DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-OOO1

IN REPLY TO:

NAVSEAINST 5239.2A
Ser 00I/122
15 Dec 08

NAVSEA INSTRUCTION 5239.2A

From: Commander, Naval Sea Systems Command

Subj: NAVAL SEA SYSTEMS COMMAND (NAVSEA) INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) Federal Information Security Management Act of 2002, Title III of E Government Act of 2002 (PL 107-347)

(b) DoD Directive 8500.01E, Information Assurance (IA) of 24 October 2002

(c) DoD Instruction 8500.02, Information Assurance (IA) Implementation of 2 June 2003

(d) SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy of 20 December 2004.

(e) OPNAVINST 5239.1C, Navy Information Assurance (IA) Program of 8 August 2008

(f) CNSS Instruction 4009, National Information Systems Security Glossary of June 2006

(g) SECNAVINST 5000.2D, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System of October 16, 2008

(h) SECNAVINST 5000.36A, Department of the Navy Information Technology Applications and Data Management of December 19, 2005

(i) DoD Directive 5220.22, National Industrial Security Program (NISP) of September 27, 2004

(j) DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) of 28 February 2006

(k) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management of 15 August 2004

(l) DoD 8570.1-M, Information Assurance Workforce Improvement Program of 19 December 2005

(m) DON CIO message, 291600Z FEB 08, Contingency Plans and Testing

(n) DoDD O-8530.1, Computer Network Defense (CND) of 8

DISTRIBUTION STATEMENT A: Approved for Public Release; Distribution is Unlimited.

Jan 2001

(o) DoDI O-8530.2, Support to Computer Network Defense of 9 March 2001

(p) United States Strategic Command (USSTRATCOM) Directive 527-1, Department of Defense Information Operations Condition (INFOCON) System Procedures of 27 January 2006

(q) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) of 28 November 2007

(r) Intelligence Community Directive (ICD) Number 503, Intelligence Community Information Technology Systems Security Risk management, Certification and Accreditation of 15 September 2008

(s) Commander, Naval Network Warfare Command Letter, Appointment of Designated Approving Authority of 6 February 2008

(t) SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements of 18 March 2008

(u) Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01 of 8 March 2006, CH 3, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)

(v) NAVSEA Instruction 2300.1, Guidance Concerning Use of NAVSEA Communications Systems of 27 June 1997

(w) SECNAV Manual 5510.36, Department of the Navy Information Security Program Manual of June 2006

(x) COMNAVNETWARCOM message, Navy Telecommunications Directive (NTD) 14-07, Personal Digital Assistant (PDA) Policy, DTG 201934Z DEC 07

(y) SECNAV Instruction 5211.5E, DON Privacy Act (PA) Program of 28 December 2005

(z) SECNAVINST 5720.47B, Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites of 28 December 2005

(aa) DoD CIO Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media of 3 July 2007

(bb) DON CIO message, Safeguarding Personally Identifiable Information (PII), DTG 171952Z APR 07

(cc) DON CIO message, Loss of Personally Identifiable

Information (PII) Reporting Process, DTG 291652Z FEB 08

(dd) DON CIO message, Department of the Navy Privacy Impact Assessment (PIA) Guidance, DTG 081547Z FEB 07

(ee) DON CIO Message 161108Z JUL 05, Effective Use of Department of the Navy Information Technology Resources

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

(gg) DON CIO message, DON Public Key Infrastructure (PKI) Implementation Guidance, DTG 061525Z October 04

(hh) Chief of Naval Operations message, Navy Common Access Card (CAC) and Public Key Infrastructure (PKI) Implementation Guidance Update, DTG 0716551Z DEC 04

(ii) COMNAVNETWARCOM message, Navy Telecommunications Directive (NTD) 07-06, Navy Public Key Infrastructure Implementation Plan, DTG 061930Z SEP 06

(jj) DoD Policy Memorandum, "Compliance and Review of Logical Access Control in Department of Defense (DoD) Processes of 24 January 2007

(kk) OPNAV Instruction 3432.1, Operations Security of 29 August 1995

(ll) DoD Instruction 5200.39, Critical program Information (CPI) Protection Within the Department of Defense of 16 July 2008

(mm) DoD 5200.1-R, Information Security Program of 14 January 1997

(nn) Chief of Naval Operations (N614)/Headquarters Marine Corps Policy, Navy-Marine Corps Unclassified Trusted Network Protection (UTNProtect) Policy of 31 October 2002.

(oo) COMNETWARCOM message, Navy Telecommunications Directive (NTD) 09-07, Classified Trusted Network Protection (CTNP) Policy (Firewall) Baseline Settings for Navy SIPRNet Enclaves, DTG 191736Z NOV 07

(pp) DON CIO message, Remote Access to Enterprise Email from Non-DoD Computers, DTG 161957Z OCT 02

(qq) NAVCYBERDEFOPSCOM message, Amplifying Instructions Regarding CAC Enablement for Outlook Web Access, DTG 072051Z DEC 06

(rr) Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG) of 15 November 2007.

(ss) SECNAV Instruction 2075.1, Department of the Navy Use of Commercial Wireless Local Area network (WLAN) Devices, Services, and Technologies of 30 November 2006

(tt) COMNAVNETWARCOM message, Information Assurance Vulnerability Management and Compliance, DTG 222009Z SEP 04

(uu) Virtual SYSCOM Joint Letter, Virtual Systems Command (VSYSCOM) Research, Development, Test and Evaluation (RDT&E) Information Assurance (IA) Architecture and Firewall Policy of 8 July 2008.

1. Purpose. The purpose of this instruction is to provide the basic policy and guidelines necessary for consistent and effective application of resources in ensuring the security and privacy of Naval Sea Systems Command (NAVSEA) systems/information in accordance with the Federal Information Security Management Act of 2002, and Department of Defense (DoD) and Department of the Navy (DON) IA policies and procedures (references (a) through (e).

2. Cancellation. The following documents are hereby canceled: (a) NAVSEAINST 5239.2 of 29 July 1998, (b) Naval Sea Systems Command Information Systems Security Guidance Manual, S0300-CA-GYD-010 of 10 April 1998, (c) NAVSEA Policy Letter 01-09 of 3 July 2001, and (d) NAVSEA Policy Letter 12-02 of 15 April 2002.

3. Acronyms, Definitions, and References. Terms, definitions, and acronyms used in this instruction may be found in references (b), (c) and (f), unless otherwise specified.

4. Objectives. The NAVSEA IA policy shall, consistent with FISMA, DoD, and DON policies and guidance:

a. Provide guidance for implementation of IA protections commensurate with the risk and magnitude of the harm resulting from unauthorized access to, use, disclosure, disruption, modification, or destruction of:

(1) Information collected or maintained by or on behalf of NAVSEA; and

(2) Information systems used or operated by NAVSEA, by a NAVSEA contractor processing Navy information, or by other organizations on behalf of NAVSEA.

b. Establish a methodology to protect the availability, integrity, authentication, confidentiality, and non-repudiation of information systems, including the ability to detect and react to attacks and intrusions, mitigate the effects of incidents, help restore services, and perform post-incident analysis.

c. Identify, train, and certify personnel performing IA functions, including both Government employees and contractor personnel, and regardless of job series or military specialty.

d. Ensure all authorized users of NAVSEA information systems receive initial IA awareness orientation and complete annual IA refresher training.

e. Incorporate IA as a critical component of the life cycle management process.

f. Require NAVSEA information systems and networks that meet the qualification for registration in DoD IT Portfolio Repository (DITPR) to be registered. Registration in DITPR is accomplished by registration in the DON variant of DITPR, known as DITPR-DON, per references (g) and (h) and periodic DITPR-DON guidance issued by DON CIO.

g. Require that all IT under NAVSEA authority that require certification and accreditation (C&A) are certified and accredited.

h. Evaluate NAVSEA IA policies and procedures annually.

i. Require all NAVSEA IT to clearly show all costs related to security considerations.

j. Ensure the use of managed risk analysis in balancing threat against NAVSEA IT and data criticality to identify and implement practical risk reducing solutions.

k. Ensure computer network incident response and reporting.

l. Ensure compliance with DoD vulnerability notification and corrective action process.

5. Scope. This instruction applies to information systems and networks operated by all NAVSEA activities and affiliated Program Executive Offices (PEO) that enter, process, store, or transmit unclassified, sensitive or classified information. This instruction and references (i) and (j) also apply to contractors supporting NAVSEA or PEO activities and contractor owned facilities operating under NAVSEA/PEO authority. This instruction encompasses all information systems (IS) and networks that are procured, developed, modified, operated, maintained, or managed for NAVSEA and affiliated PEO organizational elements.

6. Precedence. Policy and requirements set forth by higher authority take precedence over the policy established in this instruction, except where this instruction is more restrictive. Implementing authorities should identify conflicting policy to the NAVSEA DCIO-IA for resolution.

7. Background. Per references (a) and (e), IA provides the measures taken by an organization to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of its information and information-systems. IA includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Defense-in-depth and Defense-in-Breadth is the NAVSEA preferred security strategy whereby layers of protection establish an adequate security posture for a system and will be implemented throughout the NAVSEA Enterprise. The strategy is based on the concept that attacks that must penetrate multiple protection layers of the system are less likely to be successful. In addition to this layered approach, protection mechanisms are distributed among multiple locations, and each component of defense within the system provides an appropriate level of robustness. Management of risk is the objective of IA in a Defense-in-Depth and Defense-in-Breadth strategy.

Computer Network Defense (CND) embodies incident prevention, detection and response, a critical part of defense-in-depth. CND synchronizes the technical, operational, and intelligence assessments of the nature of a computer attack in order to defend against it.

8. Policy

a. General. All NAVSEA activities shall maintain an aggressive Information Assurance program designed to appropriately safeguard NAVSEA information and resources at all times with respect to confidentiality, integrity, availability, authentication, and non-repudiation based upon mission criticality, level of required information assurance, and classification or sensitivity level of information entered, processed, stored, or transmitted. Safeguarding information technology resources and information shall be accomplished through the employment of defensive layers that include the IA disciplines, as well as sound administrative practices that include budgeting, funding, and executing the actions necessary to protect all IS resources. IA shall be centrally monitored and reported as an element of mission readiness and as a management review item.

b. Local Information Assurance Authority. Commanders, Commanding Officers, Officers in Charge, and Directors of NAVSEA Field Activities are designated as the Local Information Assurance Authority for their command. This authority and responsibility shall not be delegated. The NAVSEA Command Information Officer (CIO) is designated as the Local Information Assurance Authority for NAVSEA Headquarters and affiliated PEOs.

c. IA Personnel, Training, Certification, and Management.

(1) All NAVSEA personnel, government and contractor, performing IA functions must be properly trained and certified as required by reference (k) as implemented by reference (l).

(2) All NAVSEA personnel performing IA functions shall be identified, tracked, and monitored to ensure that IA positions are staffed with trained and certified personnel. All NAVSEA activities shall establish, resource, and implement an IA training and certification program for all IA personnel in accordance with reference (k) as implemented by reference (l).

(3) Per references (k) and (l), statements of work (SOW) and contracts shall identify all IA functions and requirements to be performed by contractor personnel working within NAVSEA/PEO activities.

(4) All authorized users of NAVSEA information systems must complete DoD IA Awareness Training as a condition of access. The Local IA Authority is encouraged to add to the standardized baseline training their local IA policies and procedures. DoD IA training is as follows:

(a) Initial IA awareness orientation and

(b) Annual IA refresher awareness training.

(5) All IA training shall comply with the minimum standards published in references (k) and (l) as applicable to specific job roles.

(6) All NAVSEA personnel, government and contractor, who require privileged access to NAVSEA information systems and networks within NAVSEA/PEO activities must complete a "Privileged Access Agreement" in accordance with references (k) and (l). A sample agreement can be found in Appendix 4 to reference (l). NAVSEA activities may expand the requirements of this agreement to meet their needs.

(7) All personnel assigned to IA positions within NAVSEA/PEO activities shall be certified at the time of their appointment/assignment or become fully certified not later than six (6) months from the date of their appointment/assignment. Temporary waivers to the certification requirements for IA professionals may be requested. Waiver requests must:

(a) Be signed by the Local IA Authority,

(b) Be endorsed by the NAVSEA CIO, who will forward the request to the Operational Designated Accrediting Authority (ODAA),

(c) State what certification the individual is attempting to achieve, and

(d) Address any failed attempts to obtain the certification including the remediation measures being taken to increase the probability of success.

(e) Address any severe operational or personnel constraint issues that prevent meeting the certification requirement.

d. Contingency Planning. Commanders, Commanding Officers, Officers in Charge, and Directors of NAVSEA Field Activities shall develop, test, and evaluate contingency plans (CP) in accordance with reference (c) to describe the interim measures used to recover and restore information technology systems and service operations following an emergency or system disruption.

(1) Per reference (m), information system owners must develop a contingency plan for their respective systems, to be maintained after approval by the Program Office. A CP is required even if the system is not operated by the system owner (e.g., programs of record and type accredited systems).

(2) The contingency plan must provide specific guidance to the command IAM on the system requirements for recovery from a disruptive event or emergency for incorporation into the site's contingency and Continuity of Operations Plan (COOP)

(3) Contingency plans must adhere to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.

(4) Contingency plans must name the system in the plan. The system name must match what is registered in the Defense Information Technology Portfolio Repository/Department of Navy (DITPR-DON), and applicable certification & accreditation (C&A) documentation.

(5) The system user representative, program manager, and Designated Accrediting Authority (DAA) must approve and sign the CP. A separate CP signature page is required and must be maintained with the contingency plan.

(6) CPs shall be exercised at least twice every 12 months for Mission Assurance Category (MAC) I systems, and at least once every 12 months for MAC II and MAC III systems.

(7) Exercises must be realistic; however, a desktop exercise can be used in place of an actual physical exercise.

(8) Exercises must be documented, signed, and dated. Documentation must include the name of the system and must specifically state what was tested and the results. Shortfalls shall be documented and approved by a plan of action and milestones (POA&M). The POA&M shall be maintained to track progress and resolution of identified shortfalls.

e. Information Operations Condition (INFOCON). The Information Operations Conditions (INFOCON) system provides a framework within which commanders can increase the measurable readiness of their networks to match operational priorities. To ensure adequate incident response, Commanders/Commanding Officers of NAVSEA activities shall develop, implement, and manage INFOCONs as required in references (n), (o) and (p). Although higher authority normally prescribes INFOCON, Commanders of NAVSEA activities have the authority to increase INFOCONs in their area of responsibility when the circumstances dictate. Commanders/Commanding Officers of NAVSEA activities shall:

(1) Ensure compliance with all provisions of reference (o) by developing and implementing site-specific INFOCON procedures for executing the INFOCON system within his/her command.

(2) Determine, for purposes of this policy, which information systems and networks under his/her purview are mission-critical and/or mission-essential.

(3) Designate primary and alternate points of contact (POC) that will be responsible for coordinating all INFOCON actions required by reference (o) and by DON operational authorities.

(4) Add INFOCON POC information to the Duty/Watch Officer contact list.

(5) Be ultimately responsible for compliance of his/her command with all INFOCON requirements and be accountable for any and all non-compliance with these requirements.

f. Certification and Accreditation (C&A). All NAVSEA information systems shall be certified and accredited by the appropriate Designated Accrediting Authority (DAA) prior to being placed into operation. Reference (d) requires certification and accreditation of all NAVSEA information systems with the exception of platform IT with no network interconnection to the Global Information Grid. Certification and accreditation of NAVSEA information systems will be in accordance with references (q), as modified by the Navy Certification Authority and DAA, and/or (r), as appropriate. Certification and accreditation activities for platform IT with no network interconnection to the Global Information Grid will be in accordance with the established platform IT process.

(1) Certification is the comprehensive evaluation of the technical and non-technical security features of an information system, and other safeguards to establish the extent that a particular design and implementation meets a set of specified security requirements. The certification process results in a risk-based determination for operational use and accreditation recommendation to the DAA.

(2) Accreditation is the formal declaration by the DAA, in writing or by digital signature, that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

(a) Full accreditation with an Authorization to Operate (ATO) is always the goal for operational systems.

(b) An Interim Authorization to Operate (IATO) is allowed for fielded systems and networks for up to 180 days as deemed appropriate by the DAA. A single extension of the IATO for an additional 180 days may be granted in unusual circumstances.

(c) All IATO and any ATO with IA findings must be accompanied by an IT Security POA&M that documents identified weaknesses and specifies corrective measures, as appropriate. Corrective actions in the IT Security POA&M must be achievable within the authorization period.

(d) An IATO associated with ships under construction may be renewed until the unit is commissioned, tested, and accepted for unrestricted operations.

(e) An Interim Authorization to Test (IATT) is authorized for testing in an operational information environment or with live data for a specified time period, normally 30 to 90 days. IATTs for testing components in a Research, Development, Test and Evaluation (RDT&E) environment may be authorized for longer periods as appropriate. An IATT may be granted by the DAA. An IATT may not be used to avoid ATO or IATO determinations, requirements for authorizing a system to operate, per reference (q).

(3) For information systems developed for shipboard deployment by NAVSEA activities and affiliated PEO, the Developmental Designated Accrediting Authority (DDAA) will be responsible for ensuring completion of the DAA function for these systems during acquisition, development, Test and Evaluation (T&E) and risk mitigation prior to testing or use within the operational Naval enterprise. When a system is ready for connection to an operational network for testing or use, the ODAA will issue an IATT to accept the risk of testing performed in an operational environment. In accordance with reference (s), the DDAA for NAVSEA is the Command Information Officer (CIO).

(4) NAVSEA information systems and networks used for Research, Development, Test and Evaluation (RDT&E) purposes will be accredited by the RDT&E Designated Accrediting Authority (RDAA). In accordance with reference (s), the RDAA for NAVSEA is the Command Information Officer (CIO).

(5) Program Managers (PM) of information systems consisting of a common set of hardware, software, and firmware and intended for installation at multiple shipboard and/or shore based locations will prepare and submit type accreditation documentation to the appropriate DAA. A type accreditation allows for the installation of identical systems at multiple locations based on the validation of all the IA controls at one representative site.

(6) Information systems developed at one NAVSEA site for installation and operation at a different NAVSEA site must be fully accredited prior to installation and operation at the operational location. PMs will ensure an accreditation statement from the appropriate DAA is provided to the operational site at the time the information system is delivered for installation at the operational site.

(7) Plans of Action and Milestones (POA&M). Commanders, Commanding Officers, Officers in Charge, and Directors of NAVSEA activities and Program Managers shall develop an IT Security POA&M for IT systems under their control in accordance with reference (q). The purpose of the POA&M is to assist NAVSEA activities in identifying, assessing, prioritizing, and monitoring the progress of tasks and schedule necessary to resolve identified security weaknesses in programs and systems. The IT Security POA&M is a permanent record. Once posted, weaknesses will be updated, but not removed, after correction or mitigation actions are completed. Inherited weaknesses are reflected on the IT Security POA&Ms. IT Security POA&Ms may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. Activity CIOs are responsible

for monitoring and tracking the overall execution of system-level IT Security POA&Ms until identified security weaknesses have been closed and certification and accreditation documentation appropriately adjusted. The DAAs are responsible for monitoring and tracking overall execution of system-level IT Security POA&Ms. The PM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the DAA and the CIO.

g. Computer Network Incident Response and Reporting. Reference (t) defines an incident as an assessed occurrence having actual or potentially adverse effects on an information system. This includes, but is not limited to, attempted entry, unauthorized entry, malicious code execution, and/or an information attack on an information system.

(1) Commanders, Commanding Officers, Officers in Charge, and Directors of NAVSEA activities shall provide local monitoring of NAVSEA networks when central monitoring by the Navy Cyber Defense Operations Command (NCDOC) or the High Performance Computer Program Modernization Office (HPCMO) (for RDT&E networks using DREN) is not feasible. These Commanders shall ensure timely handling of signature threshold alerts, updates, and audit records/log files per reference (u).

(2) Response to and reporting of computer network incidents on information systems at NAVSEA activities will be in accordance with reference (t). Additionally, all computer network incidents on information systems at NAVSEA activities shall be reported to the NAVSEA Deputy Command Information Officer for IA as soon as possible following occurrence of the incident.

(3) If the NAVSEA information system contains sources and methods intelligence (SAMI), then audit records/log files shall be retained for five years. Otherwise, audit records shall be retained for one year, per reference (c), unless advised otherwise by legal counsel or Naval Criminal Investigative Service (NCIS).

h. IA Compliance Audits/Inspections and Assessments.

(1) A program of compliance audits/inspections of NAVSEA Activities to ensure compliance with DoD and DON IA policies as well as compliance with this instruction shall be implemented by the NAVSEA CIO in concert with the NAVSEA Inspector General (IG).

(2) Commanders/Commanding Officers of NAVSEA activities shall, in their role as Local IA Authorities, continuously assess the effectiveness of their Defense-in-Depth IA strategy

implementations within their commands, to include their subordinate activities. There are a wide variety of programs and services to evaluate the vulnerability of IT including: online surveys, self-assessment checklists, utilizing available training assist visits, vulnerability assessments, and site assistance visits.

i. Copyrighted Software. Copyrighted software will not be reproduced within NAVSEA, except as authorized within existing legal requirements. Personal accountability shall be enforced for all violations of copyright laws or licensing agreements.

j. Internet, Intranet and E-mail Services. Internet, Intranet and e-mail services shall be used in accordance with reference (v).

k. Privately Owned Hardware and Software. The use of privately owned hardware and software is prohibited unless approved by the requester's immediate supervisor and the organization/activity Information Assurance Manager (IAM). The processing of sensitive and classified information on privately owned resources is prohibited.

l. Boundary Defense. All NAVSEA networks shall be protected by boundary defense mechanisms to limit unauthorized access to NAVSEA information. NAVSEA networks that do not employ the use of a centrally managed enterprise boundary defense service shall maintain those services in accordance with the Unclassified Trusted Network Protection (UTNP) Policy (reference (nn)) or the Classified Trusted Network Protection (CTNP) Policy (reference (oo))for unclassified and classified networks respectively. Firewalls protecting RDT&E information systems shall be in accordance with the RDT&E baseline firewall settings policy, reference (uu). Boundary defense management shall be under the control of the organization’s IAM.

m. Electronic Spillages. An electronic spillage is defined as data placed on an IT system possessing insufficient security controls to protect the data at the required classification (e.g., SCI spillage onto TS, TS spillage onto Secret, Secret onto unclassified, etc.). This term also includes, but is not limited to situations in which Controlled Unclassified Information (CUI), such as Unclassified Naval Nuclear Propulsion Information (U-NNPI), is introduced to non-U-NNPI hardware.

(1) Employees of NAVSEA activities that originate an electronic spillage shall:

(a) Report the spillage to their Command Security Manager (CSM) to ensure proper handling and reporting of all potential compromises of classified information. This will include actions to initiate a Preliminary Inquiry (PI) required by reference (w) and coordination with the Original Classification Authority (OCA) for a classification determination to verify whether or not an electronic spillage has occurred.

(b) Coordinate with the Information Assurance Manager (IAM) to preclude further dissemination of the spillage, report the spillage as required by established Navy electronic spillage policy, and initiate spillage clean up actions as appropriate.

(2) Employees of NAVSEA activities who receive or are affected by an electronic spillage shall:

(a) Report the spillage to their Command Security Manager to ensure proper handling and reporting of all potential compromises of classified information.

(b) Coordinate with the Information Assurance Manager (IAM) to report the electronic spillage as required by established Navy electronic spillage policy.

(3) The CSM shall:

(a) Gather initial information about the spillage sufficient to initiate a PI.

(b) Pass the initial information to the IAM for initial reporting to COMNETWARCOM and gathering of additional information about affected users and IT assets.

(c) At the completion of the PI, request a classification determination from the OCA. Once the classification determination is made, report the determination to the IAM and COMNETWARCOM as required by established Navy electronic spillage policy.

(4) The IAM shall:

(a) Using initial information gathered by the CSM, make an initial report of the electronic spillage as required by established Navy electronic spillage policy.

(b) Gather additional information about affected users and IT assets for further electronic spillage reporting.

(c) Acknowledge receipt of the Electronic Spillage Situation Report (SITREP) issued by COMNETWARCOM and report additional information gathered about affected users and IT assets.

(d) Ensure the spillage is eliminated from all Navy networks as quickly as possible in accordance with established Navy policy.

n. Portable Electronic Devices (PED). Portable Electronic Device (PED) is a generic title used to describe the myriad of small electronic items that are widely available for purchase. PEDs and wireless systems include, but are not limited to, Personal Digital Assistants (PDAs) and other mobile computing devices, Mobile Telephony Devices, Pagers (including those with e-mail capabilities), Digital cameras (still and video), analog and digital sound recorders, Wireless computers and networks.

(1) The use of PEDs in NAVSEA work environments shall be in accordance with reference (rr).

(a) No PEDs shall be brought into a Sensitive Compartmented Information Facility (SCIF), except where specifically authorized in writing by the cognizant DAA. Such authorization shall include the requirement to disable the infrared (IR) and radio frequency (RF) capabilities of the PED before it is brought into the SCIF.

(b) Personally owned PEDs are not authorized for use at any NAVSEA facility or on any NAVSEA network unless specifically authorized in writing by the Local IA Authority. This is to minimize the risk of inadvertent capture of controlled information by a personal PED, since the only approved method of "sanitizing" most PEDs is physical destruction.

(c) Unless equipped with an approved application (e.g., Password Keeper for the Blackberry), PEDs will not be used to store passwords or personal identification numbers (PIN). PEDs will not be used to store safe or door combinations or classified information.

(d) With the exception of approved laptop computers, PEDs will not be used for processing of Naval Nuclear Propulsion Information (NNPI).

(e) All wireless communication systems must be certified and accredited in accordance with reference (q). Pilot projects must implement appropriate security requirements and processes during the development of the system.

(f) PEDs shall be configured with appropriate security settings prior to being issued to users.

(g) PEDs shall not be used for classified information processing unless specifically authorized in writing by the cognizant DAA. PEDs authorized for classified information processing shall meet the requirements of subsection 3.7.2 of reference (rr)

(h) PEDs without Identification and Authentication capabilities built-in or added to the system shall be used only for administrative tasks, such as maintaining appointment calendars and non-sensitive contact lists.

(i) Where feasible, PEDs shall employ up-to-date signature files that are used to profile and identify viruses, worms, and malicious code. As proven anti-virus clients for PEDs become available, these clients shall be deployed to the greatest extent in all PEDs that connect to the network.

(j) Personal Area Networks (e.g., Bluetooth) may be operated in NAVSEA network environments provided they comply with the security requirements of subsection 2.3.2 of reference (rr).

(k) PEDs that use commercial Wireless Local Area Network (WLAN) devices, services, and technologies shall comply with reference (ss).

(2) Personal Digital Assistants (PDA). The use of PDAs in NAVSEA work environments shall be in accordance reference (x). Additionally in accordance with reference (rr), PDA hot-sync operations must meet the following conditions:

(a) The hot-sync management software uses some form of access control (e.g., user password is entered before a hot-sync operation can be executed).

(b) The user disables wireless operations when a PDA is connected to the DoD wired network via a hot-sync or other interface cable.

(c) PDAs that transmit, receive, store, or process DoD information are not synced to home or personally owned PCs.

(3) Per reference (aa), all unclassified DoD data at rest that has not been approved for public release and is stored on PEDs shall be treated as sensitive data and encrypted using commercially available encryption technology. Only DON-approved enterprise DAR products may be used.

o. Use of Removable Storage Media. This policy applies to any removable storage media that can be connected to a Navy network, workstation or other computing device via cable, universal serial bus (USB), Firewire (IEEE 1394), I-link, infrared, radio frequency, personal computer memory card international association (PCMCIA), or any other external connection that would allow data to be transferred and removed. Examples of removable storage media include, but are not limited to zip drives, floppy diskettes, recordable and re-writeable compact disks (CD), recordable and re-writeable digital video disks (DVD), USB flash digital media devices (thumb drives), memory sticks/cards, PC card storage devices of all types, and mini external hard drives.

(1) Removable storage media on classified computing devices:

(a) Due to the inherent risks associated with removable storage media, ensure limited use of USB ports on computing devices that process classified material to the maximum extent possible.

(b) Approval of the Local IA Authority shall be obtained, in writing, where USB use is required for specific classified computing devices. USB devices connecting to classified networks shall be safeguarded in accordance with reference (w).

(c) Connecting any removable storage media to a classified IT system or network will make the storage device permanently classified at the same level as the system. Exceptions to the rule are for devices that are physically locked to read only and when following established Navy file transfer procedures. Finalized compact disk - recordable (CD-R) is considered read only.

(2) General use:

(a) Use of removable storage media on Navy networks will be limited to those who have an operational necessity to use the device. Where this requirement applies, commands will make every effort to provide government furnished storage devices. These devices shall provide the capability to encrypt data stored on them using commercially available encryption technology. Only DON-approved enterprise DAR products may be used.

(b) Personally owned removable storage media for use on classified networks is prohibited.

(c) Personally owned removable storage media for use on systems processing naval nuclear propulsion information (NNPI) is prohibited.

(d) Personally owned removable storage media for use on unclassified networks (i.e. non U-NNPI) is not authorized for official business and is subject to the requirements of this policy.

(e) All flash media devices must first be scanned for malicious code immediately upon accessing a Navy network and/or workstation. If antivirus scanning software is not configured to automatically scan all files when accessed, procedures must be implemented to ensure personnel manually scan media for malicious code.

(f) Removable storage media affected by an electronic spillage will be surrendered to the command Information Assurance Manager or Command Security Manager immediately until properly sanitized. Media that cannot be sanitized will be rendered unusable and destroyed in accordance with reference (w).

(g) All removable storage media shall be labeled with the highest overall classification level using the appropriate label (Standard Form 706, 707, 708, 709, 710) and include the abbreviated form of all applicable warning notices and intelligence control markings of the information contained therein. When the approved standard form labels are not feasible due to interference with operation of the system, size of the media, etc., other means for marking may be used so long as they appropriately convey the classification and other required markings.

(h) Immediately report to the Command Security Manager if any removable storage media containing classified or Controlled Unclassified Information is lost or stolen.

(i) Per reference (aa), all unclassified DoD data at rest that has not been approved for public release and is stored on removable storage media shall be treated as sensitive data and encrypted using commercially available encryption technology. Only DON-approved enterprise DAR products may be used.

p. Protection of Sensitive Information. Commanders, Commanding Officers, Officers in Charge, and Directors of NAVSEA activities shall ensure sensitive information is protected in accordance with references (b), (y), (z), and (aa).

(1) Protection of Personally Identifiable Information (PII). Commanders, Commanding Officers, Officers in Charge, and Directors of NAVSEA activities shall ensure that all NAVSEA-owned or authorized information systems comply with privacy and security requirements of references (y), (bb), (cc), and (dd). As such, Commanders/commanding officers of NAVSEA activities shall:

(a) Ensure that any laptop computer, mobile computing device or removable storage media that processes or stores a compilation of electronic records containing PII on 25 or more individuals on a single device (or less than 25 individuals where the data owner identifies a requirement for additional protective measures) is restricted to DoD owned, leased, or occupied workplaces. When compelling operational needs require removal from the workplace, the laptop computer, mobile computing device or removable storage media shall:

1. Be signed in and out with a supervising official designated in writing by senior leadership.

2. Be configured to require certificate based authentication for log on (for laptop computers and mobile computing devices where possible).

3. Be set to implement screen lock, with a specified period of inactivity not to exceed 15 minutes (for laptop computers and mobile computing devices where possible).

4. Have all PII stored on, created on, or written from laptop computers, mobile computing devices and removable storage media as applicable encrypted (minimally using NIST-Certified, FIPS 140-2). A DoD enterprise solution is being developed for encrypting all stored data. As an interim solution, WinZip 9.0 and above, which is available on most desktops, provides the required encryption protection using FIPS-197 certified advanced encryption standard (AES). WinZip passwords should be at least nine characters long and contain the following: an upper case letter, a lower case letter, a number, and a special character. Passwords should not have sequential numbers, contain any dictionary words, or contain your first or last name. WinZip encrypted files may be stored on system hard disks or transferred to external storage media as required. Users need to be aware that when WinZip is used to encrypt a file, a new encrypted file is created and the original file remains unaltered on the resident device. In some cases this original unencrypted file should be deleted to maintain security of the PII (e.g., when WinZip is used to encrypt a file on a thumb drive or other removable storage media).

(b) Storage of any form of PII is prohibited on personally owned computers (to include laptops), mobile computing devices and removable storage media.

(c) Laptop computers, mobile computing devices, and data stored on removable storage media must be password protected. Passwords should be at least nine characters long and contain the following: an upper case letter, a lower case letter, a number, and a special character. Passwords should not have sequential numbers, contain any dictionary words, or contain your first or last name.

(d) Ensure that all PII not explicitly cleared for public release is protected according to Confidentiality Level Sensitive, as established in reference (c). Additionally all owners of NAVSEA or Navy data shall conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing.

(e) Ensure that any mobile computing device containing electronic PII records removed from protected workplaces conforms to the procedures outlined in references (y) and (aa).

(f) Ensure that any known or suspected loss of PII is reported per the procedures and timelines outlined in reference (ee).

(g) Ensure Privacy Impact Assessments (PIA) are completed for all information systems that require a PIA per reference (ff). Designate a Command Representative assigned responsibility for completing and submitting required PIAs.

(2) Protection of Data at Rest (DAR). Per reference (aa), all unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, shall be treated as sensitive data and encrypted using commercially available encryption technology. Only DON-approved enterprise DAR products may be used.

q. Aggregation of Data on Unclassified Networks and Systems. Commanders, Commanding Officers, officers in Charge, Directors, and Program Executive Officers of NAVSEA/PEO activities must be alert to the compilation or aggregation of unclassified data in systems and networks that would render the data sensitive or even classified in the aggregate. If aggregation of data results in sensitive information, the information should be moved to protected systems. If the aggregation of data becomes classified, the classification authority should be notified and the data moved to the appropriate network. Paragraph 6-19 of reference (w) applies.

r. Annual Reviews and Tests

(1) All information systems must undergo annual information security reviews per references (a) and (c).

Corrective action shall be taken to address shortfalls identified. If an ATO or IATO is awarded during the year, this suffices for the annual review. However, in succeeding years, systems must be reviewed for any changes that could affect the accreditation. Completion of the review must be noted in the FISMA section of the DITPR-DON, and fall within 12 months of the previous completion date.

(2) Security controls for every information system must be tested at least annually per reference (c). Completion of the testing must be noted in the FISMA section of the DITPR-DON, and fall within 12 months of the previous completion date.

s. Information Assurance Vulnerability Management (IAVM). The IAVM process is designed to provide positive control of the vulnerability notification and corrective action process in DoD. Commanders/Commanding Officers of NAVSEA activities shall comply with the IAVM process and report IAV compliance to the appropriate Combatant Commander and the NCDOC per references (u), (n), (o), and (tt).

t. Use of Commercial E-Mail and other commercial Internet services. Per reference (ee), auto-forward of official e-mail to a commercial account or use of a commercial e-mail account for official government business is prohibited, except for as provided in reference (u). References (kk) and (ll) describe Navy and DoD policies and processes for the identification, control, and protection of critical information that indicates or reveals U.S. capabilities and activities, especially in system acquisition programs. NAVSEA personnel are therefore advised that the use of non-DoD Internet services, such as Google Calendar, hotmail.com, palm.net, chat rooms, etc. for the conduct of official NAVSEA business is prohibited.

u. PKI. Commanders/Commanding Officers of NAVSEA activities shall enable NAVSEA information systems, including networks, e-mail, and web servers, to use certificates issued by the DOD PKI and approved external PKIs as appropriate, to support authentication, access control, confidentiality, data integrity, and non-repudiation, per references (c), (n), and (ff) through (ii). Per reference (jj), PKI authentication does not eliminate the need to properly configure mandatory/discretionary access controls on private web servers, web-based systems and applications, and web portals for making authorization decisions.

(1) Software Certificates. PKI software certificates, when improperly installed, stored, or maintained, may introduce vulnerabilities to DON networks. Use of software certificates should be avoided whenever a PKI hardware-token alternative exists. This does not preclude the use of software certificates

related to the DoD External Certificate Program, device/server software certificates, and software certificates used for group/role based functions.

(2) Digital Signature. Commanders/Commanding officers of NAVSEA activities shall ensure e-mail messages requiring either message integrity or non-repudiation are digitally signed using DoD PKI. This includes email that directs/tasks or passes direction/ tasking, requests or responds to requests for resources, promulgates organization position/information external to the organization (division, department, command), discusses any operational matter, discusses contract information, financial or funding matters, discusses personal management matters, where the need exists to ensure that the email originator is the actual originator, and where the need exists to ensure that the email content has not been tampered with in transit. All e-mail containing an attachment or embedded active content (e.g. Hyperlink to a URL or active code) must also be digitally signed. Non-clickable pure text references to web addresses, URLs, or e-mail addresses do not require digital signature. Additionally, personal or non-official e-mail should not be digitally signed.

(3) Encryption. Local IA Authorities and Program Executive Officers of NAVSEA/PEO activities shall ensure that sensitive information, as defined by reference (c), and Controlled Unclassified Information, as defined in Appendix 3 of reference (mm), contained in either email or web server transactions is encrypted using DoD PKI. This provision also applies to any email that discusses any matter that may serve as an operations security (OPSEC) indicator.

v. Use of IT Assets While on Travel

(1) While IT enables us to quickly and effectively transport and exchange information, the risk to Navy IT assets is significantly greater overseas/OCONUS. Foreign intelligence services, criminal organizations, and terrorists can gain sensitive information by actively monitoring all forms of electronic communications. While most of these efforts are focused on simple intelligence collection, some of the information collected could potentially pose a threat to Operations Security (OPSEC) and Personal Security.

(2) All NAVSEA government and contractor personnel have the inherent responsibility to continually promote safe, effective, and legal use of all information resources. NAVSEA government and contractor personnel must:

(a) Exercise the highest standards of professionalism and responsible behavior with the information they obtain from or make available on the Internet and during e-mail communications; and act to protect the interests of national security.

(b) Exercise caution and protect information which could be used to harm the security interests of the United States by unfriendly foreign governments, criminal, foreign intelligence, terrorist organizations, or similar individuals and operatives.

(c) Minimize the risk of unauthorized access by traveling with only the minimum required computer assets and data.

(d) Abide by the requirements set forth in the System Authorization Access Request (SAAR) to ensure the integrity, safety, and security of Navy IT resources, including data.

(e) Keep in mind that they have no assurance of privacy in their use of a computer system/laptop when connected to the Internet, especially overseas; and when connected to the Internet and using e-mail, this connection is subject to monitoring, interception, accessing, and recording.

(f) Notify your chain of command, the site Security Office, and NCIS as soon as possible in the event of any loss of control over, compromise of IT assets or suspicious activity.

(3) When overseas/OCONUS on official government travel, NAVSEA employees may not:

(a) Use a non-DoD computer for official business or Outlook Web Access unless specifically approved by the Local IA Authority in accordance with references (pp) and (qq).

(b) Use a DoD flash/thumb drive or any portable/removable DoD media to connect to a non-DoD computer.

(c) Store and/or transport government data on personally owned or foreign-supplied portable/removable media.

(d) Use or access personal e-mail accounts for official government business.

(4) Personnel returning from overseas/OCONUS travel will coordinate with the command IAM or IT Help Desk to schedule:

(a) A vulnerability and virus scanning for IT assets used while on travel prior to reconnecting the asset to any Navy network.

(b) Remediation assistance, if necessary, for asset with identified vulnerabilities. Assets with identified vulnerabilities will be remediated prior to reconnecting the asset to any Navy network.

(5) Local IA Authorities shall limit the transport and use of IT devices overseas/OCONUS to reduce the overall risk to the Navy.

(6) NAVSEA personnel traveling overseas/OCONUS shall:

(a) Immediately report to the command Information Assurance Manager (IAM) the loss of control for any period of time, of a DoD IT asset, whether by loss, theft, confiscation, temporary misplacement, or the like.

(b) Consult/notify the command IAM whenever necessary to obtain proper guidance for computer security issues.

9. Responsibilities

a. The NAVSEA Command Information Officer (CIO) shall:

(1) Act as the Local Information Assurance Authority for the NAVSEA Headquarters activities and affiliated PEOs. In this capacity through the CIO staff:

(a) Establish and implement security mechanisms and procedures to ensure that information entered, processed, stored, or transmitted by NAVSEA information systems is adequately protected with respect to confidentiality, integrity, availability, and privacy.

(b) Monitor, detect, isolate and react to intrusions that could impact system and/or mission accomplishments.

(c) Implement procedures for reporting identified and/or suspected information system security violations.

(d) Develop and implement local policy and procedures to support effective employment of anti-virus software and a Host Based Security System (HBSS) tool. The DoD-licensed anti-virus software and HBSS tool should be used where it is feasible.

(e) Develop an approved connection process for remote access to NAVSEA systems and networks based on user needs.

(f) Implement policy whereby information on the NAVSEA Internet site is reviewed and approved by appropriate authorities prior to posting to ensure that all information will be protected commensurate with the sensitivity level of the information.

(g) Ensure initial security awareness training is provided for all newly assigned personnel involved in the management, use and/or operation of NAVSEA information systems. Training shall be conducted prior to issuance of networks and information system access authorization and tailored to the responsibilities of the position.

(h) Ensure annual security awareness training is provided for all personnel involved in the management, use and/or operation of NAVSEA information systems. Training shall be tailored to the responsibilities of the position.

(i) Ensure all NAVSEA information systems are accredited for operation at least once every three years or when changes occur that affect the security posture of the system. This can be accomplished for each system, group of systems and/or configuration.

(j) Maintain an Information Systems Accreditation Schedule (ISAS).

(k) Ensure all personnel performing IA functions are identified and tracked as members of the IA Workforce, and monitored to ensure they are properly trained and certified as required by reference (k) as implemented by reference (l).

(2) Have oversight responsibility for the security of all Information Systems throughout the Naval Sea Systems Command and associated PEOs.

(3) Act as the Developmental Designated Accrediting Authority (DDAA) and RDT&E Designated Accrediting Authority (RDAA) for all NAVSEA systems whether or not they are connected to an operational Navy network.

(4) Appoint in writing an Information Assurance Program Manager (IAPM) for NAVSEA.

(5) In coordination with the NAVSEA Inspector General, maintain and manage a robust program for IA audits and inspections.

b. The Deputy Commander for Nuclear Propulsion (SEA 08), who is also the Deputy Assistant Secretary for Naval Reactors within the Department of Energy, shall implement all policy and practices pertaining to this instruction under his cognizance. The Deputy Director Naval Nuclear Propulsion Program shall:

(1) Designate a DAA for the Naval Nuclear Propulsion Program,

(2) Designate a Naval Nuclear Propulsion Program IAM and

(3) Have oversight responsibility for the security of all Information Systems throughout the Naval Nuclear Propulsion Program.

c. Program Managers shall:

(1) Exercise the appropriate life cycle management practices to ensure their programs receive the proper Information Assurance certification and accreditation.

(2) Ensure that Navy information entered, processed, stored, or transmitted by information systems located at contractor sites is adequately protected with respect to confidentiality, integrity, availability, and privacy in accordance with this instruction and applicable DoD and DON policies.

(3) Ensure information systems operated on their behalf at contractor sites are certified and accredited by the appropriate DAA before being placed into operation and at least once every three years or when changes occur that affect the security posture of the system in accordance with this instruction and applicable DoD and DON policies.

(4) In coordination with SEA 02 or other contract management activity, ensure applicable Federal Acquisition Regulation (FAR) and Defense FAR (DFAR) supplement standard clauses are included in contracts for information technology systems and services. Additionally, ensure that such contracts identify this instruction and all applicable DoD and DON IA policies as references.

(5) Ensure Memoranda of Agreement/Memoranda of Understanding (MOA/MOU) are established, coordinated, and signed with all personnel outside the Program Management Office (PMO) designated into IA positions (e.g., IAM, IAO, etc.) for information systems supporting PMO programs.

d. The Commanders/Commanding Officers of NAVSEA Field Activities shall:

(1) Act as the Local IA Authority for their activities. The responsibility of the Local IA Authority may not be further delegated. No individual other than the Commander/ Commanding Officer may act for the Local IA Authority in their absence without the prior approval of the NAVSEA CIO.

(2) Appoint in writing, an Information Assurance Manager (IAM), Information Assurance Officers (IAO), and all personnel who perform functions of privileged access per reference (c). Maintain a current list of appointments with the NAVSEA DCIO-IA.

(3) Establish and implement security mechanisms and procedures to ensure that information entered, processed, stored, or transmitted by NAVSEA information systems is adequately protected with respect to confidentiality, integrity, availability, and privacy.

(4) Ensure that physical security measures are appropriate to protect NAVSEA information and resources.

(5) Monitor, detect, isolate and react to intrusions that could impact system and/or mission accomplishments.

(6) Implement procedures for reporting identified and/or suspected information system security violations.

(7) Develop and implement local policy and procedures to support effective employment of anti-virus software and a Host Based Security System (HBSS) tool. The DoD-licensed anti-virus software and HBSS tool should be used where it is feasible.

(8) Develop an approved connection process for remote access to NAVSEA systems and networks based on user needs.

(9) Implement policy whereby information on Internets and Intranets is reviewed and approved by appropriate authorities prior to posting to ensure that all information will be protected commensurate with the sensitivity level of the information. Align all public facing websites to the NAVSEA website.

(10) Ensure initial security awareness training is provided for all newly assigned personnel involved in the management, use and/or operation of NAVSEA information systems. Training shall be conducted prior to issuance of networks and information system access authorization and tailored to the responsibilities of the position.

(11) Ensure annual security awareness training is provided for all personnel involved in the management, use and/or operation of NAVSEA information systems. Training shall be tailored to the responsibilities of the position.

(12) Ensure all NAVSEA information systems are accredited for operation at least once every three years or when changes occur that affect the security posture of the system. This can be accomplished for each system, group of systems and/or configuration.

(13) Maintain an Information Systems Accreditation Schedule (ISAS).

(14) Develop procedures to ensure that electronic data and files are marked to reflect the appropriate classification or sensitivity. Procedures shall include provisions for handling and

destruction. At a minimum, all electronic information in the form of documents, images, or other human-viewable format, regardless of location, shall include plain-text markings indicating classification or sensitivity, as would be required if they were hardcopy products.

(15) Ensure all personnel performing IA functions are identified and tracked as members of the IA Workforce, and monitored to ensure they are properly trained and certified as required by reference (k) as implemented by reference (l).

e. The IAPM shall:

(1) Be responsible for implementing this instruction, by preparing NAVSEA-wide IA plans, policies, and guidelines.

(2) Act as the focal point for all IA issues affecting NAVSEA and its field activities.

(3) Serve as the NAVSEASYSCOM Headquarters IAM. This responsibility may be further delegated in writing to a member of the NAVSEASYSCOM Headquarters IA staff.

f. IAMs shall:

(1) Serve as the focal point and principal advisor for information assurance matters on behalf of the activity Local IA Authority (Commander/Commanding Officer). The command IAM will have a direct reporting relationship with the Local IA Authority (Commander/Commanding Officer) in all matters related to the command's IA program.

(2) Manage the site's boundary defenses.

(3) Monitor Naval Telecommunications Directives (NTD) released by COMNAVNETWARCOM and implement requirements stated in the NTD. Current NTDs that remain in effect can be found at https://infosec.navy.mil/docs/index.jsp?tab=7&folder=40&page=1.

(4) Monitor Communication Tasking Orders (CTO) released by the Navy Cyber Defense Operations Command (NCDOC) and implements requirements stated in the CTO. Current CTO can be found at https://infosec.navy.mil/advisory/index.jsp?tab=4.

(5) Maintain their professional certifications as a member of the IA Workforce as required by references (k) and (l).

10. Action. This instruction is effective immediately. All addressees shall implement this policy within their organizations.

11. Point of Contact. The NAVSEA point of contact for this instruction is the NAVSEA IAPM, Mr. Tony Geddie, SEA 00I4, 202-781-

3014, DSN 326-3014, fax number 202-781-4737, e-mail address: james.geddie@navy.mil.

K. M. MCCOY

Distribution:
SNDL C84 COMNAVSEASYSCOM Shore-Based Detachments (less C84J)
C84B CONNAVSEASYSCOM Detachments
FKP COMNAVSEASYSCOM Shore Activities (less FKP6B and FKP24)

Copy to:
SNDL FT88 EDOSCOL
PEO IWS
PEO LMW
PEO SUB
PEO SHIPS
PEO CARRIERS
NAVSHIPYD NSRO
NAVSEA Special List Y2