Chapter 16 – Cybersecurity Management

Table of Contents

References

(a) DoD Instruction 8500.01, Cybersecurity

(b) OPNAVINST 5239.1D, U.S. Navy Cybersecurity Program

(c) NAVSEAINST 5239.2B, Cybersecurity Program

(d) DoD Instruction 8500.2, Information Assurance (IA) Implementation (cancelled)

(e) DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)

(f) COMNAVIDFOR M-5239.2D, Commander's Cybersecurity Manual

(g) Federal Information Security Modernization Act (FISMA) – 2014 revision

(h) CNSSP 22, Committee on National Security Systems (CNSS) Policy on Information Assurance Risk Management for National Security Systems

(i) DoN CIO memorandum of 20 May 2014, DoN Implementation of the Risk Management Framework (RMF) for DoD Information Technology (IT)

(j) NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

(k) NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans

(l) CNSSI 1253, Security Categorization and Control Selection for National Security Systems (27 March 2014)

(m) NAVSEA ltr Ser 04/117 of 24 Nov 2014, NAVSEA 04 Compliance with Risk Management Framework

(n) NAVSEA eMASS Business Rules

(o) NAVSEANOTE 9400 ser 05Q-016/355 dated 15 Aug 2018, Naval Sea Systems Command Commander's Intent For Cybersecurity Readiness Improvements

(p) DoD Directive 8140.01, Cyberspace Workforce Management

(q) DoD 8570.01-M, Information Assurance Workforce Improvement Program

(r) CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities

(s) SECNAVINST 5230.14, Information Technology Portfolio Management Implementation

(t) NIST SP 800-147, BIOS Protection Guidelines

(u) NIST SP 800-147B, BIOS Protection Guidelines for Servers

(v) DoD Manual 5200.01 Vol 3, DoD Information Security Program: Protection of Classified Information

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

(x) DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual

(y) CNSSD No. 504, Directive on Protecting National Security Systems from Insider Threat (FOUO)

(z) DoD Directive 5205.16, The DoD Insider Threat Program

(aa) SECNAVINST 5239.20A, DoN Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual

(bb) DoN CIO memo of 8 April 2015, Coding of DoN Positions Performing Cybersecurity Functions

(cc) SECNAV M-5239.2, DoN Cyberspace Information Technology and Cybersecurity Workforce Management Manual

(dd) DoD Instruction 8551.01, Ports, Protocols, and Services Management (PPSM)

(ee) Navy Telecommunications Directive (NTD) 01-15, Registration of Internet Protocol (IP) Addresses and Domain Name System (DNS)

(ff) DISA Connection Process Guide

(gg) DoD Instruction 8100.04, DoD Unified Capabilities (UC)

(hh) DoD Information Assurance Certification Accreditation Process (DIACAP) Handbook

(ii) SECNAVINST 5239.19A, DoN Computer Network Incident Response and Reporting Requirements

(jj) OPNAVINST 3100.6J, Special Incident Reporting

(kk) CJCSM 6510.01B, Cyber Incident Handling Program

(ll) SECNAVINST 5239.3C, DoN Cybersecurity Policy

(mm) COMNAVIDFOR M-5239.3C, Cybersecurity Readiness Manual

(nn) DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

(oo) DoD Manual 5200.01 Volume 4, DoD Information Security Program

(pp) USD(I) letter of 17 May 2018, Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base

(qq) NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

(rr) SECNAV M-5210.1, Records Management Manual

Chapter 16 – Cybersecurity Management

16.1 Preface

16.1.1 Purpose

This chapter identifies a common framework for ensuring the safety, security, accessibility, and regulatory compliance of information systems owned or controlled by the SUPSHIP community. It also provides guidance for oversight of contractor-operated information systems containing controlled unclassified information (CUI) when protection of CUI is a requirement of contracts administered by SUPSHIPs.

16.1.2 Terminology

Reference (a), DoDI 8500.01, defines Information Assurance (IA) as ***cybersecurity***, the current term used by DoD to conform with National Security Presidential Directive (NSPD) No. 54 and other instructions. The purpose of cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. For the purposes of this chapter, the terms “cybersecurity” and “information assurance” should be considered synonymous. Further, “enclave” and “site” are used interchangeably by referenced documents and are intended to mean the command Information Systems (IS) environment which has received authorization (accreditation) by a designated Navy Authorizing Official (NAO).

Reference (b), OPNAVINST 5239.1D, U.S. Navy Cybersecurity Program, provides the most current guidance in implementing the Navy’s cybersecurity program and, while primarily directed to echelon 2 and above commands, should be reviewed by personnel in cybersecurity positions to assist in understanding the direction that the effort is taking to comply with cybersecurity objectives.

Many of the terms related to security certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP) have changed under the Risk Management Framework (RMF) methodology (see §16.2). Because the DIACAP to RMF transition is currently underway, the terminology will be used interchangeably in this chapter. Many of these changes are identified in this chapter’s acronym list, Appendix 16-A.

16.1.3 Responsibility

Paragraph 6.c of reference (c), NAVSEAINST 5239.2B**, Cybersecurity Program, designates commanders of NAVSEA activities as their command’s Local Cybersecurity Authority (LCA), responsible for overall implementation of IA at the command level. NAVSEAINST 5239.2B** provides cybersecurity guidance for all NAVSEA commands and

subordinate activities. It should therefore be considered mandatory reading for those involved in developing and executing the cybersecurity program at each SUPSHIP.

An Information System Security Manager (ISSM), formerly known as an Information Assurance Manager (IAM), must be appointed in writing by the commanding officer to exercise local information assurance authority controls for the command. The primary responsibility of the ISSM is to develop and oversee an effective cybersecurity program for the command and serve as the local advisor to the commanding officer for cybersecurity issues.

Reference (d), DoDI 8500.2, had been the DoD IA Implementation Guide that defined policy, assigned responsibilities, and prescribed procedures for applying integrated, layered protection of Navy information systems and networks. It has now been superseded and cancelled by DoDI 8500.01, which takes a slightly different approach. The new cybersecurity program merges DoD's efforts with the National Institute of Standards and Technology (NIST) mandates used by other agencies. Revised guidance and terminology can be expected, so ISSMs must stay abreast of changes in order to ensure implementation of the most current requirements issued for Navy commands.

Information System Security Officers (ISSOs), formerly known as Information Assurance Officers (IAOs), are also typically designated to assist in the IA effort when enclave/system size warrants additional help. The ISSM or other authorized official should ensure ISSOs are appointed for each Program of Record hosted by the command enclave. Where the ISSO for a hosted software program has been appointed by the information system owner (ISO) and is remote, the command ISSM should maintain contact for awareness of any issue that might impact the command cybersecurity posture. The ISSOs, in supporting the ISSM, report information to the ISSM as an additional duty.

Information systems are normally designed, installed, maintained, and operated by Information Technology (IT) specialists, such as network administrators, database administrators, programmers, applications and operating systems specialists, and others who are functionally assigned to the command IT Program Manager. The ISSM is a separate entity, intended to be a neutral mediator in the command's cybersecurity program; the availability, safety and security of the information within the accredited enclave is the paramount issue for this position. For that reason, the command ISSM position must be independent of responsibility for actual operation of the command IS and has a direct path of communication to the commanding officer regarding the command's cybersecurity posture.

16.1.4 Information Systems (IS) Authority to Operate

A number of directives, including enclosure 2, paragraph 7.f. of reference (e), DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), specify that the command's Information Systems are only authorized to operate if accreditation has been achieved. This holds for stand-alone systems as specified in DoDI 8510.01, enclosure 6 paragraph 1.b.(4), as well as those connected to the DoD Information Network (DoDIN), formally known as Global Information Grid and commonly referred to as the GIG. To that

end, the ISSM will focus on maintaining the command's IS accreditation by ensuring continuous effective compliance with all relevant requirements.

16.1.5 Limitations

Cybersecurity is achieved through a well-defined set of controls authorized by several public laws and implemented by numerous Federal, DoD, and Navy directives, instructions, and guides. This chapter is not intended to modify in any way the authorities, responsibilities and controls identified in those documents. Rather, the key documents which establish the foundation for cybersecurity are identified with emphasis on their critical elements.

16.1.6 Nuclear Programs

For those commands involved in nuclear shipbuilding programs, any cybersecurity issues which warrant reporting to SEA04 shall also be reported to SEA08.

16.2 Introduction

As mentioned in the preface, the commanding officer is the local authority ultimately responsible for the availability and security of the command's information systems. As the command's cybersecurity expert, the ISSM is the commanding officer's primary advisor and frontline resource for executing this responsibility. The ISSM position requires aggressive attention to the myriad details necessary to securely operate information systems in today's complex and challenging environment. The ISSM not only needs to know the status of the command's IS enclave, but also must keep the commanding officer informed, especially when problems occur. ISSMs should therefore establish an agreement with the commanding officer which clearly delineates the kind of information desired and the manner and frequency in which it will be provided. Although developed for the Fleet, reference (f), COMNAVIDFOR M-5239.2D**, Commander's Cybersecurity Manual, provides commanding officers of shore installations with the cybersecurity mechanisms and information needed to ensure continued information system security operating under controls mandated by the Federal Information Security Modernization Act (FISMA) of 2014, reference (g). The M-5239.2D** manual also offers suggestions relating to the data ISSMs should be prepared to provide to the commanding officer, either periodically or on request.

DoDI 8500.01 and subsidiary instructions define the DoD process for authorizing information systems to be certified as compliant with the current rules for information security. As directed by reference (h), CNSSP 22**, Committee on National Security Systems (CNSS) Policy on Information Assurance Risk Management for National Security Systems, DoDI 8500.01 mandates a programmed shift from the current DIACAP to the RMF approach developed by NIST. DoD expanded on the RMF and started implementing that change by issuing a revised DoDI 8510.01. The DON CIO issued reference (i), DoN CIO memorandum of 20 May 2014, with additional RMF implementing instructions for the DON. The RMF developed by NIST and introduced by reference (j), NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, imposes a number of stringent controls which must be implemented in order to obtain, retain and renew the

necessary network authorization to operate. IS security controls assessments required by NIST are identified by reference (k), NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. These and other NIST publications are subject to revision, so visiting the NIST website periodically is encouraged. For IS categorized as a National Security System, reference (l), CNSSI 1253**, Security Categorization and Control Selection for National Security Systems, expands on SP 800-53 to include special DoD criteria. Both sets of documents are necessary reading for ISSMs, IS program owners, and others involved in the respective system and enclave authorizations, and both websites offer valuable insight into cybersecurity control mechanisms now being refined in DoD processes.

DoD has provided an information paper titled Revised RMF Transition Timeline** which gives additional guidance on the transition period from DIACAP to RMF. The paper can be found at the RMF Knowledge Service** website (registration required). While this paper is intended for DoD and subsidiary policy and instruction development from which command instructions and cybersecurity operations flow, it does offer insight regarding the timeline by which all DoD information systems must complete the transition. ISSMs should therefore read it and prepare for the expected changes. Reference (m), NAVSEA letter Ser 04/117, available from SEA04Z, provides further direction on the allowable transition period and emphasizes the actions required to achieve the conversion and the consequences of not meeting the schedule. It also identifies some of the notification requirements when an authorization expires. Subsequent to the release of both of these documents, Change 2 to DoDI 8510.01 was issued which outlines additional guidance, including a more definitive timeline for the phase-in of ATO's (Authorization to Operate) based on RMF compliance.

The RMF Knowledge Service web site is DoD's official site for enterprise RMF policy and implementation guidelines and is a useful source of information to ISSMs. The web site provides tools for selecting controls under RMF, including Controls Explorer which may be of use during enclave or software planning.

Access to RMF Knowledge Service requires a CAC/DoD PKI certificate and one-time registration at https://rmfks.osd.mil/login.htm.

Network accreditation by issuance of an Authorization (aka Authority) to Operate (ATO) is provided by the designated NAO once evidence for site compliance with the most current cybersecurity criteria has been submitted and approved. If the site is not in compliance or falls out of compliance, a Denial of Authorization to Operate (DATO) may be issued instead. NAO's may appoint a Delegated Authorizing Official (DAO) to act in his/her place for low to moderate impact systems. Regardless of which official makes the accrediting decision, the same process must be followed to obtain or renew accreditation. A path for requesting initial or renewed authorization is through DoD's Enterprise Mission Assurance Support Service

(eMASS) program. By direction of the NAVSEA Command Information Officer (CIO), eMASS is the only path authorized to NAVSEA field commands for requesting an IS Certification and Accreditation (C&A), now known as Assessment & Authorization (A&A), decision. ISSMs should therefore become very familiar with the reference (n) NAVSEA eMASS Business Rules** available on iNAVSEA. The rules will be modified as RMF introduction matures, so command ISSMs should be alert for changes. eMASS will also require updating of various artifacts as changes to the command system occur after authorization. Most of the initial activity for entering system A&A requests in eMASS will reside with the information system/enclave owner but the ISSM can be a valuable resource for the owner in assuring the personnel assignments and information entered in eMASS are correct.

Once the changes necessary to complete execution of DoDI 8510.01 are definitively identified in implementing Navy instructions, the command IT staff and ISSM must complete the conversion process to the extent and within the timeframe specified by the direction received. Efforts will also be required of information system owners.

Additional guidance to the NAVSEA enterprise including field activities has been issued by reference (o), NAVSEANOTE 9400 ser 05Q-016/355 dated August 15, 2018**, Naval Sea Systems Command Commander's Intent For Cybersecurity Readiness Improvements. It provides direction for continued improvements in cybersecurity afloat and ashore. In the NAVSEANOTE, paragraph 4.g. is specific action required of field activities. The document has a restricted distribution statement but will be provided upon request to SEA04I for authorized parties.

The ISSM position is tasked by numerous DoD, SECNAV, and DON instructions with certain duties which must be performed for the command to obtain and retain the enclave/systems network authorization. Limited flexibility is allowed in the methods to meet the requirements of DoDI 8510.01 and other instructions. To complement the guidance provided in those instructions and to accomplish their assigned task, command ISSMs must develop/possess an itemized list of the tools they believe are needed, the breadth of tasking, and a list of the assets to be protected. They must then assemble the tools available, identify any shortages, and initiate action to complete the toolkit. COMNAVIDFOR M-5239.2D** provides excellent guidance in developing checklists which serve as reminders of repetitive tasking required of ISSMs and others in retaining command IS authorization. One of many web locations worthy of retention in the toolkit is the DoD Cyber Exchange web site, which provides a central location for new developments in related documents, virus alerts and other news of interest. There are numerous other sources which are available to assist command ISSMs and others in staying abreast of current cybersecurity requirements. Additionally, tools are increasingly available to help the IA/IT community record, analyze and track IA issues. An example is the Vulnerability Remediation Asset Manager (VRAM) program, a Navy Enterprise application which serves as a repository and analysis process for uploaded site vulnerability data. As these resources are identified as useful to the mission, the ISSMs should note them in the toolkit records they maintain.

16.3 Information Systems Security Manager (ISSM) Oversight

16.3.1 Fundamental Program Administration

16.3.1.1 Written Guidance

Development of a command cybersecurity program begins with establishing local directives which detail the processes and assignments necessary to comply with cybersecurity criteria. This and many other early planning steps must have been accomplished prior to requesting network authorization. Active and continuous maintenance of command instructions is as important as any other element of information assurance. Numerous resources exist which can help in this area. An example is the DoN CIO web site which has an IT Policy and Guidance section. Frequent visits to this site and others like it will assist in maintaining command instructions and implementing policies current with higher level requirements.

The Security Technical Implementation Guides (STIGs) developed by the Defense Information Systems Agency (DISA) are used to evaluate system compliance to cybersecurity requirements and develop the accreditation request. Selected STIGs establish minimum security requirements as instructed by DoDI 8500.01 and NIST 800-53 based on the software/system/enclave's declared Mission Assurance Category (MAC) and Confidentiality Level (CL). STIGs frequently address local documentation in place for processes. Failure to have adequate written instructions stating policy, identifying measures to implement requirements outlined in the relevant STIG, assigning responsibility, and recording accomplishment activity will generally result in an unsatisfactory finding. While the ISSM may not be the originator of most activity within this framework, oversight to ensure that relevant instructions are current, reflect the latest guidance, and are being followed is essential to establishing and maintaining a satisfactory command cybersecurity posture. At a minimum, the ISSM should periodically review the issue date of all applicable command instructions related to the IS operation and flag any which are more than one year old. The process owner should require a detailed review of the instructions which fall in that category to confirm processes conform to the instruction, and that the foundation-level instructions have not changed.

DISA currently releases a quarterly summary of the Security Technical Implementation Guides (STIG) in effect at the time, including modified and new releases. The ISSM should review these quarterly releases and confirm with the command IT group that all necessary changes have been incorporated in the command IT systems.

16.3.1.2 Training

Early planning must include identifying and implementing training requirements to develop and maintain a certified and qualified Cyber IT/Cyber Security Work Force (CSWF) to carry out cybersecurity functions. Identifying training requirements and ensuring training has been accomplished is not only necessary per reference (p) DoDD 8140.01, Cyberspace Workforce Management, and reference (q) DoD 8570.01-M, Information Assurance Workforce Improvement Program, but mandated for selection and retention in key IT positions. Since a

knowledgeable IT staff is fundamental to an effective cybersecurity program, the ISSM must be aware of the command's IT staff training status. In addition, the ISSM and ISSOs should participate in arranging, conducting and participating in local cybersecurity initial and refresher training for command personnel in conjunction with the Security Officer.

The ISSM shall also ensure that a process is in place to restrict access to command information systems to only authorized users with the correct credentials and who have completed DoD approved cybersecurity training. This includes initial cybersecurity awareness orientation and annual cybersecurity awareness refresher training for anyone accessing a command IS, regardless of location or employment affiliation. When group training is employed, a positive means of establishing attendance shall be utilized. For key IT positions which have requirements for periodic subject-specific training or certifications, the ISSM must have a list of those positions, the required training/certifications, the current status, and the next due date of any refresher requirements. The list and status should originate with the affected position's supervisor with initial notification and updates provided to the ISSM as they occur. Requirements for ISSM training (for those occupying those positions), certification and status must be included on the command list.

Software and IT hardware is constantly evolving. Many changes require some degree of specialized training for one or more IS team members before entering the production environment. Because individual qualifications and certifications may be impacted, providing resources to acquire the necessary training to support the change is essential. This is particularly true for those products approaching end of life or when higher echelons introduce new technology (hardware or software) to the environment. In both cases, early preparation for these changes can result in more cost-effective solutions. The command's IT Program Manager should budget time, staffing and funding for current and anticipated changes in IS software and hardware used at the command, paying particular attention to those requiring specialized knowledge or certification of personnel to continue uninterrupted operation. Awareness of future changes is a key element in the planning effort, and the Navy CIO website is an ideal place for field activities to acquire knowledge of future changes being considered. An additional resource for enterprise software information is the Navy Enterprise Software Licensing (PMM 172)** website which offers information on current and potential contracts, along with contact information.

The cybersecurity training requirements can be costly and time consuming, but are the easiest to conquer and the most common to fail. If compliance with the mandated standards will place the command's authority to operate in jeopardy, the commanding officer shall be notified with a temporary solution, along with a plan for permanent corrective action. SEA 04 must be alerted when the command's network authorization may be impacted, and a timely resolution is not available.

16.3.1.3 Configuration Control Board (CCB)

Paragraph 2.g. of enclosure 3 to DoDI 8500.01 requires that all cybersecurity-enabled IS products incorporated into DoD information systems have implemented security controls based on their categorization. Paragraph 6.a.(11) of enclosure C to reference (r), CJCSI

6211.02D, Defense Information Systems Network (DISN) Responsibilities, tasks DISA with developing and providing security configuration guidance for cybersecurity and cybersecurity-enabled IS products, including developing and updating STIGs. Within the DISA STIGs is a requirement that the configuration of each IS asset be governed by an active CCB. The main objective of the CCB is to maintain a cost effective, structured process for considering and approving changes to each command's IS. Every command with an accredited IS enclave shall have an IS CCB which considers establishment of, or changes to, the command's IS assets. This includes restricting installed administrative software to the DoD enterprise software which has been vetted and approved by DoD (and complies with reference (s), SECNAVINST 5230.14, Information Technology Portfolio Management Implementation) and other DoD/Navy approved hardware lists, some of which are changing as more enterprise-centric solutions are being created. The same holds true for connectivity and other services. The CCB should be provided a Configuration Management Plan, developed by the IT Program Manager, which details staff oversight of installed software, hardware and firmware, including versioning, licensing and certificate information. The ISSM should ensure the plan is comprehensive, current, implemented, and updated as needed. The CCB should be aware of changes, and is the authority for those changes. The CCB should also be aware of current and forecasted IT budgeting requests, approvals and shortfalls. The IT Program Manager must consider inclusion of services and maintenance in the annual budget request for hardware and software, particularly when planning addition or removal of equipment or software. The CCB may also elect to be the oversight mechanism for command cybersecurity related instructions.

The CCB has a number of controlling directives which govern how they function. For example, the SECNAV CIO has directed that all IT expenditures (except certain expendable items) must be approved through the Navy Information Dominance Approval System (NAVIDAS). Additional or revised guidance for access to special purpose information systems and sensitive data, new sources for enterprise wide purchasing, and more effective methods for securing information will occur as cybersecurity and cost control become the dominant drivers in how the Navy acquires and operates IS. The ISSM must also keep CCB members informed about compliance with recent directives when considering changes to the command IS.

The ISSM must be a key member of the CCB for IS systems, as any change contemplated in the command IS must be evaluated for cybersecurity impact. The ISSM will ensure an audit of the CCB's records occurs periodically to confirm the software packages in use have been approved and the configuration database maintained by the CCB reflects an accurate compilation of each software baseline and all changes considered since this baseline. A similar mechanism shall be in place for IS physical assets supporting the command IS.

The ISSM shall ensure that a procedure is in place to install the most recent authorized patches/revisions to command operating software and that at least one position is tasked with monitoring changes available, authorized, and installed. BIOS configuration for servers and client devices must be included in the control arrangement (DoDI 8500.01 enclosure 3, paragraph 9.b.(19) requirement). References (t), NIST SP 800-147, BIOS Protection Guidelines, and reference (u), NIST SP 800-147B, BIOS Protection Guidelines for Servers,

provide guidance for development of the command standard in this area. The ISSM must have available a status report of mandated/implemented patch changes.

16.3.1.4 Internal Controls

Reference (v), DoDM 5200.01 Vol 3, DoD Information Security Program: Protection of Classified Information, and companion volumes provide instructions regarding protection of classified and sensitive but unclassified (SBU) information; the latter has been redefined by reference (w), CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), enclosure A, paragraph 7.a.(1), as CUI. Reference (x), DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual, provides instructions for protection of military, political, diplomatic, economic, or technological information which individually or in the aggregate could be considered as critical to the proper functioning of a DoD component. A simple guiding principle is that information not designated as Distribution Statement A (approved for public release; distribution is unlimited) falls within one of the protected categories and should be safeguarded. The Security Officer and the command ISSM working as a team must be aware of these instructions and related guidance designed to allow the necessary information to flow within the command and its supporting team, while guarding against unintended access or disclosure to unauthorized parties. The command security team must ensure the local command policies include:

- Proper controls for information extracted from the IS, and destruction using authorized methods when no longer needed.
- Restricting mass downloading of information unless absolutely necessary.
- Preventing unauthorized devices from being attached to any IS component.
- Securing system back-up tapes or other authorized storage media in approved containers.
- Personnel with privileged access operate under controls which minimize the possibility of loss or compromise of information.
- Complying with all relevant instructions which are intended to prevent information leakage.
- Taking measured advantage of computer-generated audit capabilities.
- Awareness of effective techniques for information security (including OPSEC) among all personnel having access to the command IS.

The Committee on National Security Systems issued binding directive reference (y), CNSSD No. 504**, Directive on Protecting National Security Systems from Insider Threat (FOUO), to help protect National Security Systems from insider threats. As a result, reference (z), DoDD 5205.16, The DoD Insider Threat Program, was released and contains implementing instructions. Although not directly assigning responsibility to Echelon III commands, it applies to all organizational entities within DoD and is recommended reading for the command ISSM and the Security Officer.

16.3.1.5 Cybersecurity Workforce Management

Reference (aa), SECNAVINST 5239.20A, DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification, implements a DoD policy developed to strengthen personnel in the workforce who are responsible for designing, developing, operating, or maintaining the security of supporting IT infrastructures, systems, applications, and networks, including those individuals who have responsibility for maintaining the confidentiality, integrity and availability of the information contained in and transmitted from those systems and networks. Within SECNAVINST 5239.20A are a number of responsibilities assigned to the commanding officer (and subordinates) of any Navy facility which receives, processes, stores, displays, or transmits information electronically. The ISSM must be aware of those assignments and assure that the command has processes and implementing procedures in place which are effective in accomplishing the functions outlined in SECNAVINST 5239.20A. In addition, the ISSM is assigned responsibilities by reference (bb), DoN CIO memo of April 8, 2015, Coding of DON Positions Performing Cybersecurity Functions, for monitoring the command's Cybersecurity Workforce (CSWF) program to ensure it adheres to policy, guidance and standards, and provides support to Human Resources in identifying positions which should be designated as a cybersecurity assignment.

SECNAVINST 5239.20A also requires establishing a Cyber IT/CSWF Program Manager (Cyber IT/CSWF-PM) responsible for administering the organization's Cyber IT/CSWF Program. Among the many duties assigned, DoN CIO memo of April 8, 2015 includes a requirement that the CSWF-PM coordinate a review with the Office of Civilian Human Resources (OCHR) quarterly to validate Cybersecurity Workforce position information. Instead of creating a dedicated Cyber IT/CSWF-PM position within a command, SECNAVINST 5239.20A provides the flexibility for commands to utilize the services of a higher level Cyber IT/CSWF-PM when agreement is reached between the two organizations for that relationship.

16.3.1.6 Privileged Access Controls

Paragraph 6.c of NAVSEAINST 5239.2B** requires the commanders of local NAVSEA field activities to appoint in writing a command ISSM, a Cyber IT/CSWF Program Manager and all personnel who perform Cyberspace IT/Cybersecurity functions. The appointees and any other privileged access personnel are required to acknowledge in writing an understanding and acceptance of their responsibilities until access is removed, as required by DoD 8570.01-M paragraph C3.2.4.4, utilizing form SECNAV 5239/1 as required by paragraph 3 of the introduction to reference (cc), SECNAV M-5239.2, DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual. The ISSM must have a list of personnel with privileged access to the command IS and ensure compliance with the requirements associated with those positions. The objective is to minimize privileged access without adverse impact to the operation of the enclave. The process selected by the command to accomplish these steps should be included in a command instruction or policy defining the process for granting, use and removal of

privileged access, along with identification of any accompanying authorities, responsibilities and reporting requirements outlined by higher echelons.

16.3.1.7 Accrediting a Site or Enclave

Undertaking an IS site authorization or re-establishing an authorization is a demanding task and will require the ISSM, IT Program Manager and IT staff to work closely together throughout the process. Stakeholders should create a command Plan of Action and Milestones (POA&M) which outlines every intended step from start to finish, assignment of responsibility (by name or code), the timeline for accomplishment, a record of achievement, and estimated/actual labor and material costs for each step. The initial step will be to define the scope of capability (purpose) of the enclave. For example, determine if it will limit activity to hosting Commercial-Off-The-Shelf (COTS) software to provide unclassified administrative services for the command, or if the services will be more demanding (up to and including classified information processing possibly). Other issues will be the range of connections (LAN/WAN/DoDIN for example), population/composition of users (command employees, external federal employees, contractor workforce, limited public access, mix), and other considerations. Once the basic purpose and planned content is established, the MAC and CL levels can be determined and the command POA&M will chart the way for gaining authorization to operate. Tasks defined within the POA&M should ensure development of those controls and artifacts required within eMASS. Some examples of artifacts required are development of a:

- System Security Plan (SSP) or Security Assessment Plan
- Risk Assessment Report (RAR)
- Information Security Continuous Monitoring (ISCM) Plan or a Continuous Monitoring (ConMon) Plan
- Security Assessment Report (SAR)
- POA&M for identifying and mitigating risks

Many of these and others not mentioned will be living documents, requiring development and modification as the authorization request progresses through the review/testing/approval process. A part of the planning should include development of an IT contingency plan with policy, business impact analysis, prevention controls, recovery strategy, prevention and recovery training and testing, and implementation and maintenance consideration. The command plan should also include appropriate STIGs and the action required to comply; any not applicable should be acknowledged with an appropriate justification for exclusion. Most of this will be required as a part of the authorization request. The IS CCB should review and approve the command POA&M prior to initiating any effort to implement, and should be informed of progress periodically. After the command POA&M is approved by the CCB, the planned site must be registered in the DON Application and Database Management System (DADMS) and entered in eMASS as the first announced steps in the authorization process. The NAVSEA eMASS Business Rules should be referenced as a guide during the accreditation effort. The system will require qualified personnel to serve in specific roles during the authorization process. These include:

- Information System Security Engineer (ISSE) who will test the system to matching IA controls, identify weaknesses where non-compliances are noted, upload required artifacts, run the eMASS POA&M report, select a validator, and submit the controls for validation.
- Validator who will review and confirm (or return for further work) each input by the ISSE, add or edit weaknesses, severity or artifacts, make remarks to add clarity to the recommendations, and notify the ISSO/ISSE of the completed validation.
- Echelon II representative who will schedule a collaboration effort with the collaboration team after confirming the package is complete according to pre-established criteria and ready to go forward.
- Security Control Assessor (SCA) who will review the package for the management, operational and technical security controls employed within, or inherited by, an IS to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, will operate as intended, and produce the desired outcome with respect to meeting the security requirements for the system). SCAs also provide an assessment of the severity of weaknesses or deficiencies discovered in the IS and its environment of operation and suggest corrective actions to address identified vulnerabilities, and provide a recommendation for acceptance or denial of the package submittal to the NAO.

The NAO will use the package and recommendation to determine whether deployment of the IS presents an acceptable level of risk to the DoDIN and the information being processed, and then issue an ATO or DATO. In the event an existing ATO expires, is removed, or is severely restricted, the CCB should consider requiring development of a POA&M for recovery; it can be a valuable tool in planning, budgeting and measuring progress of the effort. The same is true for any major upgrades or expansions to existing accredited sites or enclaves.

As mentioned earlier, any IS hardware installed in an enclave intended to become or remain accredited must meet DoD standards. The list of tested and approved equipment is updated constantly as new devices are tendered by manufacturers or revisions to older models are incorporated. STIGs and the enclave accreditation process have numerous requirements other than hardware which also must be met. These include:

- Internal and external physical security
- Boundary controls
- Architecture mapping describing network topology
- Firewall descriptions
- Router controls
- Content security checking processes
- Demilitarized Zone (DMZ) standards
- Mobile code control
- Equipment and software inventory
- Version declaration

- Entry standards
- Emergency procedures and disaster recovery processes
- Power and environmental standards
- Other criteria which must be established and tested before requesting accreditation

The STIGs and referenced controls clearly define the necessary events which must be met. Continued maintenance for compliance after receiving accreditation is essential to retain it. A number of other actions must also be completed as a part of the accreditation process. For example, reference (dd), DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), requires ports and protocols selected for use be restricted to those authorized in Ports, Protocols, and Services Management (PPSM) registry, and provisions included to block or otherwise secure those not authorized. Obtaining IP allocations and DNS services will be necessary, following the path outlined in reference (ee) Navy Telecommunications Directive (NTD) 01-15**. Other minimum requirements include installation of a network intrusion detection system, a DMZ if publicly accessible services are provided, a firewall, and application aware proxy services. The assigned IT Program Manager usually is responsible for accomplishing most of this work with significant help from the IT staff, but the ISSM must be involved in each step of the evolution to ensure completion. In some cases, DoD guidance will specifically assign selected activity to the ISSM, while in others, the ISSM will be required to attest to the results. These details should be clearly addressed in the POA&M along with any other checkpoints which must be passed. When the enclave is approved (accredited), connection to the Defense Information System Network (DISN) will most likely be desired. A number of the artifacts developed for enclave accreditation will also be required when requesting a DISN account using the Connection Approval Process (CAP), particularly for a Non-secure Internet Protocol (IP) Router Network (NIPRNet) or Secret Internet Protocol Router Network (SIPRNet) request. DISA is designated by DoDI 8500.01, enclosure 2 paragraph 2.e, as the authorized agent for controlling that process and has published reference (ff), DISA Connection Process Guide, to assist in the application. As with most documents, the guide will evolve with time, so the command accreditation team should ensure the latest version is used. SIPRNet connections must also comply with the documentation required by the SIPRNet Connection Approval Office (SCAO) to receive the SIPRNet Interim Approval to Connect (IATC) or final Approval to Connect (ATC).

Changes to the enclave or site after accreditation must be controlled, tested when required, recorded, reported and assessed for STIG compliance, as well as any conditions accompanying the ATO. The DISA ATC decision authorized by reference (gg), DoDI 8100.04, DoD Unified Capabilities (UC), enclosure 3 paragraph 4.a.(3), is contingent on receiving and maintaining an enclave ATO and must be renewed periodically as is the case with the enclave accreditation.

16.3.2 Add New Programs to an Accredited Enclave

The DADMS is a web-enabled registry of Navy and Marine Corps systems and applications. Enterprise software which is approved for use within the Navy will be listed in DADMS. Any software not listed in DADMS and proposed to be added to the command IS enclave must be approved via the DADMS “New Add” process in order to avoid impacting the enclave

accreditation. The ISSM responsible for oversight of the enclave cannot permit introduction of unapproved/unaccredited software in the enclave. Reference (hh), DoD Information Assurance Certification Accreditation Process (DIACAP) Handbook, provided the authorized path for gaining accreditation, however, it is evolving as DoD combines the existing methodology with the NIST approach. Everyone involved in cybersecurity needs to maintain awareness of the constantly changing landscape as new threats develop and additional steps are taken to counteract them.

Software development and certification activities will originate with the software owner (referred to as the information system owner (ISO) in DoDI 8510.01 and other instructions) with help from knowledgeable program development participants, including those involved in the accreditation process. Unlike approved operating systems and enterprise software, most commands will not host custom software programs nor have a substantial role in development. However, network administrators shall not install any software in a command IS operating environment until written authorization from the CCB is received. The CCB shall not provide authorization for any software to be activated in a command IS operational environment until the software has received approval and association in DADMS by the responsible Functional Area Manager (FAM).

16.3.3 Maintain Authorization to Operate and Conduct Reviews

16.3.3.1 Maintain Accreditation

This section assumes the site or enclave:

- has been properly registered in DADMS;
- the enclave artifacts necessary for accreditation are current and have been loaded in eMASS;
- there are no Category 1 vulnerabilities or they have been mitigated and proper approvals obtained;
- accreditation has been achieved.

Upon qualifying the site (enclave) as physically and electronically ready to host information systems and after receipt of accreditation for the installed software/system, the software/system can be connected in its intended environment with the authorized security settings. The command IS CCB should be informed that the installed software is available and functional so the users can utilize the features as authorized. The accreditation letter will frequently cite directives which define the parameters and boundaries under which operation may start and continue. The ISO's host IT Program Manager and host ISSM shall ensure controls are embedded which ensure those limitations receive recognition and compliance. The criteria may be met through documented procedures, training, access restrictions, periodic examination and testing, limited input or output, or any other authorized mechanism which accomplishes management of the program/enclave within the confinement of the cited directives. The ISSM must ensure local operating procedures authorized by the command IS CCB include the controls selected to implement the ATO restrictions. Operating outside the

limits of the ATO is prohibited. The programmers, network administrators, database administrators, and other IT support staff will perform day-to-day operation of each command information system in accordance with established processes/procedures. The processes/procedures themselves shall have been developed to comply with the security requirements of the DoD, as confirmed during the A&A examination and testing process. The ISSM shall ensure that the task requirements of maintaining situational awareness, monitoring checklist compliance, conducting annual reviews, and obtaining reaccreditation of the system/site when necessary are met throughout the life cycle of the enclave.

In this section the following IA functions are addressed:

- Maintain Situational Awareness
- System Administration Oversight
- Plan for Annual Review

16.3.3.1.1 Maintain Situational Awareness

The activities to maintain situational awareness are the actions performed to maintain accreditation for software, systems, or sites that have been issued either an ATO or IATO. The purpose of these actions is to ensure that the integrity of the program, system, or site is continually monitored and any deviation from the approved configuration, settings, and processes is properly evaluated by the command's ISSM. These three monitoring activities are conducted concurrently:

- Monitor for security-relevant events
- Monitor for life cycle and accreditation status change
- Monitor quality of Security Control Implementation

16.3.3.1.1.1 Monitor for Security Relevant Events

When monitoring for security relevant events, the ISSM relies on the automated system reporting software for unusual activity or alarms triggered by out of parameter controls. Most monitoring is accomplished by the command IT staff through regular assignments as defined by established and tested command procedures and written policies, but the ISSM can request specific actions to be taken in addition to the routine checks performed. Departures from established controls when observed by the staff should be reported to the ISSO and ISSM. This monitoring occurs continuously from accreditation until decommissioning. In some cases, the IS users may report unusual behavior of IS hardware or software they are using. This is particularly true of virus infections or malware. Other out of norm indicators may be reported to the ISSO by the IT staff. Every report must be investigated to determine if a security controls compromise is imminent or has occurred. The ISSM must anticipate incidents and prepare for them before they happen. A security-relevant event is any local and/or external change in the environment, software, or system that impacts the security posture or security control compliance of that software, system, or site. Some of these events could be observed and reported by:

- Information Assurance Vulnerability Alerts or Bulletins (IAVA/IAVB)
- Any change in compliance with security controls
- Virus, worm or other malicious code infection
- Loss of integrity or confidentiality − unauthorized access
- Electronic Spillage (see reference (ii), SECNAVINST 5239.19A, DON Computer Network Incident Response and Reporting Requirements, and enclosure 7, paragraph 5 of DoDM 5200.01 Volume 3 among others)
- Discovered vulnerabilities
- Inheritance change
- Boundary vulnerabilities and changes
- Environment changes
- Reports or discoveries reported by Navy Cyber Defense Operations Command (NCDOC)

Information Assurance Vulnerability Alerts or Bulletins are released by DISA often as a part of the Information Assurance Vulnerability Management (IAVM) system, and patches to commercial operating systems or software are just as frequent. When an IAVM document is received, it explains what the vulnerability is, how critical it is, and if a patch is immediately necessary. Commercial organizations employ a Common Vulnerability Enumeration system, the equivalent of the IAVM system in use by DoD. For the command resource guarding the configuration of equipment and software impacted by IAVMs, the difficulty is connecting an IAVM notice to the commercial patch that mitigates the reported vulnerability. DISA has helped in that regard by posting a spreadsheet which clarifies the relationship, if there is one. Automated tools to maintain IS systems current with IAVM notices as necessary have, or are in the process of, being developed and fielded, as are auditing tools to scan installed systems for IAVM compliance.

Changes in security control compliance can occur when any software, hardware, process, or facility modification occurs. That is the underlying reason for frequent scans of systems using automated tools developed or tested/approved by DISA. Knowing the applicable security controls for each hosted system is necessary in assessing the potential impact of change to any element of the enclave. STIGs exist and identify the controls for most DoD approved COTS applications, and the various A&A plans will have that information for tailored development software. The ISSM should be aware of every change contemplated before it is introduced in the enclave. Most of the changes will be known to the assigned ISSOs, so communication is a necessary tool for the ISSM.

Malicious infections are commonly introduced by user download of content attachments to emails or by visiting infected web sites. Anti-virus software with current threat signatures and software which blocks access to web sites with suspicious or known vulnerabilities has helped reduce, but not eliminate, this threat. Knowledgeable users with good cybersecurity

habits are a key to controlling this exposure. ISSMs should ensure all users having access to the command IS have periodic training in infection avoidance techniques.

Unauthorized access can occur from internal or external sources. Most internal access compromises can be minimized through application of a rigorous physical security and IS access control policy. A more prevalent threat occurrence in this area is external penetrations by skilled hackers taking advantage of poor electronic boundary controls, and enabled by installed software with security weaknesses. Constant penetration testing using the latest DISA approved tools is the defense mechanism which can detect most of these weaknesses. The ISSM and ISSOs should ensure the local policy for periodic penetration testing is current and implemented, monitor the penetration testing efforts, be aware of unauthorized access events, and ensure required reporting avenues exist.

When an information compromise has been detected, the following directives, and other implementing guidance, establish a chain of reporting which must be followed:

- CJCSI 6510.01F, Information Assurance and Support to Computer Network Defense (CND)
- OPNAVINST 3100.6J, Special Incident Reporting (restricted access), reference (jj)
- CJCSM 6510.01B, Cyber Incident Handling Program, reference (kk)

The ISSM must be familiar with this process and ensure a procedure is in place which provides for each reporting requirement to be accomplished. Commands may have a separate ISO who functions as the primary contact for receiving IS compromise notices, but the ISSM must be a part of the process for the purpose of determining if or how the enclave and its components may have been impacted. The ISSM shall always be certain the commanding officer and NAVSEA 04 are aware of each compromise and is provided assurance the reporting process has been followed.

Electronic spillage generally refers to a security incident that results in the transfer of classified or CUI onto an unaccredited (unauthorized) information system for the appropriate classification level and/or dissemination restrictions. A majority of these incidents are the result of user carelessness and could have been prevented with more consideration. The ISSM's responsibility for spillage is preventive in nature: provide support for a command program that ensures training, awareness and attention to detail by those entrusted with information access is not just implemented but is effective, coupled with a procedure which provides processes and assignment of responsibility which ensure any spillage is promptly and properly contained, reported and scrubbed as mandated by existing DON policy. Generally, the commanding officer and SEA04 will also need to be advised of confirmed spillages. The IT Program Manager working in coordination with the Security Manager will determine if additional steps to prevent a recurrence are needed after investigating the incident.

Vulnerabilities may be discovered by routine scanning, reports from external agencies, penetrations detected during operation, or the periodic cybersecurity reviews. Any known vulnerability must be assessed by the ISSM for severity, operational impact, corrective

measures needed, and reporting requirements. The knowledge of vulnerability must be shared with the cybersecurity community as defined in the relevant command procedure. Because of the evolutionary nature of vulnerabilities and the defense against them, an aggressive approach by the cybersecurity staff in the utilization of programs designed to detect and correct them is necessary. The command's enclave cybersecurity compliance may be impacted by changes in the DoD or DON cybersecurity criteria, the requirements of which entails a continuous awareness by the command IT staff and ISSM. For example, the position assigned responsibility for ports, data services and protocols within the command's enclave (normally a network technician/engineer) must monitor policies and implementing instructions at the DoD or sub-tiers which authorize those IT access points. DoDI 8551.01 establishes requirements in that area, but is subject to change as is any other policy, directive or instruction. For those network accreditations issued prior to 27 July 2017 (the issue date of change 1 to the current DoDI 8551.01), the current command instruction and implementing controls must be evaluated in a timely manner to determine if any changes are necessary. From that analysis, a determination can be made regarding any modifications necessary to the cybersecurity posture. The command instruction should include a requirement that the ISSM be informed at the initiation and conclusion of the event. This process holds true for every dynamic attribute impacting the command's network accreditation and foundation A&A package.

Inheritance changes at a tenant enclave are always possible, are usually outside the control of the tenant, and can have undesirable or unintended consequences. The command cybersecurity program must provide for an effective communication with all parties which put in place the inherited controls impacting the command's enclave accreditation.

Any changes to the cybersecurity posture, either local or external, must be documented and assessed for severity. If the event impacts the software, system, or the environment, the ISSM will evaluate what risk it has introduced to the software, system, site, enclave, and/or DoDIN. If immediately returning to the original configuration is not practical, the commanding officer shall be promptly notified of the potential problem.

Collaboration through the Echelon II sponsor with the SCA (formerly known as Certifying Authority (CA)) and/or NAO, may be necessary to make a final risk determination. In some cases, minor or even no corrective action may be needed due to a very low and acceptable risk posed by the event. In this case, the ISSM will take action if any is required, record the findings for historical purposes, and return to continually monitoring the software or system and environment for security relevant events.

If a security event presents an unacceptable risk to the software, system, enclave, or DoDIN, but the corrective actions identified do not require a change of the accreditation, the ISSM will ensure that the event is documented and reported to any impacted process owners and will monitor execution of the corrective actions by the IT staff. The ISSM will also ensure that the corrective actions were effective in mitigating or reducing the risk and will document the results of the corrective actions that were applied. The commanding officer, along with SEA 04, will be notified of the resolution, as required. The ISSM will then resume monitoring for security relevant events.

If a security event presents an unacceptable risk to the software, system, enclave or DoDIN, and corrective actions proposed do not acceptably mitigate or manage the vulnerability, the accreditation will be affected. The ISSM shall document and immediately report the event to the commanding officer and, via the chain of command, the SCA/NAO who will determine the required actions. The ISO, IT staff, power users, SEA 04, and others who may be critically impacted (defined collectively as stakeholders) shall also be informed. Actions required by the SCA/NAO may be severe, including possibly disconnection from the DoDIN, system shutdown, or software de-installation as described in the command's IS Decommission Activity instruction.

16.3.3.1.1.2 Monitor for Life Cycle and Accreditation Changes

The ISSM continuously monitors the software, system or the environment for any life cycle and/or accreditation status change from the time of accreditation (or installation) until decommissioning. Any potential change in the life cycle or accreditation status of the software, system and/or environment must be assessed by the ISSM. If a change in the life cycle and/or accreditation status is eminent, the ISSM must notify the commanding officer and collaborate with the stakeholders to determine the course of action that will be taken.

A change in accreditation may be an upgrade, downgrade or expiration/DATO. If the change is an upgrade, the only action required by the ISSM is to receive and document the accreditation change. The ISSM will then resume monitoring activities consistent with the upgraded system requirements.

If the accreditation is a downgrade and the software or system is still needed as determined by the ISO and stakeholder collaboration, the IT Program Manager or ISO and supporting parties will implement necessary changes to correct any shortcomings identified, and then revert back to re-executing the Security Authorization Package (SAP) as described in the implementation plan which was developed to certify the original software or enclave for operation. The commanding officer and SEA 04 will be immediately notified. Accreditation downgrades should not be a surprise to the ISSM; an aggressive local cybersecurity oversight program will disclose most problems as they develop. Once the software/ or system issues are resolved and accreditation restored, the ISSM must examine the local controls to determine why oversight did not detect and prevent the initial downgrade root cause.

A change in life cycle will result in either the resumption of monitoring activities, modification of the current accreditation, re-registration of the software/ or system, or decommissioning the software/ or system. If the life cycle change results in software/ or system decommissioning, the ISSM will ensure removal of the software/ or system from operation as described in the commands' IS Decommission Activity instruction. Decommissioning a system with a presence in eMASS requires activity in that forum and should be provided for in the command Decommission Activity instruction. DoDI 8510.01 enclosure 6 paragraph 2.f.(7) provides guidance in this area.

If the life cycle change does not result in decommissioning, the ISSM and the stakeholders must collaborate to determine if the life cycle change adversely impacts the security posture of the software, system, enclave, and DoDIN. If the change does not impact the security posture, the ISSM will document the change in the software or system's A&A package and resume monitoring activities. If the change does adversely impacts the security posture, the ISSM will ensure the software or system is re-registered in DITPR-DON in compliance with reference (ll), SECNAVINST 5239.3C, DON Cybersecurity Policy, and DoN CIO Memorandum dated December 5 Dec, 2011, as a new system and begin the A&A process for the new system. When the security posture is impacted but to a lesser extent, the existing accreditation may be modified upon request. Communication between the ISSM, ISO, Echelon II sponsor, and SCA/NAO will establish which event is necessary.

16.3.3.1.1.3 Monitor for Quality of Security Control

The ISSM continuously monitors for the quality of security control implementation to ensure the continued effectiveness of security functionality. Actions that must be taken include, but are not limited to:

- reviewing the inheritance relationships between systems and/or network, firewall changes
- reviewing audit logs
- conducting spot audits
- conducting vulnerability scans
- checking for changes to the security controls as listed in the RMF Knowledge Service**

In addition, the ISSM will also be aware of the date the software, system, or site is due for annual review. This monitoring occurs continuously from accreditation until decommissioning.

Because software, systems and enclaves are interrelated, the ISSM must annually review all inheritance relationships to ensure that any inherited security controls are still valid and provide the required security functionality to the inheriting system.

The ISSM will also check the latest security control list (for the system's Mission Assurance Category (MAC) and Confidentiality Level (CL)) and compare it with the software or system's last validation report. If there is no difference, or if the difference between the updated security control list and the software or system's last validation report does not impact the security posture of the software, system, or environment, the ISSM will resume the monitoring activities. Any difference between the latest security control list and the software or system's validation report may indicate a change in security control compliance and must be assessed for a possible change in the software, system, or environment's security posture.

If the security posture of the system or environment has changed significantly, the system may have to be re-registered as a new version in eMASS and cycled through the A&A process again. The ISSM shall evaluate the degree of change, communicate with the authorizing officials, including the Echelon II sponsor, to establish the necessary action to be taken, and implement any guidance received.

16.3.3.1.2 System Administration Oversight

System Administrators are typically assigned to perform a variety of IS duties. Among these may be periodic scans of operational systems for security vulnerabilities, reporting results, IAVM patching and testing, scans for unauthorized devices, periodic testing for continued STIG compliance, assuring anti-virus definitions are current, user account management, and a host of other activities. The use of well-written, standardized checklists (usually crafted from STIG requirements) can ease this burden and markedly reduce the vulnerability exposure of IT products. DISA has a number of automated checklists developed for this purpose. Much of the system qualification necessary during SAP development will require use of automated checklists tailored to the applications and local configuration. An aggressive cybersecurity program will make frequent use of checklists to examine the operating systems' resistance to outside attacks after network accreditation is received. Checklists are implemented by system administrators and database administrators, but the ISSM must be aware of, and validate via audit, the checklists being used and that only those complying with DoD policy are in use, the schedule of planned use, the frequency at which the systems are actually being tested, and the results of the tests. Feedback from the checklist program should be one of the methods on the list of tools created by the ISSM, as properly written and implemented automated checklists can be a powerful indicator of system susceptibility to compromise. When automated checklists are updated by DISA or other authorized originators, applicability to embedded software in the enclave must be considered. A record of these events must be a part of the cybersecurity history maintained by the IT staff, just as usage, results and corrective action, when necessary, is documented. The ISSM must be proactive in assuring compliance is achieved. The ISSM is also tasked with defining selected controls on enclave installed software. For example, STIG rule SV-56679 states the operating system must allow only the ISSM (or individuals or roles appointed by the ISSM) to select which computer system auditable events are to be audited. A similar rule exists for any installed Database Management System (DBMS). If this function is redelegated, a list of those persons/roles assigned that responsibility must be maintained by the ISSM.

16.3.3.1.3 Plan for Annual Review

As the system or site approaches its 12-month anniversary of accreditation, the ISO representative, with assistance from the ISSM, will initiate an annual review as described below in the Conduct Annual Reviews section. In maintaining a three-year network accreditation, also in the Conduct Annual Reviews section, internal reviews are required to be completed prior to the end of each twelve-month cycle for the first two years, while a complete command review followed by a reaccreditation request is scheduled during the third year. The NAVSEA CIO eMASS Business Rules provide mandatory guidance in initial,

modification, renewal, and deactivation of IS system/ or enclave accreditation for all commands functioning under the NAVSEA A&A process. Step by step instructions are provided, including timelines. ISSMs and the IT Program Manager must be intimately familiar with these rules as failure to comply can result in loss of IS accreditation for the command.

16.4 Cyclic Events

16.4.1 Keep Management Informed

As stated previously, an activity's commanding officer is designated as the local information assurance authority. The ISSM is responsible for assuring that the commanding officer is kept abreast of the activity's IS cybersecurity posture, existing weaknesses, steps being taken to mitigate, status of compliance with higher level institutionalized requirements, including reporting, anticipated events or changes which may impact command IS cybersecurity, scheduled reviews both internal and external, budgetary or personnel issues involving command IS cybersecurity, and any other information which may play a part in the command IS cybersecurity health. A summary of past cybersecurity inspection results and status of actions taken to address any findings from those inspections should be a part of the information provided. Periodic briefings where the status of the overall picture can be displayed are encouraged.

Another management program which must be considered is the SUPSHIP Manager's Internal Control Program (MICP). OMB Circular A-123 was originally developed in response to the Federal Managers' Financial Integrity Act of 1982. It has since been expanded to include a host of other congressional mandates for internal controls and reporting, including those in FISMA. As such, any significant issues related to the management of the command information systems, including cybersecurity issues, must be identified as a part of MICP. A component of the MICP is program and performance metrics. The MICP assessment unit information, the annual review required by DoDI 8500.01, and any reviews conducted by external parties, should present an accurate measure of the cybersecurity management effectiveness at the command and each should agree in substance with all other inspection components. Should this not be the case, the ISSM must consider adjustments to the command's internal processes and related procedures to correct the shortfalls.

16.4.2 Status Requests and Reports

The command can also expect requests from external sources for information relating to the health of the command IS. Unscheduled data calls from various agencies regarding intrusion attempts, current system resources, key personnel certification status, progress in internal inspections, mitigation of cybersecurity weaknesses, and patch configuration are some typical subjects. Most of these will be issues which are reportable by law or regulation. Defense Information Systems Agency, Fleet Cyber Command, Navy Cyber Defense Operations Command, Navy Information Dominance Forces, and other entities focused on protection of information and information systems have various reporting requirements which evolve with time and require input from many sources, including NAVSEA and subordinate commands.

In addition, certain events that may occur in accredited systems have mandated reporting requirements invoked on the host command. In some cases, specific positions within the host command are assigned the reporting responsibility by NAVSEA or higher-level instructions, and in all cases the local implementing instructions should identify the position tasked for initiating or executing any reporting requirement. The ISSM should be aware of all reporting criteria related to cybersecurity and must be aware of compliance reporting which is triggered by events which could impact the command enclave accreditation. Regardless of the point of reception for ad hoc data calls relating to the command information systems, the command instructions addressing responses to information systems data calls or reporting requirements should require the receiving party to notify the ISSM of the information requested, the time frame required for the response, the availability of the information, and the responsible party within the command that will service the call. The ISSM should determine any possible relationship to the command's information system enclave accreditation and notify the commanding officer if a nexus exists.

16.4.3 System Backups and Restore

Each command IT Program Manager shall establish a periodic system back-up plan which conforms to the information assurance controls developed for the A&A package, meets the needs of the operating environment, the criticality of the data to the users, and the parameters imposed by the system owners when the software program(s) were conceived. The ISSM should ensure the command IS CCB is aware of the plan and any changes under consideration. Back-up schemes for each software program or associated database may vary depending on these and other factors. The ISSO assigned to the program should confirm to the ISSM that a back-up scheme exists, is institutionalized, implemented, and accomplished according to the planned schedule, and conforms to the requirements defined by the program owner and approved as a condition of the software accreditation process. As a part of the overall plan, the IT Program Manager or designated representative must include a provision for safe storage of the back-up media which is consistent with relevant instructions and the command IT Contingency Plan. The ISSM should review the back-up plan annually to confirm compliance with the IT Contingency Plan and the A&A submittal.

Restoration from system equipment failures, software glitches, data corruption, disaster recovery, and other unplanned events must be considered. A local instruction defining the steps to be taken (including assignment of responsibility, level of authorization, notice to users, documentation of actions performed, and all other reasonable controls) to accomplish a full or partial restoration of every information system should be a prominent feature of each system. The ISSM must confirm the existence of a command instruction for this event (a desk guide is an option for small enclaves), conformance to cybersecurity controls, annual "dry runs" to confirm practicality, and implementation when necessary.

16.4.4 Shutdown System

In case of emergent circumstances, receipt of a DATO, or as a result of monitoring activities, an application or system may need to be shut down (disconnected from the DoDIN and local operating environment) or the entire enclave may be impacted. The commanding officer,

SEA 04 and the ISO must be notified immediately. A warning to system users should be provided, with as much lead time as is possible. The shutdown may be short-term until problems are corrected, or it may be permanent. When an unplanned shutdown is warranted, the software or system must be disconnected and the ISO/ISSM/IT team shall execute corrective actions immediately. If the corrective actions resolve the problem, the actions are verified (tested) for effectiveness, and the A&A documentation is updated to reflect the actions, normal operations may then be resumed after gaining permission from the SCA/NAO though the chain of command. The ISSM shall ensure the commanding officer and SEA 04 are notified of the resolution.

If corrective action cannot be taken, the ISSM, in consultation with the commanding officer and the information system owner, must then determine if the software or system will be reaccredited or if it will be decommissioned (removed). Protection of the enclave should be first priority. In some cases, if the compromises can be mitigated or are minor, the only action required may be a request for a modification to the existing software accreditation. Communication among the ISO, ISSM, SCA, echelon II sponsor, and NAO will determine if that is an acceptable option. For reaccreditation action, the system categorization process starts the RMF evolution again. If the software or system will be removed, the stakeholders must be notified and the ISSM shall ensure the de-install procedures identified in the relevant instruction are followed.

16.5 Periodic Assessment

16.5.1 Conduct Annual Reviews

The purpose of the annual review is to ensure that the cybersecurity posture of the software, system or site is assessed and reported at least annually. The review shall be documented and results provided to the commanding officer. Annual reviews are mandated by enclosure 4, paragraph 2.b.8. of DoDI 8510.01. Annual reviews of the enclave are the primary responsibility of the command IT Program Manager. Annual review of each hosted software is the primary responsibility of the software owner, assisted by the assigned ISSO and the host IT staff. The role of the command ISSM is to ensure each review takes place, is properly conducted, and results are recorded and reported using the most current requirement.

In the event a designated ISSO is reassigned or departs and is no longer available to perform the duties necessary as an ISSO, a replacement must be appointed if the assigned system is still in operation. The relief ISSO must be fully qualified with the appropriate certifications, and should institute a review of the assigned system which is equivalent to the annual review expected of the software owner or ISSO team, within the constraints that are imposed by the position. If someone not certified at the level required is appointed, the steps required to bring them to that level (including timeframes) must be untaken, and any controls necessary in the interim must be implemented. In the event a designated ISSM is reassigned/ or departs, a replacement must be appointed if operation of the enclave as an accredited entity is still required. The relief ISSM must be fully qualified with the appropriate certifications, and should institute a review of the entire enclave which is equivalent to the

annual review, within the constraints that are imposed by the position. If someone not certified at the level required is appointed, the steps required to bring them to that level (including timeframes) must be untaken, and any controls necessary in the interim must be implemented. For any appointment of personnel who are less than fully certified at the level required, SEA04 must be informed of the plan (with timeline) for resolving the issue. Failure to follow through or meet the mandated timeline could result in system operating restrictions, up to and including a requirement to discontinue operation of the enclave and hosted software.

16.5.1.1 Review Security Controls

The ISSM must obtain the validation results for assigned or inherited security controls and review them with the remainder of the A&A package of the system or site for accuracy. Currently, a minimum of 1/3 of the security controls must be evaluated during the annual reviews in order that all security controls will have been evaluated during the three-year network accreditation cycle. The ISSM will ensure the A&A package is updated by the IT Program Manager or ISO if any discrepancies are discovered prior to testing and validation.

16.5.1.2 Test/Validate Applicable Security Controls

Once the responsible parties and command ISSM have verified the accuracy of the A&A package, the Validation Plan and Procedure for the software, system, or site as applicable should be executed by the IT staff. The ISSM will review the test results and compare them with the test results documented in the validation report portion of the previous Validation Plan and Procedure document of the A&A package.

Using the artifacts provided, the ISSM then confirms the software, system, or site is in compliance with all applicable security controls. If in compliance, the ISSM shall ensure that the validation report portion in the current Validation Plan and Procedure document of the A&A package has been updated. If not in compliance, or if a degradation to the cybersecurity posture occurred, the system owner and command ISSM must analyze the problem and coordinate a solution with the stakeholders, if necessary, which is then documented in the A&A package. The IS Security POA&M will also be updated to reflect the necessary corrective action. The command ISSM must ensure that Category 1 security control non-compliances have been reported to the Echelon II sponsor and authorizing officials immediately upon detection.

16.5.1.3 Compile Annual Review Package

The command’s designated ISSM must also update the system security control compliance status along with the dates conducted. The host command ISSM (if not the owner designated ISSM) should be aware of the update. The final step is for the system owner ISSM to draft a Statement of Compliance using the SAR format, with the concurrence of the host command ISSM. Included in the review must be a risk assessment for the purpose of identifying security control risks to command operations, command assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security

controls that would mitigate this impact. Also included is a security review for the purpose of evaluating the current security plan, controls, testing, and necessary changes.

The Annual Review Package (also known as the Security Authorization Package) at this point consists of the SSP, SAR, RAR, IT Security POA&M, and Statement of Compliance. Once the package is complete, the software/ owner, enclave owner/, or ISSM signs and submits it to the SCA, with the permission of the commanding officer, unless otherwise directed by the SCA. The Risk Assessment Report must be approved (signed) by the commanding officer annually. The NAO/SCA may allow less critical security controls to be tested less frequently, require critical security controls to be tested more frequently, or only require submission of an Information Security Continuous Monitoring Plan (ConMon) report annually (the standard package development is still needed). Communication through the Echelon II sponsor with the assigned SCA/NAO will determine what standards are appropriate for the command's IS.

16.5.1.4 Plan and Prepare for Other Mandated Reviews

Due to the critical nature of information flow within and between commands and other interested parties, cybersecurity has become and will remain a topic of interest throughout the government. As a result, a number of reviews are mandated for the life of any information system operated by the command. Some have obvious connections to cybersecurity and others are more obscure. Among these are:

- The Manager's Internal Control Program, where the IT organization, IT staff training, cybersecurity positions, IS asset control, and other IS attributes related to command management control will be examined periodically.

- NAVSEA Performance and Compliance Inspection (Inspector General scheduled examination of command operations). A thorough review of the command IS operation will almost always be accomplished by the IG team.

- Cyber Security Inspection (CSI) by a FLTCYBERCOM Office of Compliance and Assessment (OCA) team. This review is normally accomplished with or near the request for renewal of the command's Authority to Operate.

- An inspection patterned after the CSI is normally accomplished by a command internal team prior to the OCA team arrival and as a preparation for that event. The primary purpose is to develop assurance that the command cybersecurity posture is compliant with the internal and external criteria which governs award or retention of enclave/ or software accreditation.

The ISSM should conduct in-depth planning for each of these events and any others not on the list which may impact the command cybersecurity posture. For example, the internal plan in preparation for a CSI should be robust and thorough, including a review of:

- network infrastructure
- DNS configuration
- DNS operating system functioning under Windows

- DNS operating system functioning under UNIX
- internal vulnerability scan
- wireless and VOIP security if those capabilities exist
- complete enclave review
- Host-Based Security System review
- physical security review
- examination of the demilitarized zone
- cybersecurity workforce improvement plan
- access management
- asset management
- privileged user authorization
- PII protection
- compliance with other STIGs
- other areas as deemed appropriate

While the IT Program Manager and others may create and implement the plan, the ISSM must provide active oversight of the planning, development, execution, results, and reporting. The findings of any one of these reviews can have a major impact on retention of the command's authority to operate an information system.

16.6 Accreditation Renewal

16.6.1 Reaccredit

As specified in enclosure 6, paragraph 2.e.(4)(a) of DoDI 8510.01, network accreditations are issued with an authorization termination date (ATD) specified of not more than three (3) years from the network accreditation issue date with certain exceptions. If this is the third annual review and the software/ or enclave does not fall within the exceptions permitted by DoDI 8510.01, or if significant changes have been made to the software, system, or site, the system owner or IT Program Manager, with the assistance of the command IT staff and command ISSM, must compile a reaccreditation A&A package consisting of the following minimum requirements:

- Updated SSP
- Updated RAR
- Updated SAR
- Updated IT Security POA&M
- Statement of Compliance
- Signature page

The ISO/IT Program Manager shall begin the SAP review process prior to the ATD. The NAVSEA CIO Business Rules for eMASS provide the timeline for starting the process.

Any comprehensive review, including reaccrediting, must be a teaming effort of the ISO/IT Program Manager, the command ISSM, the entire IT staff, and other stakeholders. As the command's cybersecurity technical lead, the ISSM will guide the effort and keep the

commanding officer informed of progress. Once the reaccreditation A&A package is complete, the ISO/IT Program Manager submits it in accordance with the NAVSEA CIO Business Rules for eMASS, much like the original accreditation.

16.6.2 Continuous Process Improvement

It is incumbent on the ISSM and IT staff to look closely at vulnerabilities that the package documents and to consider possible mitigations even if the risk associated with the vulnerability is low. The command IS CCB should be aware of any previously undisclosed cybersecurity exposure and the options and costs of addressing vulnerabilities so an informed decision can be made. One of the ISSM's duties will be to make such information available to the CCB for their risk assessment. If the command's continuous cybersecurity effort is effective, most risks will already have been identified as a natural result of the processes in place and any new information will be minimal. If this is not the case, the ISSM and IS stakeholders need to re-evaluate the existing processes to determine where they can be strengthened.

As a primary source of information for security practices, the Navy Information Dominance Forces command is a valuable resource for practical methods that can be implemented during the daily operation of IS. In particular, reference (mm), COMNAVIDFOR M-5239.3C**, Cybersecurity Readiness Manual, was developed to provide assistance to ISSMs, ISSOs and the other members of the cybersecurity team. It was designed for forces afloat, but most practices can easily be adapted to shore installations.

In addition to internal efforts, exchange of information between commands facing similar IS situations involving problems encountered, actions taken to resolve problems, solutions that were effective or less so, errant steps along the way, and methods employed to approach the issues are also helpful. In recognition of this, SEA 04 representatives will host a periodic meeting among command ISSMs. It is strongly recommended that command ISSMs and other command IT personnel attend these meetings, with a pre-arranged list of topics to be discussed. One of the topics will always be the current cybersecurity challenges of the respective command enclaves, along with any planned expansion or contraction of hosted systems and anticipated cybersecurity difficulties with those changes. This meeting will allow for a free exchange of information among field personnel using the agreed to agenda as a baseline.

16.7 Oversight of Shipbuilder/Subcontractor Cybersecurity Processes

16.7.1 Purpose

When contractually invoked, DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, reference (nn), provides detailed requirements for a contractor to provide adequate security on all contractor covered information systems. Shipbuilding and ship repair contracts are currently being issued with DFARS 252.204-7012 invoked. Contracts will also frequently have a Contract Security Classification Specification

(DD Form 254) as an attachment. One criterion that may be listed as a requirement on the DD Form 254 is reference (oo), DoD Manual 5200.01 Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI). As with any contract provision, when the cited DFARS clause, DoD Manual 5200.01 Volume 4, or some other provision to protect CUI is invoked as a requirement in a shipbuilding or ship repair contract, the assigned Contract Administration Office (CAO), such as a SUPSHIP, is obligated to provide oversight of contractor implementation and execution. The purpose of this section is to provide guidance in accomplishing that objective. When DFARS 252.204-7012 is not invoked in a contract under the command's administration, this section does not apply.

16.7.2 Responsibility

Contractor-owned and operated IT systems contain devices and software very similar to government-owned systems and are supported by similar personnel resources, although guidance for qualifying both may differ in details. The technological requirements are identical, and therefore oversight of a contractor system, however limited in purpose, will require expertise which already exists within the command. The commanding officer may assign the task of contractor cybersecurity oversight to any person or organization within the command, while ensuring the assigned parties have the knowledge and qualifications necessary to execute the mission effectively. The various project manager representatives (PMRs) should notify the commanding officer or responsible assigned task owner when any contracts under their purview contain DFARS 252.204-7012 as a requirement so command oversight may be planned and implemented.

16.7.3 Limitations

DoD Manual 5200.01 Volume 4 specifies the controls and protective measures developed for DoD CUI at the time it was issued and identifies the use of distribution statements on unclassified technical documents as a means to facilitate control, distribution, and release of such documents. Additional federal policy was anticipated when DoD Manual 5200.01 Volume 4 was first released and has been promulgated by multiple agencies and commands on a continuing basis. Most will impact how government oversight of contractor IT systems containing CUI is accomplished but will have no effect on the contract criteria itself.

There are three important considerations regarding the government's oversight function. First, when more than one contract requirement exists for protection of CUI, a method of resolving possible conflicts within the invoked requirements must be considered. Oversight personnel should consider the contractual merits of each requirement and may develop an opinion on which criteria should govern, but the final authority in such cases resides with the contracting officer.

The second point concerns implementing guidance. Reference (pp), USD(I) letter of 17 May 2018, Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base, designates the Defense Counterintelligence and Security Agency (DCSA) as the lead agency for developing a plan for Defense Industrial Base cybersecurity oversight and implementing procedures. It is a complicated issue, however, due to the large number of

DoD contractors with CUI-containing IT systems and the variety of contract administration offices with oversight responsibility. Additionally, DFARS 252.204-7012 is a relatively new requirement (October 2016) which suggests that it will take some time for government oversight procedures to fully develop. Unfortunately, the threat of CUI compromise exists now, as does the large number of contracts already issued with CUI protection requirements invoked. This section, therefore, provides interim guidance to the SUPSHIP community until additional details become available. Note also that the contractor's responsibilities are limited to what is specified in the contract. In some cases, particularly for long-duration contracts such as those associated with ship construction, the contract may identify requirements that are superseded by newer references issued subsequent to contract award. Unless a contract change is made invoking the newer requirement, it is the original reference cited in the contract that establishes the contractor's responsibilities. For this reason, it is a good practice to maintain copies of older references that are cited in contracts.

The third point is risk management. Just as the government program for internal control of CUI is based on risk management, so too is any required contractor CUI control program. There are provisions for contractors to deviate from contractually invoked requirements, provided they can show the requirement is not applicable or their program has alternate but equally effective methods for CUI security. The system for consideration is outlined in DFARS 252.204-7012 paragraph (b)(2)(ii).

DFARS 252.204-7012 paragraph (b)(2)(i) invokes reference (qq), NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, but allows exceptions to some provisions when approved by a designated government official. NIST SP 800-171 also contains some caveats which must be considered when developing oversight criteria. For example, under most circumstances a nonfederal partner having CUI stored, processed or transmitted by their IT systems are limited to assuring the security objective of confidentiality (i.e., a nonfederal partner is not required to directly address integrity and availability in their planning effort unless the contract specifically requires it). Since there are different versions of NIST SP 800-171, knowing which version is applicable to the contract invoking DFARS 252-204-7012 is important. As with all command contract oversight efforts, the assigned personnel must limit their efforts to criteria invoked within the contract or cited documents and avoid using the standards applicable to government systems. or versions of requirement documents which are dated after the contract is signed or otherwise not applicable, unless the contractor elects to use a later (or earlier) version if that option is available within the contract.

16.7.4 Training

The command oversight agent for contractor CUI security and confidentiality shall include in the training and qualification requirements for each billet the subjects necessary to accomplish contractor oversight effectively and lay out a schedule for satisfying both one-time and recurring requirements. Retention and maintenance of qualifications in the IT technical areas is necessary to establish credibility with contractor personnel performing the CUI security/confidentially functions within that organization. Also necessary are skillsets for contract oversight, including auditing, claims avoidance, SUPSHIP operations, records

management, risk management, and Technical Support Management (TSM) software. For the case of TSM, one-time training is required for the use of this application.

16.7.5 Introducing IT Oversight in New or Modified Contracts

For many contractors, (and subcontractors), government oversight of their internal IT processes will be a new experience. Government personnel assigned to this oversight role should prepare a plan of action and approach their shipbuilding or ship repair contractor counterparts to confirm that the contractor understands the requirements and options, to discuss guidelines governing how the process will be conducted in a manner designed to be most efficient for both parties, to identify how results will be disclosed during or soon after each oversight event, and to discuss the method for resolving issues that may be identified during the process. Flow-down of requirements to impacted subcontractors should be included in the discussion. Prior to engaging with the contractor, government participants should reacquaint themselves with the contractual issues such as actions to avoid claims and constructive changes (see SOM 3.13.3.2.4, Constructive Change Orders).

16.7.6 Methodology for IT Oversight

The approach used for oversight of contractor covered systems is modeled after the SUPSHIP Contract Administration Quality Assurance Plan (CAQAP), addressed in SOM chapter 9. The CAQAP employs the following seven elements to provide a systematic program for ensuring compliance with contract requirements:

- Planning
- Document Review
- Procedures Evaluation (PE)
- Product Verification Inspection (PVI)
- Quality Audits
- Corrective Action
- Quality Data Evaluation (QDE)

These same elements are employed for contractor IT oversight, modified as appropriate for this specific application.

16.7.6.1 Planning for Oversight and Implementation

The objective of contractor IT oversight planning is the efficient and economical application of resources to ensure effective oversight of the shipbuilder's compliance with contractually invoked cybersecurity requirements. The goal is to identify and bring about correction of deficiencies in the shipbuilder's network security before CUI information is compromised. Risk-based planning is encouraged.

When the command is administering a contract that contains requirements for protection of CUI, the assigned organization must develop and maintain a program that will adequately monitor the shipbuilder's IT efforts as they relate to CUI security requirements. The oversight

plan must be reviewed on a scheduled basis and, if necessary, modified to accommodate changes in contract language or the results of oversight data or other security indicators. The review and any changes to the oversight plan shall be documented. NAVSEA 04Z (SUPSHIP Management) sponsors a centralized software program, Technical Support Management (TSM), designed to facilitate documentation of contract oversight efforts. Shipbuilding contractors have the opportunity to receive, process, and respond to Corrective Action Requests (CARs) using TSM, which benefits both parties by reducing paperwork and expediting resolutions.

At a minimum, the oversight plan shall include processes for:

a. Review of contracts, modifications and related documents to determine requirements for contractor performance in control and security of processes and information systems containing or otherwise touching CUI.

b. Planned distribution of SUPSHIP effort between procedural review, procedural compliance assessment, contract compliance assessment, and, when applicable, subcontract compliance assessment.

c. Evaluation of contractor internal procedures which impact protection of CUI within contractual requirements. The purpose is to ensure the contractor's written procedures are technically adequate and released to the implementing parties in a timely manner. Approval of the procedures by the oversight authority is not required unless the contract specifies otherwise. The results of this phase must be documented in TSM.

d. Observation to ensure the contractor accomplishes work to the requirements of their established procedures. Checklists must be developed to accomplish this phase and results must be documented in TSM.

e. Inspection on a sample basis to validate conformance to contract requirements. The purpose of this effort is to assure that procedures, or steps within the procedures, which may be undocumented, understated, misinterpreted, or deficient in some respect, do not result in a missed opportunity to comply with the intent of the contract CUI protections as a whole. Checklists must be developed to accomplish this phase and results must be documented in TSM.

f. Delegating requirements to the command responsible for contract oversight of subcontractors subject to prime contract requirements who develop, receive, or process CUI. Usually, the command’s Quality Assurance (QA) department issues Letters of Delegation to the government agency assigned oversight responsibility for the subcontractor. An internal agreement between the command IT and QA organizations should be established to complete the delegation process.

g. Documentation of corrective action requested, accomplished and verified when a deficiency or other inadequacy is noted in the contractor's compliance with contract requirements.

Any documented issue that is reasonably assessed by the command ISSM as a serious breach of CUI security, or is likely to gradually compromise CUI security over an extended period of time, should also be reported to affected PMRs and NAVSEA 04I.

Oversight shall include assurance that contractors promptly report events that have a reporting timeline as defined in DFARS 252.204-7012.

If, during oversight, the command ISSM is made aware of a condition which is outside the invoked contract requirements but presents an unacceptable risk to the confidentiality or security of CUI, NAVSEA 04Z should be notified.

16.7.6.2 Document Review

The purpose of document review is to verify that the contractor's documented procedures and technical data comply with contractual requirements. The command will already have processes to evaluate technical data such as ship construction drawings, test procedures and reports or similar information, most of which will be submitted as required by the Contract Data Requirements List (CDRL). Others may be developed by the ship specifications or other invoked requirements. Regardless of the reason for development, the contract will normally have a clause which either allows or requires access to those documents be provided to the administering contract office. The existing processes (or new ones if necessary) should include consideration of CUI control and security. If not already completed, SUPSHIP should:

a. Prepare listings of all contractually required procedures and technical data that identify if government review and/or approval is required.

c. Document all reviews and approvals, including those that do not contractually require government review.

d. Notify the contractor of non-compliant procedures and technical data.

e. Adjudicate items found deficient and follow-up to ensure satisfactory correction.

16.7.6.2.1 Procedure Review

Most contracts require the contractor to develop written procedures for each element of contractor performance that describe how that element will be accomplished. When that requirement exists, SUPSHIP will identify those procedures subject to review based on the degree of risk. Some contracts will require some or all procedures to be submitted as a CDRL for government review and/or approval. Others may not, but usually require that the procedures be made available for review. Procedures for processes which involve CUI, explicitly or indirectly, will be reviewed for conformance to the CUI confidentiality requirements contained in the contract. Procedures are categorized as follows:

Category 1: Procedures for which NAVSEA approval is required by contract. For CUI, these will be rare.

Category 2: Procedures for which SUPSHIP approval is required (commonly submitted by CDRL) or where the contract requires government approval or review.

Category 3: Procedures not falling into Categories 1 or 2, but copies are to be furnished to the SUPSHIP for information, review and comment as time permits.

All Category 1 procedures must be submitted to NAVSEA for technical concurrence. This review includes newly developed procedures and subsequent revisions and changes.

Contractor procedures addressing engineering, manufacturing, quality, SCM and other areas within the contractor's control are usually evaluated by the SUPSHIP departments providing contract oversight in those areas. Frequently, CUI will be located in those procedures to provide technical guidance to their employees during operations. The SUPSHIP process for CUI oversight must consider the most effective method for identifying, recording and communicating CUI issues within the organization and with the contractor.

SUPSHIP shall maintain a list of all contractor procedures that may impact CUI confidentiality required by DFARS 252.204-7012 and other invoked contract requirements. The list, as determined by the local SUPSHIP, will identify the category and track status of approvals and/or reviews. When a contractor does not develop required written procedures or fails to correct inadequate procedures, SUPSHIP may initiate a CAR.

16.7.6.2.2 Technical Data Review

Technical data review is normally performed by SUPSHIP C/200 using the process defined in paragraph 9.3.1.2.2 of this manual. When the technical data submittal has information that qualifies as CUI under the contract requirements, the appropriate controls must be instituted, including any limited distribution statements necessary. This is particularly true when the data contained therein is derived in part or whole from CUI that was provided or made available to the contractor under any contract. An agreement between Code 200 and the command's contractor IT oversight agent should be reached which defines who will document and administer the corrective action when CUI is the issue. At a minimum, the command's contractor IT oversight agent should be aware of the issues as they develop and determine, in the aggregate, if the contractor's overarching CUI cybersecurity system is in control.

16.7.6.3 Procedure Evaluation

Process Evaluation (PE) is the element that verifies that the contractor is complying with the internal written quality procedures, and that the procedures are accomplishing the intended purpose of protecting the security and confidentiality of CUI. PEs are usually conducted by observing the contractor performing the associated process, but with CUI that may be difficult. In the case of CUI, PE can primarily be performed by examining the controls imposed by the process and determining if the expected result was achieved. PEs are associated with process control whereas PVIs are associated with product contract compliance. PEs shall be conducted utilizing checklists or an attribute system. They are to be accomplished as early as possible and periodically throughout the performance of work to confirm the sufficiency and adequacy of the CUI control procedures in operation. Process audits may be used in lieu of PEs when the command determines that is the most efficient method.

Evaluation of new or revised contractor procedures involving CUI and requiring government review or approval (Categories 1 and 2), or other process documentation as identified by the Supervisor, shall be conducted at the time of the contractor's initial publication of the procedure. If unable to perform at that time, the reason or situation will be documented along with a plan for future evaluation. Evaluations should include participating in sufficient examination of the contractor’s operations described by the document to ensure contract requirements are met.

When the length of the contract permits, continuing evaluations of all applicable documents should be scheduled and conducted after the initial evaluation. When a continued evaluation of a document indicates that the contractor is maintaining satisfactory control of quality, the frequency of evaluation may be reduced. When continued evaluation of a process document indicates the contractor is not maintaining control of CUI, appropriate corrective action should be taken and the frequency of evaluation should be increased.

16.7.6.4 Product Verification Inspection (PVI)

Product Verification Inspection is the element that verifies that the end result conforms to contract requirements. For example, if, while using a PVI checklist to record an examination of submitted CDRLs containing CUI, a failure to include the required distribution control statements is found (regardless of whether the contractor’s process required it), the products (CDRLs) should be considered deficient. If the contractor performs penetration testing on their IT system in accordance with an internal procedure, recording that under PE would be appropriate. If the results are made available to the government, recording the results under PVI would be appropriate. PVIs are accomplished by the cognizant SUPSHIP representative by physical examination, verification, and/or concurrent inspection of product content. Product CUI control audits may be used in lieu of PVI in many cases.

PVIs shall be conducted utilizing checklists or an attribute system that is reviewed and updated to account for changes and revised contract requirements (including updated internal procedures, CDRLs, or deliverable documents when the update is a consideration during change negotiation).

Adjustments in the frequency of inspections will depend on nonconformity rates and problem areas that develop. If performing concurrent inspection with the contractor, the government observer should verify results of the examination or test by the contractor, and validate that the contractor’s recorded product inspection results concur with the government’s product inspection results.

16.7.6.5 CUI Control Audits

An audit for control of CUI is the process of systematic examination of an organization’s CUI security/confidentiality function or system. It is an essential management tool for verifying and assessing processes, for determining the effectiveness of achieving defined target levels, for providing evidence concerning the reduction and elimination of problem areas, and for examining compliance with higher level directives.

External audits are the CAQAP element that examines and evaluates the contractor's products, processes, services and systems. Such audits are referred to as "process audits" or "product audits".

Process audits and product audits may be performed to examine and evaluate any CUI process, function, product or entity based on local needs and conditions. These audits may be routine, or may be prompted by significant changes in the contractor's program for protection of CUI, major issues with the contractor's SSP or resulting POA&M, or by a need for follow-up corrective action for previously identified systemic problems.

SUPSHIPs shall have a written procedure for planning and conducting external (contractor) CUI control audits. As a minimum, this procedure shall address:

- Identifying the scope of the audit and any areas of special emphasis
- Preparing an audit schedule after discussions with the impacted contractor
- Issuing a letter to the contractor formalizing the audit schedule
- Selecting audit team members with the requisite knowledge and experience
- Assigning audit team responsibilities
- Establishing documentation requirements for reporting, collecting and compiling audit findings into a final report
- Handling and distribution of a final report
- Follow-up actions

Pulse audits are a specific type of external audit during which the SUPSHIP and contractor concurrently conduct the audit. The purpose of a pulse audit is to ensure that both the SUPSHIP and contractor agree on the findings at the time the audit is conducted. Another benefit of the pulse audit is the opportunity to align CUI control metrics. Consideration of this process requires both parties to agree that the benefits outweigh any difficulties, so it is an option, not a requirement.

16.7.6.6 Documentation and Corrective Action

For consistency, each command should use the documentation and corrective action process described herein where possible. Tailoring details to accommodate the affected contractors is allowed. In all cases, procedures defining oversight implementation are required, as are records of efforts undertaken and results.

Both positive and negative results should be recorded. Where non-compliance with contract requirements is observed, the issue must be documented, reported to the responsible contractor, and resolution requested. TSM provides the mechanism for doing that. TSM is a "cradle to grave" historical record keeping system. Among other capabilities, it has work flow design which controls the rights for assigned participants to originate, change, view, review, approve, release, respond to, evaluate response, refute response, and close corrective action requests, as well as documenting observations and attaching relevant documents. Should any contractor not have a connection to TSM, or decline to use the program, TSM

shall still be used by SUPSHIP but the recorded issues can be printed or otherwise conveyed in a traceable manner to the responsible contractor. In those rare cases where the contract requires a different method for interfacing with the contractor, that method shall be used in addition to TSM (for historical purposes) unless SEA04Z approves avoiding the duplicate effort (in effect, a waiver for the requirement to use TSM).

16.7.6.6.1 Defect Classification

Critical Defect – A direct violation of the contract or invoked documents (contract clauses, FAR, DFARS, invoked NIST Special Publications, NISPOM, UCNI criteria, etc.) which will seriously compromise the security or confidentiality of CUI. Conflicts between contractor procedures and contract requirements can be considered critical when the activity of the contractor in implementing the internal instruction is also in conflict with the contract requirements.

Major (Significant) Defect – A departure from established industry standards or clear violation of contractor developed CUI security processes, procedures or other available instruction which may impact the security or confidentiality of CUI or the systems containing it. Omissions of details in contractor procedures for specific contract requirements which have a high probability of improper CUI controls or inconsistent implementation also fall under this classification.

Minor (Administrative) Defect – Issues such as occasional conflicts within internal contractor procedures involving CUI. Also, the absence of clarity or necessary guidance in contractor procedures involving CUI.

16.7.6.6.2 Defect Notification and Corrective Action Requests (CAR)

Deviations from contract requirements or published internal contractor policies and procedures addressing the program for security or confidentiality of CUI always require recording and most necessitate requesting corrective action. Verification of any corrective actions is also required, as is closing the issue when verification is complete. Some commands may have an agreement with their contractors to recognize any contractor defect documentation as adequate to justify not separately requesting corrective action by the Supervisor when the defect is observed by the government representative. In such cases, the command should still record the defect in TSM, but include in the observation record closing action with the contractor’s defect record ID number as a rationale for not separately requesting corrective action.

The CAR is the method by which the Government informs the contractor of a condition that is not in conformance with contractual requirements. The condition may be a deficient product or a process that may result in a deficient product. The following paragraphs defines the types CARs available in TSM and the criteria for their use.

16.7.6.6.2.1 Type A

Type A CARs will be issued for all detected minor defects. In such cases where the minor deficiency is corrected on the spot, a type A CAR will be initiated and made available to the contractor for information. No contractor response is required for type A CARs when the condition is corrected on the spot. Some commands further subdivide type A CARs into AN and AF. The AN designation is for corrections applied immediately with the CAR closed automatically in TSM. Type AF CARs document issues which require some level of effort by the contractor that can stretch beyond “on the spot” and will remain open until the originator manually closes them in TSM.

16.7.6.6.2.2 Type B

Type B CARs will be issued for all major deficiencies discovered or when a trend of recurring minor deficiencies is detected. Also, when a contractor fails to act on a type AF CAR in a reasonable timeframe, the originator should consider elevating the issue to a type B CAR.

Most critical defects warrant a type C CAR, but some commands may find it more effective to use a type B CAR to initiate the notification and corrective action process if it is within the power of craft level contractor personnel to correct.

16.7.6.6.2.3 Type C

A type C CAR will be issued in the form of formal correspondence to the contractor. A type C CAR will be issued when:

- critical defects are identified that most likely will require contractor management intervention
- previous methods fail to obtain satisfactory results
- severity of the situation warrants

Type C CARs shall be issued when the Supervisor’s delegated authority for signing correspondence has been passed to department heads or other positions within the command. Type C CARs are used to notify the contractor's appropriate level of management that a serious CUI problem exists within their organization and immediate management action must be taken to comply with the provisions of the contract. A copy of each type C CAR shall be furnished to the SUPSHIP contracts department and to SEA 04Z. TSM does not have the same capabilities for type C CARs that it does for type A and B CARs, as the recipient, format, processing and closure differs somewhat among commands. However, TSM provides storage and retrieval capabilities which can be of use for historical purposes.

16.7.6.6.2.1 **Type D**

Type D CARs will be issued in the form of formal correspondence to the contractor. When a type C CAR fails to obtain satisfactory results, or when the severity of the situation warrants, a type D CAR shall be issued by the Supervisor or the contracting officer notifying the contractor's top-level management (usually the president of the company) that a significant CUI security or confidentiality problem exists within their organization and immediate management action must be taken to comply with the provisions of the contract.

A copy of each type D CAR shall be furnished to the SUPSHIP contracts department and to SEA 04Z. TSM does not have the same capabilities for type D CARs that it does for type A and B CARs, as the recipient, format, processing and closure differs somewhat between commands.

16.7.6.6.3 Terminology and Guidance

Correction to Defect is the term used on a CAR to request that a contractor correct an identified non-conformance and provide a response as to the specific actions taken to correct the defect.

Correction to Cause is the term used on a CAR to request that a contractor provide a clear and informative response as to the root cause of a non-conformance and the specific actions taken to prevent reoccurrence.

Type A CARs are limited to correction of defect. Type A CARs will not be used to request correction to cause.

In addition to correction of defect, correction of cause may be used on type B CARs where SUPSHIP has determined that it is warranted. Correction to cause shall be requested when the defect is a result of a systemic problem in the contractor's process, a result of a deficiency in a contractor's procedure, or the defect is determined to be of a recurring nature. When correction of defect and correction of cause are both requested on the same type B CAR, the tendency is to focus on the defect. The correction to cause normally becomes secondary (correction of cause can take more time, and correction of the defect and correction of cause is often assigned to different levels of personnel in the contractor's organization). For that reason, most commands will find it more effective to issue two CARs, one for correction of defect and a separate one for correction of cause, but the option of requesting both on the same CAR exists in TSM and is left to the discretion of the command.

Type C & D CARs typically address significant programmatic issues, usually citing examples of several related defects which warrant asking for correction to cause. However, management is given broad authority to decide what issues and level of detail a type C or D CAR contains.

16.7.6.6.4 CAR Closure

When a type A or B CAR is returned by the contractor, SUPSHIP will evaluate the contractor's response (including elimination of causes to prevent reoccurrence when appropriate) and verify the acceptability of the corrective action taken. If the actions taken by the contractor are determined to be acceptable, SUPSHIP will indicate this on the CAR in TSM and close the CAR. If the contractor's actions are determined to be unacceptable, SUPSHIP will return the CAR to the contractor utilizing TSM for further action.

For type C and D CARs, SUPSHIP will evaluate the contractor's response to assure it addresses each point in the CAR and verify the acceptability of the corrective action taken or promised. If the actions taken by the contractor are immediate and determined to be

acceptable, the command may elect to respond with a letter to the contractor indicating the issue is closed, or utilize some other process for closing that has been coordinated with the contractor. If the response is acceptable but the actions promised will take some time to implement, the command may elect to provide a conditional closing action with the caveat that the issue may be reopened if the actions promised are not fully implemented or prove unsatisfactory. Alternately, the command may choose to leave the issue open until all actions are complete. If the contractor's actions are determined to be unacceptable, SUPSHIP will respond accordingly.

16.7.6.7 Data Evaluation

Data evaluation provides for the collection, evaluation and use of SUPSHIP and contractor data collected or available during the oversight effort. Operating procedures within SUPSHIP will be established to describe the system to be used for collecting, evaluating, maintaining, and using the data.

16.7.6.7.1 Data Selection

At a minimum, the data to be evaluated will include the following:

a. Results of all observations (PR, PE & PVIs) to include a defect rate analysis

b. CARs

c. Results of any audits or surveys

d. Results of critiques, such as may be held after a cybersecurity incident

e. Available contractor data relating to CUI security and confidentially, particularly the SSP, POA&M, internal audits, and DFARS/NIST compliance.

16.7.6.7.2 Data Evaluation

SUPSHIP will evaluate the data individually or collectively at established periodic intervals in order to:

a. Adjust the intensity of application of basic CUI oversight elements outlined in this chapter

b. Provide a basis for acceptance or rejection of resultant products where required

c. Provide a basis for determining contract compliance of a contractor's CUI security and confidentiality program and written procedures

d. Determine effectiveness of contractor's CUI security and confidentiality program

e. Provide a basis for recommending process improvement initiatives to the contractor

16.7.6.7.3 Records

TSM is the designated oversight electronic record keeping system for SEA 04's shipbuilding/repair contract administration field activities. TSM has a number of rule-based work flows for type A and B CARs embedded in it. A help engine is included in TSM to guide

users through the various activity modules available. Each command also has a TSM Operating Guide available which explains how command employees should use TSM.

Unless otherwise stated in applicable directives, records which document oversight of contractor CUI security and confidentiality will be retained and disposed of in accordance with reference (rr), SECNAV M-5210.1, Records Management Manual. Each command has a Records Liaison Officer (RLO) or a position with equivalent functions. When there is a question regarding what is an official record or what retention time is required, contact with the command RLO for assistance.

Appendix 16-A: Acronyms

A&A	Assessment & Authorization (formerly C&A)
ATD	Authorization Termination Date
ATC	Approval to Connect
ATO	Authorization to Operate
C&A	Certification and Accreditation (obsolete term; replaced by A&A)
CA	Certifying Authority (obsolete term; replaced by SCA)
CAO	Contract Administration Office
CAR	Corrective Action Request
CCB	Configuration Control Board
CD	Certification Determination
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CL	Confidentiality Level
ConMon	Continuous Monitoring Plan
COTS	Commercial Off-The-Shelf
CSWF	Cyber Security Work Force
CUI	Controlled Unclassified Information (formerly SBU)
DAO	Delegated Authorizing Official
DIACAP	DoD Information Assurance Certification and Accreditation Process (obsolete process; replaced by RMF)
DADMS	DON Application and Database Management System
DATO	Denial of Authorization to Operate
DCSA	Defense Counterintelligence and Security Agency

DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITPR-DON	Department of Defense Information Technology Portfolio Repository-Department of The Navy
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network (formally GIG)
DON	Department of the Navy
eMASS	Navy Enterprise Mission Assurance Support Service
FAM	Functional Area Manager
FISMA	Federal Information Security Management Act
GIG	Global Information Grid (obsolete term; replaced by DoDIN)
IAC	Information Assurance Controls (obsolete; replaced in RMF by Security Control)
IAM	Information Assurance Manager (obsolete term; replaced by ISSM)
IAO	Information Assurance Officer (obsolete term; replaced by ISSO)
IATO	Interim Authority to Operate
IATC	Interim Approval to Connect
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IG	Inspector General
ISO	Information System Owner

ISCM	Information Security Continuous Monitoring
ISSE	Information System Security Engineer
ISSM	Information System Security Manager (formerly IAM)
ISSO	Information System Security Officer (formerly IAO)
MAC	Mission Assurance Category
NAO	Navy Authorizing Official
NAVSEA	Naval Sea Systems Command
NAVSEAINST	Naval Sea Systems Command Instruction
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSPD	National Security Presidential Directive
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Office of the Chief of Naval Operations Instruction
PM	Program Manager
PMR	Program Manager Representative
POA&M	Plan of Action and Milestones
PPSM	Ports, Protocols, and Services Management
RAR	Risk Assessment Report
RMF	Risk Management Framework
SAP	Security Authorization Package (formerly DIP)
SAR	Security Assessment Report
SBU	Sensitive But Unclassified (obsolete term; replaced by CUI)
SCA	Security Control Assessor (formerly CA)
SCAP	Security Content Automation Protocol

SCTM	Security Requirements Traceability Matrix
SECNAVINST	Secretary of Navy Instruction
SECNAV-M	Secretary of the Navy Manual
SIP	System Identification Profile
SIPRNet	Secret Internet Protocol Router Network
SRR	Security Readiness Review
SSP	System Security Plan (including Security Controls Traceability Matrix)
STE	Security Test and Evaluation (ST&E)
STIG	Security Technical Implementation Guide
SUPSHIP	Supervisor of Shipbuilding, Conversion and Repair, USN
TSM	Technical Support Management
VOIP	Voice Over Internet Protocol