing Mission assurance category I information.

(5) Backups shall be stored and securely protected in a manner and for retention periods commensurate with the type of information on the backup.[38]

(6) Backup solutions must be technically compatible with the computing environments that they support. Media used for storage should be serviced and must be verified by testing to be effective.

[38] Attention should be given to insure that Federal, operational, legal and business continuity requirements are met. For example, archives of patient records may be required to be stored for years while incremental, "daily" backups may only be required for weeks. Responsibility rests with the Program Managers to ensure that the backups for their systems are appropriate to satisfy other (non-IA) requirements sources.

b. Roles and Responsibilities

(1) The IAPM shall determine retention requirements.

(2) ISSMs shall monitor to ensure that the backup policies are being met.

(3) ISSOs/NSOs shall:

(a) Monitor to ensure that backups are performed appropriately.

(b) Ensure that the backups are effective (i.e., compatible with the current computing environment).

(4) Facilities Security Managers shall ensure that backups are stored securely and according to policy.

(5) System/Network Administrators shall be responsible for performing backups and ensuring that the backups are appropriately tested and stored.

(6) Users shall be responsible for backing up their own data files.

2.6.4 Maintenance

Maintenance helps to ensure that systems operate to support MSC. Consequently, maintenance support shall be available to ensure the operation of systems commensurate with the criticality of the enclave. All persons who access a system to perform maintenance shall have the clearance and need to know to access the highest level of information on the system or shall be monitored by someone with technical expertise to detect unauthorized system modifications.

a. Action

(1) Maintenance support shall be available to respond within 24 hours of failure for systems processing Mission assurance category III information.

(2) Maintenance support shall be available to respond 24 X 7 immediately upon failure for systems processing Mission assurance category I and II.

(3) Maintenance personnel shall be authorized, controlled and monitored appropriately for the level of security required and the Mission assurance category of the system and enclave.

(4) Remote maintenance shall only be performed with approval of the DAA.

b. Roles and Responsibilities

(1) The DAA shall determine whether or not to approve remote maintenance for IT systems, if requested.

(2) The IAPM shall develop procedures for ensuring that maintenance is performed securely and timely.

(3) ISSMs shall:

(a) Document and maintain on file the processes for determining authorization and the list of authorized maintenance personnel.

(b) Determine the level of detail required in the maintenance log.

(c) Ensure maintenance support is available on a schedule commensurate with the Mission assurance category of the system.

(d) Make a request to the DAA if remote maintenance authority is desired.

(4) Facilities Security Managers shall develop escort procedures for maintenance personnel.

(5) Program Managers shall initiate, allocate funds and manage maintenance contracts.

(6) System/Network Administrators shall:

(a) Supervise the activities of maintenance personnel, as appropriate.

(b) Review the actions of maintenance people, as appropriate.

(c) Not perform remote maintenance unless approved.

2.6.5 Disposal and Data Remanence

Documents, equipment and machine-readable media shall be cleaned or disposed of appropriately to ensure that data is released to only those who are authorized.

a. Action

(1) All documents, equipment and machine-readable media containing sensitive or classified data shall be cleared and sanitized before being released outside of classified controls or before being released for use at a lower level of classification. Clearing media by erasing the data or overwriting it in one pass is sufficient when the media does not leave the facility in which it is located.

(2) Documents, machine-readable media and equipment shall be destroyed in compliance with DoD and DON policies and procedures.[39]

(3) Objects shall be purged of all information before being released back to the system.

b. Roles and Responsibilities

(1) The IAPM shall:

(a) Periodically issue detailed instructions for disposing of documents, equipment and machine-readable media.

(b) Approve software programs and equipment used for clearing and purging data storage media.

(c) Approve procedures for removal of external markings from data storage media.

(2) ISSMs shall:

(a) Maintain plans for clearing, purging, destroying, removing external markings and disposing of computer data storage media.

(b) Provide adequate information on data remanence for users, operations personnel and other security personnel to make sound decisions concerning risks, requirements and procedures.

[39] DoD Regulation 5200.1-R, "DoD Information Security Program," January 1997, NAVSO P-5239-26, "Remanence Security Guidebook", September 1993.

(c) After ensuring that classified information has been properly purged, determine whether or not to approve removal of external markings from computer data storage media.

(3) ISSOs/NSOs shall:

(a) Ensure that users are properly disposing of all media.

(b) Maintain proper control of equipment and information.

(4) Facilities Security Managers shall ensure that all procedures for the disposition of equipment and media are carried out.

(5) System/Network Administrators shall:

(a) Ensure that users have the technical capability and resources to dispose of the media.

(b) Configure systems to ensure that data remanence is appropriately controlled.

(6) Users shall dispose of media according the IAPM's instructions.

2.7 IA Infrastructure

IA is maintained through a combination of personnel, IT, administrative and physical means that are validated through testing and are fully documented.

2.7.1 Personnel IA Controls

Personnel IA controls shall be used to ensure that only trained and authorized individuals with appropriate clearance and need-to-know will have access to systems and data.

2.7.1.1 Clearance and Need-to-know

Individuals requiring access to sensitive or classified information or IT systems shall be processed for access authorization in accordance with DoD personnel security policies. Only individuals who have a valid need-to-know that is demonstrated by assigned official government duties and who satisfy all personnel security criteria shall be granted access.

a. Action

(1) Individuals requiring access to sensitive or classified information shall be processed for access authorization in accordance with DoD and DON personnel IA policies.[40]

(2) Access to systems and information by foreign nationals shall be controlled according to DoD and DON policy.[41]

(3) Only individuals who have a valid need-to-know, demonstrated by assigned official government duties, and who satisfy all personnel IA criteria (e.g., IT position sensitivity background investigation requirements)[42] may be granted access to information with special protection measures or restricted distribution as established by the information owner.

b. Roles and Responsibilities

(1) ISSM shall ensure the ISSOs perform periodic audits of users clearance and need to know.

(2) ISSOs/NSOs shall periodically audit to ensure users have the correct access.

(3) Program Managers shall:

(a) Ensure that users have been correctly processed for access authorization and termination.

(b) Ensure that users access is based on appropriate clearance and need-to-know.

(4) Users shall only access information for which they have clearance and need-to-know.

[40] DoD 5200.2-R, DoD Personnel Security Program, January 1987, SECNAVINST 5510.30a, DON Personnel Security Program, March 10, 1999, SECNAVINST 5510.36, DON IS Program Regulation, March 17, 1999.

[41] DoD 5230.20, Visits, Assignments, Exchanges of Foreign Nationals, August 12, 1998, DoD 5230.25, Withholding of Unclassified Technical Data from Public Release, November 6, 1984, SECNAVINST 5510.31C, Policy and Procedures for Control of Foreign Disclosure in the DON, December 31, 1992.

[42] DoD 5200.2R, DoD Personnel Security Program, January 1987.

2.7.1.2 IA Training and Awareness

Upon new hire and at least annually thereafter, all MSC IT system users shall receive training and familiarization to perform their assigned IA responsibilities. General and specialized training shall also be provided. Training shall be tracked for all users.

a. Action

(1) General IA Training: All users (MSC employees, civilian and government; and MSC contractors) who manage, design, develop, maintain or operate MSC IT systems shall undergo IA training and awareness on assignment and at least annually thereafter. The MSC IA Awareness and Training Program consists of the following:

(a) IA training and awareness briefings shall include the following:

- Threats, vulnerabilities, and risks associated with the system. IA objectives (i.e., What needs to be protected?)
- Responsibilities and accountability associated with system security.
- Information accessibility, handling and storage considerations.
- Physical and environmental considerations, which are necessary to protect the system.
- System data and access controls.
- All IA related plans such as Incident Response, Configuration Management and Continuity of Operations or Disaster Recovery.
- Authorized system configuration and associated CM requirements.
- Notification and reporting requirements and structure for security violations.
- Consequences of non-compliance with IA policies and procedures.

(b) IA refresher or annual training and awareness may include various combinations of the following:

- Self-paced or formal instruction.
- IA education bulletins.
- IA posters, training films and tapes.
- Computer-aided instruction.

(2) Specialized training: All specialized training shall also include the topics identified for General IA Training. This will eliminate the need for these personnel to attend two IA training sessions.

(a) System and Network Administrators: All MSC system and network administrators must receive training and achieve certification in accordance with current DON policies.

(b) ISSM/ISSOs: IA training for the ISSM/ISSOs shall provide a comprehensive background in computer security and cover IA policies and procedures in such related areas as Information, Physical, Personnel, Software/Hardware, Administrative and Communication security and contingency planning.

b. Roles and Responsibility

(1) The IAPM shall:

(a) Publish and maintain policy guidelines on IA awareness and training.

(b) Assign responsibility for implementing the IA awareness and training program.

(c) Brief the DAA and CO on IA issues routinely so they remain aware of the current status of IA.

(d) Review and approve training for ISSM.

(2) The Enterprise ISSM shall:

(a) Attend the DON ISSM Course or equivalent subject to IAPM approval.[43]

(b) Prepare policy on IA awareness and training.

(c) Track IA training for all personnel.

(3) Site ISSMs shall:

(a) Attend the DON ISSM Course or equivalent subject to IAPM approval.

(b) Develop and present IA training courses and briefings.

(c) Develop and distribute awareness material and bulletins.

[43] DON ISSM Course

(d) Ensure all personnel receive the appropriate IA training associated with their jobs and maintain records of training received and report compliance to the Enterprise ISSM.

(4) ISSOs/NSOs shall:

(a) Be responsible to ensure that training is implemented for all employees.

(b) Attend specialized training as approved by the IAPM.

(5) Managers or supervisors shall ensure their personnel receive the appropriate training.

(6) System/Network Administrators shall be trained and certified in accordance with DON policy.

(7) Users shall attend IA awareness and training sessions.

2.7.2 Administrative Security

Administrative controls provide a layer of protection that primarily addresses the accountability of the users by such measures as limiting access, monitoring and auditing use of the system. Where technical controls are infeasible or cost prohibitive, administrative controls may be used to achieve equivalent IA objectives but only after review by the ISSM and approval by the DAA.

2.7.2.1 Logical Access

Logical access controls shall be implemented to restrict access so that only authorized users based on classification and need-to-know can gain access to data, workstations, applications and networks. This shall include such things as a comprehensive account management process, encryption, policies on foreign nationals and non-repudiation capabilities.

a. <u>Action</u>

(1) System or network access shall only be gained through the presentation of an individual identifier such as a unique user ID and password. Passwords must be case sensitive 8-14 character mix of upper case letters, lower case letters, numbers and special characters, including at least one of each (e.g. Passwd2!). Passwords must expire when they are 90 days old but must not be able to be changed until they are 3 days old. Users must not be able to use any of their 25 most recent passwords. Deployed systems with limited data input capabilities shall implement these measures to the extent possible.

(2) Account management shall use the following controls.

(a) Accounts must be created with the minimum set of rights and permissions necessary to perform basic job functions with authorized system resources. IDs and passwords are only issued to authorized users after receiving a valid request. Accounts shall not be shared nor shall accounts be reused by renaming or editing its properties. Accounts for services or proxies must be unique to the service or proxy.

(b) Whether for a new or existing account, passwords shall be set to expire immediately, so that the system prompts the user to change the password upon initial logon.

(c) Inactive user IDs shall be retained in the system for 2 years.

(d) Users must be informed of the requirements for creating and protecting their password.

(e) All privileged user accounts shall be established and administered in accordance with a role-based access scheme that organizes privileges into roles.

(f) Group authenticators may be used only in conjunction with an individual authenticator. Their use must be kept to a minimum and must be explicitly approved by the DAA. In most cases, rights and permissions shall be assigned to groups, and individual user accounts shall be assigned to one or more of the groups.

(3) To prevent unauthorized access and unauthorized modification or destruction of data, file and object permissions shall be set to only allow the creator or owner of a file to modify it and only authorized personnel, such as system administrators, can take ownership of files or other objects.

(4) Use of privileged accounts shall be limited to privileged functions; that is, privileged users shall use non-privileged accounts for all non-privileged functions.

(5) A plan for assigning permissions to carry out separation of duties and least privilege principles shall be documented and enforced through access control procedures.

(6) Individual foreign nationals representing a foreign nation, coalition or international organization shall be authorized access to specific MSC networks or systems containing classified or sensitive information only when mechanisms are in place to strictly limit access to information that has been cleared for release to the entity the foreign national represents in accordance with DoD and DON policy.[44]

[44] DoD 5230.20, DoD 5230.25, SECNAVINST 5510.31C.

(7) Controls to identify authorized users who are contractors, DoD direct or indirect hire foreign nationals employees, or other foreign nationals shall be subject to DoD requirements as promulgated by DON to preclude unauthorized disclosure of classified or sensitive information.

b. Roles and Responsibilities

(1) ISSMs shall:

(a) Ensure that users understand the requirements for the use and protection of passwords.

(b) Develop a plan for implementing separation of duties and least privilege.

(c) Monitor to ensure that foreign nationals are only allowed access to appropriate IT systems and follow DON and DoD procedures.

(2) ISSOs/NSOs shall:

(a) Determine the rights and permissions to be assigned to the various roles.

(b) Monitor access controls to ensure they are implemented correctly.

(3) System/Network Administrators shall:

(a) Create and manage user accounts according to specifications.

(b) Plan for and implement controls that limit access to those users that have authorization, and enforce the principles of separation of duties, least privilege, and need to know.

(c) Implement controls to provide accountability for any changes made to data or other objects.

(d) Disable user accounts when notified that the user no longer needs access.

(e) Only provide access to foreign nationals after they have been adequately cleared and if the system is configured appropriately to protect information.

(4) Managers and supervisors shall:

(a) Submit new user account requests.

(b) Validate that users have the appropriate privileges and access.

(c) Notify System/Network Administrator and ISSO/NSO when a user no longer requires access.

(5) Users shall:

(a) Protect their account information from unauthorized disclosure.

(b) Use privileged access only to carry out privileged functions.

(c) Only access and use systems and information for which they are authorized.

2.7.2.2 Session Controls

Session controls shall be employed to restrict access based on inactivity and multiple logon attempts. Session controls shall be used to inform users about account activity. All users shall be warned that they are entering a government information system, and are provided with the appropriate privacy and security statements to include statements informing them that they are subject to monitoring, recoding and auditing.

Mechanisms and procedures shall be employed to monitor all IT systems and enclaves for unauthorized activity; to detect, report, and document the integrity of the enclave or system and any unauthorized activity such as attempted or realized penetrations of those systems and networks; and to institute appropriate countermeasures or corrective actions. Such activities shall be in accordance with DoD guidance.[45]

a. Action

(1) Systems processing sensitive and classified information shall detect an interval of inactivity and block further access until the user reestablishes the connection using the proper validation.

(2) Access shall be denied after three unsuccessful logon attempts and System Administer interaction shall be required for reactivation.

(3) For IT systems processing sensitive or classified information, if the system allows for multiple logon sessions for each user ID, the system shall provide a capability to control the number of logon sessions.

[45] DoD O-8530-2.

(4) When users attempt to access MSC IT systems, the system shall display the legally approved warning banner prior to successful logon, informing the user that by using the system, they consent to being monitored. Proceeding beyond the warning banner requires a keyboard action that signifies acceptance of the terms of access. The warning banner must appear the first time a user accesses the system, the network, as well as local and remote resources.

(5) An automated, continuous on-line monitoring and audit trail creation capability shall be deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and to automatically disable the system if serious IA violations are detected.

(6) Session controls shall also be used, contingent on system capability, to inform users upon successful logon, of the date and time of the user's last logon, the location of the last logon and the number of unsuccessful logon attempts using this user ID since the last successful logon.

b. Roles and Responsibilities

(1) The Enterprise ISSM shall ensure that new IA products have the capacity to enforce session controls.

(2) ISSMs shall monitor and review session controls to ensure that they are implemented appropriately.

(3) ISSOs/NSOs shall be responsible for investigating inconsistencies in the logon history and if it is determined that an IA incident has taken place they must follow approved procedures.

(4) System/Network Administrators shall:

(a) Configure systems to limit sessions and provide accountability for all sessions.

(b) Configure system to timeout after fifteen minutes of inactivity and to lockout account after three failed logon attempts.

(c) Configure the system to monitor and react to IA violations as appropriate.

(d) Configure the warning banner message.

(e) Reactivate accounts as needed.

(5) Users shall limit sessions and notify the ISSO of any inconsistencies in the logon history notification.

2.7.2.3 Auditing

Auditing shall be in place to ensure that each person who accesses a system is accountable for their actions. Audit records shall be sufficiently detailed to reconstruct events that lead to a security violation, malfunction or other adverse event, and determine its cause and scope. These records must be protected and reviewed as appropriate for the level of concern for the system. The level of auditing, the frequency of review, and the level of protection for the audit logs must be based on the sensitivity of the data.

a. <u>Action</u>

(1) Logs and audit trails shall be reviewed at least weekly, but preferably once a day, for indications of inappropriate or unusual activity. Suspected violations of IA policies shall trigger an alert be analyzed and reported in accordance with enclave IA procedures.

(2) Audit records must include at least the following:

(a) User ID.

(b) Identity of device that accessed the system.

(c) Date and time of event.

(d) Number of successful and failed attempts.

(e) Type of event.

(3) At a minimum, an audit record shall be made of the following types of events:

(a) Use of identification and authentication mechanisms.

(b) Introduction of objects into a user's address space (e.g., file open, program initiation).

(c) Deletion of objects.

(d) Actions taken by computer operators and system administrators and/or system security officers.

(e) Other security relevant events.

(4) All IT systems will provide for monthly reports of all security violations, including incorrect passwords and off-hour activity. The Administrator may alter content and frequency of these reports as deemed necessary for proper audit and control.

(5) Audit records must be retained on a write-once/read-many device, such as a CD-R, or on a write-only device, such as a printer for at least six months and for at least 1 year for sensitive, classified, or Mission assurance category I or II information.

(6) The contents of audit trails must be protected against unauthorized access, modification or deletion. For systems processing Mission assurance category I or II information, or classified information access, changes to the data shall be recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.

b. Roles and Responsibilities

(1) ISSMs shall:

(a) Ensure that the IT system transactions are effectively audited and that the audit trails are reviewed by the ISSOs/NSOs.

(b) Investigate suspected or confirmed violations and pursue according to policy.

(c) Review the recommendations of the ISSOs from the audit reviews.

(d) Periodically review the audit trails.

(2) ISSOs/NSOs shall:

(a) Review audit logs and audit trail data to identify and analyze security-related weaknesses and report suspected or confirmed violations to the ISSM.

(b) Ensure that controls are in place to protect audit data.

(c) Ensure that security alarms are in place and functioning properly.

(d) Report to the ISSM on the effectiveness of security procedures, based on the audit analysis, and recommend improvements.

(3) Program Managers shall ensure that the audit records are securely retained for the appropriate length of time based on the sensitivity level of the information audited.

(4) System/Network Administrators shall configure the system to audit the correct attributes and react to system and user activity based on the level of security required for the information on the system.

(5) Users shall assist in any investigation of suspected or confirmed security violations.

2.7.2.4 Security Violations, Incidents and Response

MSC shall adhere to an incident response plan that defines reportable security incidents, outlines a standard operating procedure for incident response, provides for user training and establishes an incident response team.

a. Action

(1) Security violations and incidents shall be subject to disciplinary action up to and including administrative separation and criminal prosecution. Security violations and incidents shall include, but are not limited to, loss of hardware/software/documentation, unauthorized access, unauthorized utilization of IT assets or services, exceeding authority, disruption, misuse, espionage, hoaxes and malicious code attacks.

(2) An incident response plan that defines reportable security violations and incidents, outlines a standard operating procedure for response, provides for user training and establishes a response team shall be enforced.[46]

(3) The incident response plan shall be tested at least annually for Mission assurance category II and III systems, and at least every 6 months for Mission assurance category I systems.

b. Roles and Responsibilities

(1) The IAPM shall:

(a) Prepare an incident response plan.

[46] NAVSO P-5239-19, Incident Response Guidebook, August 1996.

(b) Communicate with external organizations when required by the specifics of the incident.

(c) Assess reported incidents and if it is determined that they are globally significant develop a response and distribute it to all ISSMs.

(2) The Enterprise ISSM shall:

(a) Maintain records of all security violations and incidents.

(b) Report globally significant incidents to the IAPM for MSC-wide collection and dissemination.

(3) Site ISSMs shall:

(a) Investigate potential or real security violations and incidents.

(b) Report incidents to the Enterprise ISSM.

(4) ISSOs/NSOs shall ensure that all security incidents or violations are investigated, documented and reported to the ISSM.

(5) System/Network Administrators shall ensure that systems and networks are configured to identify security violations and incidents according to policy.

(6) Users shall:

(a) Be trained on the appropriate use of the IT system, what constitutes a security violation or incident, and investigation of security and incident reporting procedures.

(b) Assist in incident response, as appropriate.

(c) Report all suspected or real incidents to ISSOs/NSOs.

2.7.3 Physical Security

MSC shall protect personnel, equipment, facilities, and information. MSC shall implement controls to secure these assets from physical threats, intentional or otherwise. Physical security considers environmental protections, physical access to computing facilities, critical utilities and labeling of data.

a. Action

(1) Comprehensive physical security controls shall be developed and enforced.[47]

(2) Devices that display or output classified or sensitive information in human-readable form shall be positioned to deter unauthorized individuals from reading the information.

(3) Procedures to ensure the proper handling and storage of information shall be implemented, such as end of the day security checks, unannounced security checks and, where appropriate, the imposition of a 2-person rule within the computing facility.

(4) Systems with SBU information on non-removable media shall be in a locked office or building during non-duty hours, or they must be secured in some way to prevent loss or damage.

(5) Documents and equipment shall be stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD policy.[48]

b. Roles and Responsibilities

(1) The IAPM shall review and determine whether to approve the physical security procedures for IT assets and computing facilities.

(2) ISSMs shall:

(a) Coordinate with the Facilities Security Manager to ensure that physical security procedures support the IA Program.

(b) Review the annual physical security threat assessment to determine if IA controls are adequate.

(3) Facilities Security Managers shall develop and enforce physical security procedures.

(4) ISSOs/NSOs shall ensure that proper information handling and storage procedures are developed and enforced.

(5) Users shall ensure that all IT assets are used and stored securely.

[47] OPNAVINST 5530-14C, DON Physical Security, December 10, 1998.

[48] DoD Regulation 5200.1-R.

2.7.3.1 Environmental Protection

Environmental controls including humidity, temperature, and lighting shall protect personnel and equipment based on the operational needs of the site. Fire detection and suppression equipment shall be installed that meets the operational needs of the site.

a. Action

(1) An automatic emergency lighting system shall be installed that covers emergency exits and evacuation routes for Mission assurance category III systems, and all areas necessary to maintain full operations for Mission assurance category I and II systems.

(2) Battery-operated or electric stand-alone smoke detectors shall be installed in IT facilities for Mission assurance category III systems; the fire department receives an automatic notification of any activation of the smoke detection or fire suppression system for Mission assurance category I and II systems.

(3) Handheld fire extinguishers or fixed fire hoses shall be available should an alarm be sounded or a fire be detected for Mission assurance category III systems, and a fully automatic fire suppression system shall be installed that automatically activates when it detects heat, smoke or particles for Mission assurance category I and II systems.

(4) Humidity controls shall be installed that provide an alarm of fluctuations potentially harmful to personnel or equipment operation; adjustments to humidifier/de-humidifier systems may be made manually for Mission assurance category I systems and an automatic humidity control shall be installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation for Mission assurance category II and III systems.

(5) A master power switch or emergency cut-off switch to IT equipment shall be present. It shall be located near the main entrance of the IT area and it shall be labeled and/or protected by a cover to prevent accidental shut-off.

(6) Temperature controls shall be installed that provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected; adjustments to heating or cooling systems may be made manually for Mission assurance category III systems and automatic temperature controls must be installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation for Mission assurance category I and II systems.

(7) Automatic voltage control shall be implemented for critical IT assets.

(8) Users shall be trained on the use of environmental controls.

b. Roles and Responsibilities

(1) The IAPM shall review and determine whether to approve the environmental controls for computing facilities.

(2) ISSMs shall coordinate with the Facilities Security Manager to ensure that the environmental controls support the IA Program.

(3) Facilities Security Managers shall ensure that environmental controls are in place to provide for operational continuity commensurate with the Mission assurance category of the system.

(4) Managers and supervisors shall ensure that employees receive initial and periodic training in the operation of environmental controls.

(5) Users shall be responsible for ensuring that they appropriately operate the environmental controls to maintain an acceptable level of security.

2.7.3.2 Critical Utilities and Supplies

Critical supplies, including hardware, software and firmware, and utilities shall be protected to ensure an adequate level of operation based on the level of concern. This could include such things as maintenance or spare parts, uninterrupted power supplies and arrangements for alternative communication lines.

a. Action

(1) Arrangements shall be in place for alternate long haul communications services capable of restoring in accordance with DoD and DON policies and procedures:

(a) Partial operations within 72 hours for Mission assurance category III systems.

(b) Full operations within 24 hours for Mission assurance category II systems.

(c) Full operations without loss of operational continuity for Mission assurance category I systems.

(2) Electrical power shall be able to be restored by manually activated power generators upon loss of power from the normal source for Mission assurance category III systems.

(3) An uninterrupted power supply (UPS) shall be installed:

(a) On emergency generators capable of restoring sufficient power to continue partial operations for Mission assurance category II systems.

(b) On generators, or there is an alternate power supply source capable of continuing full operations for Mission assurance category I systems.

(4) Arrangements for restoration of critical utilities to include alternate long haul communications services must be tested annually for Mission assurance category III systems, semi-annually for Mission assurance category II systems and quarterly for Mission assurance category I systems.

b. Roles and Responsibilities

(1) ISSMs shall:

(a) Coordinate with the Facilities Security and Utilities Manager to ensure that the procedures for maintaining critical supplies and utilities support the IA Program.

(b) Ensure that arrangements are in place for alternate long haul communication services as appropriate for the Mission assurance category.

(c) Ensure that arrangements for restoring critical utilities are tested as appropriate for the Mission assurance category.

(2) ISSOs/NSOs shall:

(a) Monitor to ensure that critical supplies and utilities are protected or there is a sufficient redundancy.

(b) Test restoration plans according to Mission assurance category.

(3) Facilities Security and Utilities Managers shall:

(a) Maintain critical supplies and utilities to ensure operational continuity commensurate with the Mission assurance category of the system.

(b) Ensure the UPS are installed and that electricity can be restored according to the Mission assurance category of the system.

(4) System/Network Administrators shall configure and maintain controls for ensuring the continued operation or availability of critical utilities and supplies.

(5) Users shall be responsible for ensuring that they act appropriately to maintain the use and availability of critical utilities and supplies.

2.7.3.3 Physical Access to or of IT Assets

Physical access controls shall be used to deter unauthorized entry into facilities and the critical areas that support or affect IT operations. Particular attention shall be paid to the physical security of IT systems that are not continuously operated or attended. Areas that house essential networked components (routers, firewalls, servers, switches, etc.) must be designated, and function as restricted areas accessible to administrative personnel only. The same applies to local area network (LAN) and telecommunications wiring closets. Such areas should be included in a physical security plan.

a. Action

(1) Every physical access point to facilities housing IT assets critical to enclave operations shall be guarded or alarmed 24 X 7.

(a) For Mission assurance category III facilities, two forms of identification are required to gain access to the facility. Internal access restrictions are not required.

(b) For Mission assurance category II facilities, all access points are observed 24 X 7, and intrusion alarms are centrally monitored. Two forms of identification are required to gain access to the facility. Internal access restrictions are not required.

(c) For Mission assurance category I facilities, all access points are observed 24 X 7, and intrusion alarms are centrally monitored. Two forms of identification are required to gain access to the facility. Internal access is restricted based on need-to-know and is enforced by a third form of identification.

(2) Buildings that house equipment shall have the structural integrity to provide effective physical security at a reasonable cost.

(3) Workstations shall be protected by setting the screen saver to activate after no more than 15 minutes of inactivity, by requiring a password to unlock the screen and keyboard, and by personnel locking or logging off the workstations when leaving their work areas.

(4) Visitor procedures shall include a detailed log and supervision of all visitors shall be escorted, or otherwise under surveillance at all times.

(5) All Non-MSC personnel shall wear a separate and distinguishable badge that differentiates them from MSC employees.

(6) Any government information or equipment taken off government property shall be protected according to the level of sensitivity of the information or equipment.

b. Roles and Responsibilities

(1) The IAPM shall review and determine whether to approve the procedure for ensuring that access to IT assets is limited.

(2) ISSMs shall coordinate with the Facilities Security Manager in developing the physical security policies.

(3) Facility Security Managers shall:

(a) Be responsible for ensuring that physical access to IT assets is limited according to policy.

(b) Institute a visitor log and review the log to ensure that the appropriate persons are being allowed access.

(c) Coordinate with the ISSM in developing the physical security policies.

(4) System/Network Administrators shall configure workstations with an automatic password protected screen saver.

(5) Users shall:

(a) Protect IT assets both within and outside of government property, this includes following procedures for locking or logging off their workstations.

(b) Wear badges in plain view at all times while on MSC property and shall remove them when in public.

(c) Challenge anyone who is not wearing a badge while on MSC property.

(d) Invoke the screensaver or log off the machine when it is not in use or when the user steps away from their desk.

2.7.3.4 Marking and Labeling

All information, human readable output, media, data storage devices and hardware that stores, processes, transmits or displays data in any form or format that is not approved for public release shall be clearly labeled with the classification and sensitivity level and any other dissemination, handling or distribution instructions to prevent unauthorized access. For further guidance contact the ISSM or consult appropriate DoD and DON policy. [49]

a. Action

(1) All information, human readable output, media, data storage devices, printers, monitors and other hardware that stores, processes, transmits or displays data in any form shall be labeled according to the highest classification that can be stored, processed, transmitted or displayed.

(2) Removable media shall be marked as classified if they have ever been used on a classified system or if the status of their write-protect feature could not be determined while in use on any system, classified or unclassified.

(3) If it is difficult to mark non-removable media or hardware itself, the label shall be affixed in a readily visible position on the cabinet that encloses the media or hardware.

(4) Information, media, data storage devices and other hardware introduced into a classified environment shall be treated as classified until appropriate inspection determines otherwise.

b. Roles and Responsibilities

(1) ISSMs shall:

(a) Monitor to ensure that labeling is appropriately performed for all media and equipment, in accordance with this policy.

(b) Provide guidance to users in the marking and labeling of information, media, data storage devices and hardware, as appropriate.

(2) ISSOs/NSOs shall label storage devices, printers, monitors and other hardware according to the appropriate classification.

(3) Facility Security Managers shall make classification labels available to users.

[49] DoD Regulation 5200.1-R, SECNAVINST 5510.36, DON IS Program Regulation, March 17, 1999.

(4) The System/Network Administrator shall assist in labeling any IT assets for which they are responsible.

(5) Users shall mark all media they handle.

2.7.4 Security Documentation and Testing

Security documentation shall be developed and protected based on the level of concern for the information contained in the documentation. Security Testing shall be carried out to ensure that IT systems and infrastructure components are appropriately configured and are being used according to policy.

2.7.4.1 System Security Authorization Agreement

All systems and enclaves shall be documented with an SSAA. The SSAA will contain IA relevant information and consequently can be very sensitive, requiring a high level of protection.

a. Action

(1) SSAAs shall require additional protection if they contain risk assessments or residual risk statements that identify specific vulnerabilities associated with a system or application, that are not considered to be public, widely known vulnerabilities. The entire SSAA must be classified, or the classified information must be removed and placed in separate classified document, such as a classified appendix.

(2) Any additional documents that pertain to an IT system, such as certification letters, appointment letters, host site IA requirements, TEMPEST survey letters, shall be included in the accreditation documentation file.

b. Roles and Responsibilities

(1) The DAA shall review SSAAs and determine whether they are sufficient to support accreditation.

(2) The IAPM shall maintain a library of SSAAs.

(3) ISSMs, or a person whom an ISSM delegates, shall prepare SSAAs.

(4) System/Network Administrators shall document, as part of the SSAAs, if operations prevent them from configuring systems to comply with IA policies.

(5) Program Managers shall work with the ISSM in preparing the SSAAs for systems under their purview.

(6) Users shall be familiar with contents of the SSAA.

2.7.4.2 Other Security Documents

Other security documents shall be created, managed, protected, and tested based on DoD, DON and MSC needs and requirements.

a. Action

(1) Authorized User Lists shall be created and maintained to document the identity of all users of MSC IT systems.

(2) Visitors Control Logs shall be created and maintained to document the identity of visitors to IT facilities.

(3) Each MSC IT system shall have a documented standard operating procedure (SOP), which covers all applicable IA practices and procedures.

(4) The SOP shall be given to every user of the system.

(5) Any exceptions to established DoD, DON or MSC policies, as well as exceptions to this instruction, shall be documented in a waiver request to the DAA.

(6) Documentation shall be included with IA software and hardware components.

(7) Documents required by other sections of this policy may require testing, e.g., Continuity Plans and Disaster Recovery Plans.

(8) All documentation shall be protected according to its level of sensitivity or classification level.

b. Roles and Responsibilities

(1) The DAA shall review and determine whether or not to approve SSAAs and waiver requests.

(2) The IAPM shall:

(a) Maintain a library of all approved waivers,

(b) Ensure that policies and procedures exist for the appropriate management and protection of security documentation.

(3) ISSMs shall:

(a) Maintain IA documents according to DON and DoD policy.[50]

(b) Ensure that documentation accompanies new IA software and hardware.

(c) Maintain a library of approved waivers for systems under their purview.

(4) ISSOs/NSOs shall:

(a) Develop and maintain Authorized User Lists.

(b) Develop SOPs for all systems that include IA concerns to be given to all users of the system.

(5) Facility Security Managers shall create and maintain the Visitor Control Log.

(6) System/Network Administrators shall review Authorized User Lists against audit of user IDs to ensure that only the users are gaining the appropriate access to systems.

(7) Program Managers shall:

(a) Request a waiver from the DAA for any exception to IA policies or procedures.

(b) Shall furnish IA documentation for all new IT system procurements.

(8) Users shall follow all SOPs.

2.7.4.3 Security Testing

The MSC IA program shall regularly and systematically assess the IA posture of information systems and enclaves, and MSC-wide services and supporting infrastructures through a combination of self-assessments, independent assessments and audits, formal

[50] NAVSO P-5239-13, Vol. II.

testing and certification activities, system and network vulnerability or penetration testing, and IA program reviews, in accordance with national, DoD, DON and MSC policies.[51] A comprehensive set of procedures shall be implemented that tests all patches, upgrades and new DoD information systems prior to deployment or operation.

a. Action

(1) Automated tools shall be periodically used to check the security configurations of IT systems to verify that they comply with SSAA and Accreditation statement as well as MSC, DoD and DON guidance.

(2) All MSC sites shall maintain on-line automated vulnerability assessment tools for each server, including servers that other organizations manage remotely. The sites must review their server configurations at least once a month to ensure that they comply with the appropriate security configuration policy, e.g., SRGs and STIGs.[52]

(3) An annual IA review shall be conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the IA goals.

(4) Penetration testing shall be performed for all MSC IT systems. This test shall include periodic, unannounced attempts to penetrate key computing facilities.

b. Roles and Responsibilities

(1) The DAA and the IAPM shall review penetration test results and annual IA reviews.

(2) ISSMs shall:

(a) Review and determine whether to approve testing schedules and procedures.

(b) Ensure that assessments are performed annually on all MSC systems and enclaves. These reviews may need to be independently validated based on the type of information or system.

[51] See, for example, Public Law 106-398, Title X, Subtitle G, Government Information Security Reform Act (GISRA), October 30, 2000.

[52] NSA Security Reference Guides.

(c) Review the penetration tests and send a summary report to the IAPM and DAA.

(d) Approve testing tools for use in testing.

(3) ISSOs/NSOs shall:

(a) Ensure that testing tools are available.

(b) Develop a comprehensive testing schedule and set of procedures for all systems and enclaves under their purview.

(c) Review test results and monitor testing for compliance with IA requirements.

(3) System/Network Administrators shall:

(a) Test changes to the system for their impact on IA.

(b) Perform penetration tests and send the results to the ISSO/ISSM for review and a summary of the results to the IAPM/DAA for review.

(c) Review server configurations for IA compliance with approved configuration.

(4) Program Manager shall ensure that upgrades and changes get IA testing before going live.

2.7.5 Miscellaneous Provisions

The following IA provisions pertain to daily operations that all MSC enclaves will encounter and may, if not addressed properly, introduce vulnerabilities into MSC.

2.7.5.1 Personal Electronic Devices

Personal electronic device's (PEDs) are almost ubiquitous tools with a size and functionality that make them both advantageous for the user but have the potential of introducing new risks into operating environments. PEDs shall be prohibited without the authorized approval of the DAA. If approved, PEDs shall be operated securely within the limits of DAA approval. PEDs shall be operated and maintained in accordance with current DoD and DON policy and guidance. PEDs include, but are not limited to, laptops, cell phones, handheld computers.

a. Action

(1) PEDs shall be prohibited from use unless specifically approved for use by the DAA.

(2) Accreditation for PEDs devices shall indicate where the device can be used and the types of information it can process and store.

b. Roles and Responsibilities

(1) The DAA shall accredit PEDs indicating where the device can be used and the types of information it can store and process.

(2) ISSMs shall prepare the SSAA for the PEDs taking into account where the devices can be used and what types of information can be contained on them.

(3) System/Network Administrators shall configure the PEDs to meet the requirements of the authorization to operate.

(4) Users shall:

(a) Secure mobile devices just as they secure other movable information assets.

(b) Operate PEDs according to the accreditation instructions and appropriate guidance. They shall have a copy of the accreditation letter in their possession when the device is not in their regular workspace.

2.7.5.2 Non-Governmental IT Assets

Non-governmentally-owned IT assets must only be brought into the workplace with prior approval from the ISSM. They must comply with all MSC IA requirements.

a. Action

(1) Owners shall be informed that MSC assumes no liability for the use, theft or physical damage of their hardware or software used in the workplace.

(2) Users of non-governmentally-owned computers will observe the same safeguards, such as virus control, as other MSC IT assets.

(3) The use of non-governmentally-owned IT hardware and/or software shall be restricted to a specific and temporary contingency at 90-day intervals not to exceed 180 days. Permission will be formally granted if the use of non-governmentally-owned IT assets is in the best interest of MSC. Requests will be addressed through the chain of command to the ISSM. MSC accepts no liability for the use of this equipment.

b. Roles and Responsibilities

(1) ISSMs shall:

(a) Review and determine whether or not to allow requests to use non-governmental IT assets for MSC work.

(b) Ensure that non-governmental IT assets comply with all IA requirements and that their use does not extend beyond the 180 day limit.

(c) Inform the owner of the non-governmental IT asset that MSC is not liable for any damage to the IT asset.

(2) Users shall:

(a) Not use non-governmental IT hardware or software for MSC work without the express authorization of the ISSM.

(b) Be responsible to make certain that any privately owned software used on an MSC system is a legal licensed copy.

2.7.5.3 Web Servers

Web servers shall be configured to comply with DoD, DON and MSC guidance.

a. Action

(1) All MSC web servers shall be configured to comply with the latest DoD, DON and MSC guidance.[53] If operational requirements prevent administrators from implementing all the derived requirements, they must obtain the necessary waivers.

(2) The information for all websites shall be considered not releasable by default, and without a specific approval for public release, must be managed to ensure that official MSC information remains in the control of the MSC whether the web site is MSC owned, operated or outsourced. Public release of information requires an IA and policy review in accordance with DoD and DON policy.[54]

(3) Annual risk assessments shall be performed on all MSC public web servers.

b. Roles and Responsibilities

(1) ISSMs shall:

(a) Ensure that any information on web sites for public release is reviewed appropriately.

(b) Perform annual risk assessments of public web servers.

(2) System/Network Administrators shall:

(a) Ensure that information on websites is protected in accordance with policy.

(b) Configure web servers to comply with the latest DoD, DON and MSC policy and guidance.

2.7.5.4 Remote Access

Remote access shall be appropriately encouraged, especially in accordance with national telecommunications and disabilities acts, but in all cases it shall managed to ensure the session confidentiality.

[53] ITSG, SECNAV R 211930Z, DON Worldwide Web Policy, October 1998.

[54] DoD Directive 5230.9, Clearance of DOD Information for Public Release, April 9, 1996, DoD Instruction 5230.29, Security and Policy Review of DOD Information for Public Release, May 6, 1996,.

a. Action

(1) MSC host IT systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and DMZs, or through systems that are isolated from all other systems through physical means. This includes remote access for telecommuting.

(2) Remote access to IT systems must always use encryption to protect the confidentiality of the session. The session level encryption shall equal or exceed the robustness required for the particular type of data transmitted. Authenticators are restricted to those that offer strong protection against spoofing.

(3) Information regarding remote access mechanisms (e.g., dial-up connection telephone numbers) shall be protected.

(4) Secured telephone devices used in non-secure environments shall comply with all applicable DoD, DON and MSC policies and procedures.[55]

(5) Remote management of systems shall only be allowed when controls are in place to assure accountability and security of all actions.

b. Roles and Responsibilities

(1) ISSMs shall monitor to ensure that remote access is using appropriate IA controls.

(2) ISSOs/NSOs shall ensure that secured telephone devices used in non-secure environments are installed, configured and maintained according to policy.

(3) System/Network Administrators shall configure systems to securely regulate access to the Internet and remote access.

(4) Users shall:

(a) Protect remote access information and mechanisms.

(b) Assume all liability in the event they choose to perform official functions on personally owned, off-site computer systems, such as virus infection to a home machine while checking e-mail remotely, in any case the non-governmentally owned equipment must meet all requirements in this document.

[55] CINCPACFLT, Pearl Harbor HI, 122126Z IA Advisory No. IAA-001-02, March 2002.

2.7.5.5 Mobile Code

In accordance with established MSC, DON and DoD procedures, deployment of mobile code shall be restricted based on its potential to cause damage. A mobile code registration and approval process to prevent the development or acquisition of unacceptable mobile code for deployment within the IT system or enclave shall be implemented.

a. Action

(1) All categories of mobile code shall be blocked, unless it comes from assured or trusted sources as determined by the ISSM.

(2) Because the risk is unknown, administrators must block all uncategorized mobile code by all available means at the enclave boundary, on workstations and on the application layer.

(3) In accordance with established DoD, DON and MSC procedures, mobile code shall be categorized, controlled and deployed based on its potential to cause damage if used maliciously.[56]

(4) A mobile code registration and approval process to prevent the development or acquisition of unacceptable mobile code for deployment within the IT system or enclave shall be implemented.

b. Roles and Responsibilities

(1) The IAPM shall update the mobile code policy as appropriate.

(2) ISSMs shall:

(a) Develop and implement a process for categorizing mobile code and controlling its use.

(b) Determine which sources are considered assured or trusted.

(c) Review systems to ensure that they are configured according to policy.

(3) ISSOs/NSOs shall review and monitor audit traffic to ensure systems are configured correctly and users are in compliance.

[56] DoD Memorandum, Policy Guidance for use of Mobile Code Technologies in DoD Information Systems, November 7, 2000.

(4) Program Managers shall submit requests to the ISSM for approval of mobile code used in their systems.

(5) System/Network Administrators shall configure systems to only allow permitted mobile code.

(6) Users shall only use approved mobile code types.

2.7.5.6 Virus Protection

All servers, workstations and mobile computing devices shall implement virus protection that includes a capability for automatic updates, content checking for email with attachments and to check data arriving by FTP and HTTP.

a. Action

(1) Virus detection signatures shall be updated at least weekly from one of the following two sources:

(a) The MSC Intranet web site: http://intranet.msc.navy.mil.

(b) The Navy IA web site: http://infosec.navy.mil.

(2) Before using storage media and files they shall be checked for viruses.

(3) System users shall be informed about virus protection procedures by memo, e-mail, signs at building entrances and other means.

(4) All virus incidents shall be reported to the ISSO.

(5) All virus incident reports must contain at least the following information:

(a) The date and time of the incident

(b) The name and title of the administrators making the report, with contact information

(c) The name of the affected user (if applicable)

(d) The name of other personnel who are involved (if any)

(e) The name, type and nature of the virus (if known)

(f) The method of detection

(g) The method of removal

(h) The source of the virus (if known)

(i) The extent of the damage (if known)

(j) The status of the incident

(k) Any additional comments or supporting documentation that is pertinent

b. Roles and Responsibilities

(1) The IAPM shall collect and communicate in quarterly reports to the USTRANSCOM, DON and other agencies as required.

(2) ISSMs shall collect all virus incident reports and forward them to the IAPM.

(3) ISSOs/NSOs shall:

(a) Keep the users informed about anti-virus procedures.

(b) Collect from the users and report to the ISSM all virus incidents.

(3) System/Network Administrators shall:

(a) Implement and administer virus protection.

(b) Ensure that virus definitions are updated appropriately.

(4) Users shall:

(a) Use anti-virus controls as directed.

(b) Report virus incidents to the ISSO.

2.7.5.7 Acceptable Use

Use of any IT system shall be for official use and authorized purposes only. Use shall be with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

a. Action

(1) The use of any IT system, including the use of the Internet, shall constitute consent to monitoring at all times, and there is no expectation of privacy.

(2) The following uses of the Internet are authorized:

(a) During work hours:

- Internet searches to research work-related issues
- Brief Internet searches to enhance your job-related professional skills
- Job searches in response to Federal government downsizing
- Emails for job-related purposes

(b) Outside of work hours (such as lunchtime):

- Sending a brief email to a family member or friend
- Brief Internet searches that do not involve prohibited Internet activities

(3) The following uses of the Internet are prohibited at all times:

(a) Stock trading

(b) Listing anything for sale

(c) Any activity for personal financial gain

(d) Accessing any sites with following subject matters:

- Pornography
- Gambling
- Computer games
- Computer hacking
- Chat
- Building or coding personal home pages
- Writing, forwarding or participating in chain letters or illegal, fraudulent, deceptive, malicious or criminal activities

- Fund raising activities, unless approved by the Commander
- Partisan political activity
- Malicious software activities
- Religious lobbying
- Using e-mail to transmit anything obscene, offensive or illegal

(4) Personal e-mail accounts outside of the MSC shall be used with caution, and e-mails from unknown sources shall not be opened.

(5) Instant messaging traffic to and from individually configured instant messaging clients that interact with a public service provider shall be prohibited within MSC networks. Both inbound and outbound public service instant messaging traffic shall be blocked at the enclave boundary.

b. <u>Roles and Responsibilities</u>

(1) The DAA shall ensure that confirmed violations are appropriately pursued.

(2) ISSMs shall investigate all violations of the acceptable use policy and determine whether the violation should be forwarded to the DAA.

(3) ISSOs/NSOs shall monitor system use to ensure that users are limiting their use of the Internet and e-mail to acceptable uses as defined above or more restrictively as appropriate, and forward potential or confirmed violations to the ISSM.

(4) Managers and supervisors shall:

(a) Ensure that users are aware the acceptable use policies.

(b) Report any suspected or real violations of acceptable use policy to the ISSM.

(5) Users shall only use the Internet according to the above guidance or any more restrictive guidance as applicable.

2.8 Program and Budget

All IA investments within MSC shall be continuously aligned to the mission and business needs identified through the enterprise IA architecture, and coordinated across related acquisition programs and operational domains.

a. Action

(1) IA shall be traced as a programmatic entity by MSC and visibility extended into MSC's budget execution. A discrete line item for IA shall be established in planning programming and budget documentation.

(2) Strategic IA goals and annual IA objectives shall be established in accordance with the strategic plans and funding and progress toward those objectives shall be tracked, reported and validated.

(3) Management controls shall be in place, which provide reasonable assurance against waste, loss, unauthorized use and misappropriation.

b. Roles and Responsibilities

(1) The IAPM shall ensure that the IA program is funded and that the funds are managed appropriately.

(2) Program Managers shall include line item for IA in new systems in development and annually budget for existing systems.

Section Three

Classified System and Enclaves

3.0 CLASSIFIED SYSTEM AND ENCLAVES

In addition to the normal concerns of an unclassified system, the controls discussed in this section shall be required for classified systems. Safeguards shall be applied so that classified information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity and is marked properly as required. When classified information is involved, the information security requirements in DoD 5200.1-R shall be met.[57]

3.1 Networks and Infrastructure

Beyond the general controls applicable for all computing environments, when transmitting classified information, additional controls shall be applied, involving such things as communication and emanations security.[58]

a. Action

(1) Users shall not transmit classified information over any communications system, except with approval, using approved IA procedures and practices.

(2) STU III or other crypto devices shall be utilized for all classified PCs and LANs.

(3) Classified data that is transmitted through a DoD, DON or MSC network that is cleared to a lower level than the data being transmitted shall be encrypted using NSA-approved cryptography.[59] The conduct of all DoD COMSEC activities, including the acquisition of equipment used to protect classified information, and systems shall be in accordance with DoD Directive C-5200.5.[60] Information of different classifications sharing the same transport media is encrypted using, at minimum, NIST-certified cryptography to prevent the commingling of data. Information in transit through a network at the same classification level, but which is kept separate for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography.[61] This control

[57] DoD 5200.1-R

[58] OPNAVINST C5510.93E, DON TEMPEST/PDS Procedures January 10, 2002, NAVSO P-5239-22 Protected Distribution System Publication, October 1997.

[59] Trusted Product Evaluation Program.

[60] DoD Directive C-5200.5, Communications Security, April 21, 1990.

[61] FIPS Pub. 140-2.

can be waived if not required by the Information Owner. Sources and methods intelligence (SAMI) information in transit through a network at the same classification level must be encrypted using NSA-approved cryptography.[62]

(4) Classified data that is encrypted with VPN techniques shall be handled at its original classification level unless an NSA-endorsed Type 1 (designed to secure classified information) cryptographic device is used.[63] If declassification of data is required (e.g., to allow for transmission over non-secure networks), an NSA-endorsed device must be used.

(5) A TEMPEST assessment shall be been requested for all IT systems processing Top Secret (TS), Special Intelligence (SI), Sensitive Compartmented Information (SCI) and for Sensitive And Below Interoperable (SABI) systems in a foreign country.

(6) There shall be shielded spaces for TOP SECRET/SCIF IT systems.

(7) Protected distribution systems (PDS) shall be used for the transmission of unencrypted classified data over through unsecured spaces.[64]

(8) PDSs shall be approved by SPAWARSYSCEN.

(9) All interconnections of MSC IT systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems. Interconnections of Intelligence Community and DoD systems with MSC systems shall be accomplished using a process lead by the MSC DAA.

b. Roles and Responsibilities

(1) The IAPM shall ensure that all communication IA controls used in classified systems are appropriately configured and implemented.

(2) ISSMs shall implement communication IA controls to ensure the safety of classified systems.

(3) ISSOs/NSOs shall monitor systems to ensure that they are appropriate configured.

[62] Trusted Product Evaluation Program.

[63] Trusted Product Evaluation Program

[64] NAVSO P-5239-22, PDS Publication, October 1997, OPNAVINST C5510.93E, DON TEMPEST/PDS Procedures, January 10, 2002.

(4) System/Network Administrators shall configure systems to enforce communication IA controls appropriately for classified systems.

3.2 Enclave Boundaries

a. Action

(1) For all IT systems that process classified information, boundary defense mechanisms, to include firewalls and network IDS, shall be deployed at the enclave boundary to the WAN, AND at layered or internal enclave boundaries.

(2) Only classified Internet sites may be accessed from a classified system.

b. Roles and Responsibilities

(1) ISSMs shall review the boundary policies and procedures and ensure that they meet current standards for protecting the classified enclave and systems.

(2) ISSOs/NSOs shall monitor boundary safeguards and network devices to ensure that they are configured to provide the level of security appropriate to the classification.

(3) System/Network Administrators shall implement and configure enclave boundary safeguards according to the security classification and Mission assurance category of the system or enclave.

3.3 Computing Environments

a. Action. A departmental reference document such as a SRG or a STIG shall constitute the primary source for security configuration or implementation guidance for the deployment of IT assets. For a system processing classified information, if a departmental reference document is not available, the system owner works with NSA to draft configuration guidance for inclusion in a departmental reference guide.

b. Roles and Responsibilities

(1) The Enterprise ISSM shall review the configuration and implementation policies and procedures and ensure that they meet IA requirements.

(2) ISSOs/NSOs shall review and monitor the configuration of IT assets.

(3) System/Network Administrators shall implement and configure IT systems according to the guidance appropriate for the particular security classification and Mission assurance category of the system or enclave.

(4) The Program Manager shall work with NSA to develop configuration guidance if none exists.

3.4 Life Cycle Management

a. Action

(1) Except as authorized by the DAA, personnel who perform maintenance on classified information systems shall be cleared to the highest level of information on the system.

(2) Cleared personnel who perform maintenance on a classified DoD IT system shall require an escort unless they have authorized access to the computing facility and the IT system. If uncleared or lower cleared personnel are employed, a fully cleared and technically qualified escort monitors and records all activities in a maintenance log.

(3) Non-US citizens shall not perform maintenance on classified systems.

(4) Remote maintenance shall not be permitted on classified systems, unless approved by the DAA.

b. Roles and Responsibilities

(1) The DAA shall review and determine whether to approve requests to allow remote maintenance.

(2) The Enterprise ISSM shall develop procedures for ensuring that maintenance personnel are appropriately controlled for the classification level of the system or enclave.

(3) Site ISSMs shall document and maintain on file the processes for determining authorization and the list of authorized maintenance personnel.

(4) Facilities Security Managers shall develop escort procedures for maintenance personnel.

(5) System/Network Administrators shall supervise the activities of maintenance personnel at all times.

3.5 Personnel Security

a. Action

(1) Individuals requiring access to classified information shall be processed for access authorization in accordance with DoD and DON personnel IA policies. These requirements will vary based on the sensitivity level of the information.

(2) Processing of classified information on privately owned computer systems or software shall be strictly prohibited.

b. Roles and Responsibilities

(1) ISSOs/NSOs shall periodically audit to ensure users have the correct access.

(2) Managers and supervisors shall:

(a) Ensure that users have been correctly processed for access authorization and need-to-know before users are allowed system access.

(b) Ensure that Users are aware of the prohibition against using privately owned computers for processing classified information.

(3) Users shall:

(a) Only access information for which they have clearance and need-to-know.

(b) Not process classified information on privately owned computer systems.

3.6 Administrative Security

a. Action

(1) If a classified enclave contains SAMI and is accessed by individuals lacking an appropriate security clearance for SAMI, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave.

(2) For IT systems processing classified information, multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics shall be presented to the registration authority.

Additionally, to the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password.

(3) Access control labels shall be associated with objects.

(4) For IT systems that process classified information, upon successful logon, the user shall be notified of the date and time of the user's last logon, the location of the user at last logon and the number of unsuccessful logon attempts using this user ID since the last successful logon.

(5) Audit records containing SAMI shall be retained for at least 5 years on a write-once/read-many device, such as a CD-R, or on a write-only device, such as a printer.

(6) In addition to the auditing defined in Section Two, IT systems that handle classified information shall also audit:

(a) Data required to audit the possible use of covert channel mechanisms.

(b) Privileged activities and other system level access.

(c) Starting and ending time for access to the system.

(d) Activities that might modify, bypass or negate safeguards controlled by the system.

(e) IA relevant actions associated with periods processing or the changing of security labels or categories of information.

(7) The contents of audit trails shall be protected against unauthorized access, modification or deletion. This includes backing the audit records up not less than weekly onto a different system or media than the system being audited, for systems that process classified information.

b. <u>Roles and Responsibilities</u>

(1) Site ISSM shall review all policies and procedures to ensure that they meet the minimum requirements for the classification level of the system or enclave.

(2) Facility Security Managers shall be responsible for maintaining audit records for the appropriate time period based on the type of information audited.

(3) ISSOs/NSOs shall monitor to ensure that systems are appropriately configured to protect the audit trail.

(4) System/Network Administrators shall:

(a) Configure systems to protect the audit trail appropriately based on the type of information audited.

(b) Configure the system to maintain the appropriate level of security based on the classification level of the system or enclave.

3.7 Physical Security

Spaces processing classified data shall meet DoD and DON requirements.[65]

a. Action

(1) Automated markings on classified output shall not be relied on to be accurate.

(2) If an area is not cleared for open storage, when not in use, classified media shall be stored in containers GSA approved safes with X07 locks.

(3) All media shall be marked and protected commensurate with the requirements for the highest security classification level and most restrictive category of the information ever stored until the media are declassified (e.g., degaussed or erased) using a DoD-approved methodology, unless the information is declassified or downgraded.

b. Roles and Responsibilities

(1) Site ISSMs shall:

(a) Review all physical security procedure to ensure that they meet the minimum requirements for the classification level of the system or enclave.

(b) Mark media and equipment used in classified spaces.

(2) Facilities Security Managers shall ensure spaces containing classified information are protected according to the classification level of the system or enclave.

[65] OPNAVINST 5530-14C.

(3) Users shall comply with all physical security requirements.

3.8 Security Documentation and Testing

a. Action

(1) The SSAA shall require additional protection if they contain risk assessments or residual risk statements that identify specific vulnerabilities associated with a system or application, that are not considered to be public, widely known vulnerabilities. The entire SSAA must be classified as confidential, or the classified information must be removed and placed in separate classified document, such as a classified appendix.

(2) Any documentation that contains classified information shall be marked and protected according to the classification of the information it contains.

b. Roles and Responsibilities

(1) ISSMs shall ensure that any classified information in any documentation shall be protected accordingly.

(2) ISSOs/NSOs shall monitor documentation to ensure that it is protected according to the classification of the information it contains.

Section Four

Definitions

4.0 DEFINITIONS

Automated Information System (AIS) Application

For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in reference (k). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS)). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in reference (j); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (MAIS).

Enclave

A 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. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks and data processing centers.

Evaluation Assurance Level

A collection of assurance components from the Common Criteria methodology that represents a point on a predefined assurance scale.

Mission Assurance Category

Applicable to 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 categories are primarily used to determine the requirements for availability and integrity services. (Note: The definition of mission assurance category is operationally focused and differs from that of mission criticality in the Clinger-Cohen Act of 1996, and the one used for reporting to Congress under Section 8121 of the FY 2000 Defense Appropriations Act, both of which pertain to information technology procurement, not to information or mission assurance support to deployed forces.)

Mission Assurance Category I

Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a Category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission assurance category I systems require the most stringent protection measures.

Mission Assurance Category II

Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission assurance category II systems require additional safeguards beyond best practices to ensure adequate assurance.

Mission Assurance Category III

Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission assurance category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

Outsourced IT-based Process

For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Platform IT Interconnection

For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration and remote upgrade or reconfiguration.

Section Five

Acronyms and Abbreviations

5.0 ACRONYMS AND ABBREVIATIONS

AIS	Automated Information System
CAP	Connection Approval Process
CCB	Configuration Control Board
CM	Configuration Management
COMSC	Commander, Military Sealift Command
COMSEC	Communication Security
DAA	Designated Approving Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DON	Department of the Navy
EAL	Evaluated Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance
IAPM	Information Assurance Program Manager
IAVA	Information Assurance Vulnerability Alert
IDS	Intrusion Detection System
ISSE	Information Systems Security Engineering
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KMI	Key Management Infrastructure
LAN	Local Area Network
MSC	Military Sealift Command
NIAP	National Information Assurance Partnership
NIPRNET	Nonclassified Internet Protocol Router Network

NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Intranet
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSA	National Security Agency
NSO	Network Security Officer
PKI	Public Key Infrastructure
SABI	Secret and Below Interoperability
SAMI	Sources and Methods Intelligence
SBU	Sensitive But Unclassified
SCI	Special Compartmented Information
SI	Special Intelligence
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Information (DoD Special Access Program)
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedures
SRG	Security Recommendation Guide
SSAA	System Security Authorization Agreement
SSL	Secure Socket Layer
ST&E	Security Test & Evaluation
STIG	Security Technical Implementation Guide
SW	Software
TS	Top Secret
UPS	Uninterruptible Power Supply
USTC	United States Transportation Command
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

References

Enclosure (3)

REFERENCES CONTINUED

(b) Public Law 106-398, Title X, Subtitle G, GISRA, October 30, 2000

(c) Navy-Marine Corps NIPRNet Enclave Protection Policy, November 30, 2001

(d) MSC Public Key Infrastructure Roadmap, October 17, 2001

(e) DoD Memorandum, Policy Guidance For Use of Mobile Code Technologies in DoD Information Systems, November 7, 2000

(f) DoD Regulation 5200.1-R, DoD Information Security Program, January 1997

(g) DoD Directive 5230.9, Clearance Of DoD Information For Public Release, July 15, 1999

(h) DoD 5230.20, Visits, Assignments, Exchanges of Foreign Nationals, August 12, 1998

(i) DoD 5230.25, Withholding of Unclassified Technical Data from Public Release, November 6, 1984

(j) SECNAV R 211930Z, DON Worldwide Web Policy, October 1998

(k) DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release, May 6, 1996

(l) DoD Regulation 5200.2-R, DoD Personnel Security Program Regulation, January, 1987

(m) DoD Directive 8500.1 October 24, 2002

(n) DoD Instruction 8500.bb (Draft), February 1, 2002

(o) NIST FIPS PUB 140-2, Security Requirements For Cryptographic Modules, October 10, 2001

(p) SPAWAR Technical Memorandum, VPN Devices and Applications Used in the US Navy Unclassified Networks, February 2, 2000

(q) OPNAVINST 5530.14C, DON Physical Security, December 10, 1998

(r) SECNAVINST 5510.30A, DON Personnel Security Program, March 10, 1999

(s) SECNAVINST 5510.31C, Policy and Procedures for Control of Foreign Disclosure in the DON, December 31, 1992

(t) SECNAVINST 5510.36, DON IS Program Regulation, March 17, 1999

(u) CINCPACFLT Pearl Harbor HI 122126Z, Information Assurance Advisory No. IAA-001-02, March 2002

(v) X.509 Certificate Policy for the United States Department of Defense, Version. 5.2, November 13, 2000

(w) Deputy Secretary of Defense Memorandum, DoD PKI, August 12, 2000

(x) NAVSO P-5239-04, Information Systems Security Manager Guidebook, September 1995

(y) NAVSO P-5239-07, Information Systems Security Officer Guidebook, February 1996

(z) NAVSO P-5239-13, Vol. II, December 2000 (aa) NAVSO P-5239-16, Risk Assessment Guidebook, September 1995

(bb) NAVSO P-5239-19, Incident Response Guidebook, August 1996

(cc) NAVSO P-5239-22, PDS Publication, October 1997

(dd) NAVSO P-5239-26, Remanence Security Guidebook, September 1993

(ee) DoD Instruction O-8530.2, Support to Computer Network Defense, March 9, 2001

(ff) DoD Directive C-5200.5, Communications Security, April 21, 1990

(gg) OPNAVINST C5510.93E, DON TEMPEST/PDS Procedures, January 10, 2002

(hh) Memorandum 5230, MSC Connection Approval Process, July 22, 2002

(ii) USTC, Information System Security Handbook for Program Managers, March 2002