SECNAVINST 5239.3B
DON CIO
17 June 2009

SECNAV INSTRUCTION 5239.3B

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY INFORMATION ASSURANCE POLICY

Ref: (a) Federal Information Security Management Act of 2002,
           Title III of E-Government Act of 2002, Public Law
           107-347 (codified in section 40 of title 44, United
           States Code)
       (b) SECNAVINST 5430.7P, Assignment of Responsibilities
           and Authorities in the Office of the Secretary of the
           Navy, of 26 Jun 08
       (c) Committee on National Security Systems (CNSS)
           Instruction 4009, National Information Systems
           Security Glossary, revised Jun 06
       (d) Joint Publication 1-02, Department of Defense
           Dictionary of Military and Associated Terms, 12 Apr
           01, amended 30 May 08
       (e) DoD Directive 8500.01E, Information Assurance, of
           24 Oct 02
       (f) DoD Instruction 8500.2, Information Assurance
           Implementation, of 6 Feb 03
       (g) through (ddd), see enclosure (1)

Encl: (1) References (continued)
       (2) Reference Location Table
       (3) Definitions
       (4) Acronyms

1. Purpose

    a. Establish Information Assurance (IA) policy for the
Department of the Navy (DON) consistent with national and
Department of Defense (DoD) policies.

    b. Designate the DON Chief Information Officer (DON CIO) as
the DON official assigned responsibility and delegated
authority, in accordance with references (a) and (b), in order
to ensure the requirements contained in these references are
carried out within the Department of the Navy.

c.   Assign responsibilities in the Department of the Navy for developing, implementing, managing, and evaluating DON IA programs, policies, procedures, and controls per reference (b).

2. Cancellation. SECNAVINST 5239.3A.

3. References, Definitions, and Acronyms. Location of references is as indicated in enclosure (2). Definitions used in this instruction are provided in references (c) through (f), and are expanded upon in enclosure (3). Acronyms are provided in enclosure (4).

4. Objectives. To establish an IA methodology within the Department of the Navy that utilizes policies for people, processes, strategy, and technology, consistent with the Federal Information Security Management Act (FISMA) and comprehensive DoD-wide approaches defined in national and DoD policy for protecting Information Technology (IT) and information. This DON IA policy shall:

a.   Provide guidance on implementing 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 the Department of the Navy; and

(2) Information systems and networks used or operated by the Department of the Navy, DON contractors processing DON information, or other organizations on behalf of the Department of the Navy.

b.   Establish an integrated Department-wide approach to protect the availability, integrity, authentication, confidentiality, and non-repudiation of DON information, information systems, and networks, 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.   Link the concept of Computer Network Defense (CND) with the precepts of IA.

d.   Establish standards for identifying, training, and certifying personnel performing IA functions, including military and government employees, and contractor personnel, regardless of job series or military specialty;

e.   Require that all authorized users of DON information systems and networks receive initial IA awareness orientation and complete annual IA awareness refresher training;

f.   Incorporate IA/CND as a critical component of the IT life cycle management process;

g.   Require registration of all DON information systems or networks that meet the qualification for registration in the DoD IT Portfolio Repository (DITPR). 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 the DON CIO;

h.   Require that all IT under DON authority that require Certification and Accreditation (C&A) are certified and accredited in accordance with reference (e);

i.   Ensure coordination at all levels with the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RD&A)), in order to support the IA needs of the Department of the Navy through appropriate technology research, development, and acquisition efforts;

j.   Evaluate DON IA policies and procedures annually;

k.   Require that DON IT programs document security costs;

l.   Ensure the use of managed risk analysis in balancing threats against DON IT and data criticality in order to identify and implement practical risk reduction solutions;

m.   Ensure a comprehensive computer network incident response and reporting process; and

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

5. Scope

    a. This instruction applies to all DON owned or controlled
information systems as defined in reference (e), Title 40 of the
United States Code, and the Clinger-Cohen Act, operated by a
contractor or other entity on behalf of the Department of the
Navy, that receive, process, store, display, or transmit DoD or
DON information, regardless of Mission Assurance Category (MAC),
classification, or sensitivity, except as noted below.

    b. The policy and requirements of the Department of Defense
and the Federal Government take precedence over any conflicting
requirements of this instruction. Implementing authorities
should identify conflicting policy to the DON CIO for
resolution.

    c. Nothing in this policy shall alter or supersede the
existing authorities and policies of the Director of Naval
Intelligence regarding the protection of sensitive compartmented
information and special access programs for intelligence that
fall under the purview of reference (i).

6. Background

    a. IA, as defined in reference (e), includes measures that
protect and defend information and information systems by
ensuring their availability, integrity, authentication,
confidentiality, and non-repudiation. This includes providing
for restoration of information systems by incorporating
protection, detection, and reaction capabilities.

    b. A quality IA program entails having sound information
system security and configuration management programs, per
references (a), (e), and (f). There shall be a means to protect
information and information systems against:

        (1) Unauthorized access or modification, whether in
storage or during processing or transit; and

        (2) The denial of service to authorized users, including
those measures necessary to detect, document, and counter such
threats.

c. The DON IA strategy is a combination of defense-in-depth (multiple layers of defense for an IT system) and defense-in-breadth (defense across the life-cycle spectrum). This approach takes the strategic, enterprise-wide view, considers the total life cycle of DON IT, and integrates people, technology, and operations to establish variable barriers across multiple layers and dimensions of networks. The strategy provides for a layered defense aimed at weakening or defeating attack, and that attacks that must penetrate multiple layers of protection are less likely to be successful. Dispersed protection includes distributing protection mechanisms among multiple locations, with each component of defense of the asset providing an appropriate level of robustness. Management of risk is the objective of IA in a defense-in-depth/defense-in-breadth strategy.

d. As noted in references (e) and (f), CND is a critical part of a defense-in-depth strategy, as it includes incident prevention, detection, and response. CND synchronizes the technical, operational, and intelligence assessments of the nature of a computer attack to defend against cyber attacks. The Joint Task Force for Global Network Operations (JTF-GNO), Navy Cyber Defense Operations Command (NCDOC), Marine Corps Network Operations and Security Center (MCNOSC), and Naval Criminal Investigative Service (NCIS) provide technical, operational, and intelligence assessments of computer network attacks and vulnerabilities as indicated below:

(1) The JTF-GNO, under United States Strategic Command (USSTRATCOM), is the lead organization for identifying and mitigating threats to DoD information networks, and directing the defense of the Global Information Grid (GIG).

(2) The Navy NCDOC and MCNOSC, as the designated CND service providers for the Navy and Marine Corps, respectively, report incidents and associated analytical results to the JTF-GNO and the respective DON Deputy CIO, who will ensure timely reporting of any formally reported incident to the DON CIO.

(3) The NCIS maintains investigative authority for criminal acts or espionage related to computer network security incidents, and coordinates information regarding such incidents with the law enforcement counterintelligence community.

e. Critical to IA is ensuring measures are in place to protect against unauthorized access to DON information and information systems. Reference (j) requires a common identification standard to be used when issuing identity credentials to Federal Government employees and contractors for accessing federal facilities and information systems. Reference (k) establishes standards for complying with reference (j). The next generation Common Access Card (CAC) is DoD's vehicle for meeting references (j) and (k) requirements.

f. Reference (l) provides additional detailed background and guidance for implementation of an IA program.

7. <u>Policy</u>

a. IA Personnel Training, Certification, and Management

(1) The Department of the Navy shall comply with references (m) and (n), and shall provide support for continually improving DoD IA workforce management processes.

(2) All IA personnel performing IA functions must be properly trained and certified as required by reference (m).

(3) Commanders, commanding officers, officers in charge, and directors, hereinafter referred to as "commanders of DON organizations," shall identify all IA functions to be performed and identify which IA functions require certification to be held by contractors in their statements of work and contracts, per references (m) and (n).

(4) All authorized users of DON information systems must complete DoD IA approved training as a condition of access. Commanders of DON organizations may add to the standardized baseline training their specific Department of the Navy, Service, and local IA policies and procedures. DoD IA training includes initial IA awareness orientation and annual IA awareness refresher training.

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

(6) DON training organizations shall include appropriate IA content in professional military education to develop leadership understanding of the critical importance of IA to successfully execute the DON's mission.

(7) IA workforce certification and training status shall be monitored and reported by the Services to the DON CIO to meet DoD reporting requirements and be included in the annual FISMA report. Commanders of DON organizations shall ensure supporting records are maintained to include the methodology and processes used to identify and track the IA workforce; and use, to the extent possible, existing databases and tools to satisfy these IA reporting requirements.

b.   Defense-in-Depth/Defense-in-Breadth. Commanders of DON organizations, shall implement a defense-in-depth/defense-in-breadth IA strategy to mitigate information security risks across the entire life cycle of the system or network. Except where otherwise indicated, references (e), (f), and (o) provide guidance for establishing and implementing these defensive measures which shall, at a minimum, include the following:

(1) Boundary Defense. Commanders of DON organizations shall use boundary protection mechanisms to limit unauthorized access to DON information and information systems and networks. These mechanisms may include, but are not limited to, Communications Security (COMSEC), routers, firewalls, and Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS). Personnel using these mechanisms will have the ability to implement counter-measures as vulnerabilities occur. These mechanisms are to detect intrusion attempts and send early alerts to security personnel or initiate automatic blocking when intrusion attempts are detected.

(2) Access Control. Commanders of DON organizations shall control unauthorized internal and external access to their information systems and networks.

(a) Connection. Commanders of DON organizations shall obtain formal authorization to interconnect information systems and networks per references (e), (f), and (p).

(b) Privileged Users. Commanders of DON organizations having IT assets shall designate, in writing,

7

Information Assurance Manager (IAM), IA officers, and all
personnel who perform functions of privileged access per
reference (f).

(c) Security and Privacy Notices. Commanders of DON
organizations shall require all DON information systems and Web
sites to display the approved privacy notices per references (q)
through (s). The DoD warning banner is not required on DON
public Web sites, i.e., Web sites that allow open, unrestricted
access to the public or allow unrestricted access from the
Internet. DON public Web site requirements are contained in
reference (r).

(d) The Insider Threat. Commanders of DON
organizations shall plan risk mitigation strategies to counter
the insider threat. Insider security threats (whether
intentional or unintentional) are potentially more serious than
the external threat because insiders do not have to penetrate
multiple layers of defense.

(e) Use of Commercial Electronic Mail (e-mail). Per
reference (t), 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 (o).

(f) Access by Foreign Nationals and Contractor
Personnel. Commanders of DON organizations shall control access
to DON information systems and networks in accordance with
relevant national and DoD policies and guidance, including
references (e), (f), and (u) through (aa). Access to DON
information systems and networks shall be based on a
demonstrated "need-to-know" and granted per references (e) and
(u). Foreign exchange personnel and representatives of foreign
nations, coalitions, or international organizations may be
authorized access to DON information systems and networks
containing classified information or information that could be
considered Controlled Unclassified Information (CUI), to include
sensitive information, defined in reference (e), only if all
applicable reference (e) requirements are met, including the
following policies and procedures:

1. Sanitize or reconfigure DON information
systems and networks to prevent unauthorized access to

classified and CUI by foreign nationals. Per reference (v), access should be regulated through the use of positive technical controls such as a Demilitarized Zone (DMZ) and ensuring Web sites are properly configured to grant access to only authorized personnel.

        2. Identify foreign nationals and contractors, per references (f) and (o), in DON e-mail addresses, e-mail display names, and automated signature blocks.

    (3) Remote Access. Commanders of DON organizations shall control remote access to DON information systems and networks per references (f), (o), (u), (w), (bb), and (cc).

      (a) Government-furnished computer equipment, software, and communications with appropriate security measures are the primary and most secure means for remote access, and are required for any regular and recurring telework arrangement that involves CUI or sensitive information, per reference (dd).

      (b) CUI, and sensitive information defined in reference (e), shall be protected as specified in subparagraphs 7b(4) and 7b(10)(b) below.

      (c) All remote connections will be identified, authenticated, and logged, per reference (o).

      (d) All remote access to DoD information systems and networks, to include telework access, shall be mediated through a managed access control point, such as a remote access server in a DMZ. Remote access shall use encryption to protect the confidentiality of the session, per reference (f).

      (e) Authentication and confidentiality requirements for remote access sessions will be implemented using National Security Agency (NSA)-approved COMSEC and keying material for classified systems and National Institute of Standards and Technology (NIST)-approved COMSEC and DoD Public Key Infrastructure (PKI) certificates for unclassified systems. The use of DoD PKI certificates, protected by a hardware token, such as the CAC, and accessed through the associated approved reader and middleware, is the primary method for remote client-side authentication.

(f) All computers used for remote access must have DoD approved antivirus and firewall protection that includes the capability for automated updates as per reference (f). The most current definitions and updates for these applications must be loaded prior to establishing remote access sessions.

(g) Publicly accessible computers (e.g., computer labs, public kiosks, Internet cafes, libraries, morale, welfare and recreation facilities) shall not be used for remote access. Public Wireless Fidelity (WiFi) hotspots (e.g., coffee shops, hotel WiFi, airports) may be utilized as long as requirements in subparagraphs 7b(3)(e) and 7b(3)(f) above are met.

(4) Protection of CUI. Commanders of DON organizations shall ensure CUI is protected in accordance with references (e), (q), (r), (u), (w), (x), (ee), and (ff). All DON information owners shall conduct risk assessments of CUI and identify those needing more stringent protection for remote access or contained on portable electronic devices (e.g., laptops, personal electronic devices) or removable storage devices (e.g., thumb drives, compact discs). Any portable electronic device or removable storage device containing CUI removed from protected workplaces must conform to the procedures outlined in references (q), (x), and (dd) through (ff). Examples of CUI may be found in enclosure (3), Definitions.

(5) Protection of Data at Rest (DAR). Per reference (ee), all unclassified DoD DAR that has not been approved for public release and is stored on portable electronic devices (to include laptop computers) or removable storage devices shall be treated as CUI and encrypted using DON-approved enterprise DAR products that utilize DoD-approved encryption technology.

(6) Aggregation of Data on Unclassified Networks and Systems. In some cases, unclassified information may become classified if determined so by an original classification authority or if a security classification guide outlines the specific compilation relationships. Commanders of DON organizations 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, in accordance with reference (x). If aggregation of data results in CUI or otherwise 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 Secret Internet Protocol Router Network (SIPRNet) or Joint Worldwide Intelligence Communications System (JWICS), as appropriate, and removed from the unclassified network or system.

(7) Incident Response and Intrusion Detection. The goal of an IDS/IPS is to detect and identify unauthorized use, misuse, and abuse of computer assets by both internal network users and external attackers in "near real time." Utilizing the requirements of reference (o), the NCDOC and MCNOSC will perform timely incident handling and analysis of computer network attacks that occur on the DON network.

(a) NCDOC and MCNOSC shall centrally manage and monitor DON IDS/IPS systems. This constitutes the DON's responsibility to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of DON operations, and report computer incidents in accordance with references (o), (x), and (gg) through (ii).

(b) Commanders of DON organizations shall work closely with NCDOC and MCNOSC to provide local monitoring when central monitoring is not feasible and/or to further the defense-in-depth and defense-in-breadth strategies of the Department of the Navy. These commanders shall ensure timely handling of signature threshold alerts, updates, and audit records/log files per reference (o).

(c) DON network audit records shall be retained for 1 year per references (f) and (jj), under Standard Subject Identification Code (SSIC) 7510.1(b), "Internal Audit". Unless otherwise superseded by another SSIC, or if directed by legal counsel, NCIS, or higher level authority, the audit record may be held beyond its approved record retention schedule for the purpose of litigation or ongoing investigation.

(8) Malicious Mobile Code/Virus Detection and Neutralization. To protect DON systems from malicious or improper use of mobile code, commanders of DON organizations shall assess and mitigate the risks of this technology, per references (o) and (kk), and:

(a) Ensure that DoD or DON-approved anti-virus Host Intrusion Prevention Systems (HIPS), as appropriate, are installed on all information systems and that these mechanisms are updated regularly. Anti-virus and HIPS policy shall be configured to perform these updates automatically, reliably, and through a centrally controlled management framework, where feasible.

(b) Report malicious code outbreaks to the appropriate combatant commander and to the NCDOC or MCNOSC per references (o), (gg) and (ii).

(9) Virtual Private Networks (VPNs). VPNs help to ensure confidentiality and integrity of remote connections. Of the available options for remote access, VPNs are the preferred method when using government-furnished or government-contracted equipment. Commanders of DON organizations shall consider mandating the use of VPN to protect and control internal and external access to their information systems and networks, once a mission need for remote access is established. If administrators need access to information systems from outside the enclave, they must:

(a) Establish a VPN connection using government-furnished equipment under their user account (with user privileges). All remote access to DON classified systems or networks shall utilize NSA-approved COMSEC and keying material. Commanders of DON organizations shall mandate the use of VPN devices that have current NIST Federal Information Processing Standard (FIPS) 140-2 validation certification to protect and control internal and external access to their unclassified information systems, once a mission need for remote access is established.

(b) Elevate permissions to the appropriate level to conduct administrator tasks once a secure connection is established.

(c) Terminate the connection when administrator tasks are complete.

(10) Identity Management. Commanders of DON organizations shall use identity management capabilities in accordance with reference (j) to validate and securely

authenticate an identity (human, device, or process) requesting use of a DON IT asset prior to granting access, with the exception of weapons systems. Identity management includes, but is not limited to, the use of the CAC, PKI, and biometric technologies.

(a) CAC. Per references (ll) and (mm), the CAC shall be the primary identity credential supporting interoperable physical access to DON installations, facilities, buildings, and controlled spaces, and logon access to all unclassified DON networks. The Department of Defense is modifying the CAC to meet the requirements of references (j) and (k).

(b) PKI. Commanders of DON organizations shall enable DON information systems, including networks, e-mail, and Web servers, to use PKI certificates issued by the Department of Defense and approved external PKI certificates, as appropriate, to support authentication, access control, confidentiality, data integrity, and non-repudiation, per references (f), (nn), and (oo). Per reference (pp), 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.

<u>1</u>. Software Certificates. PKI software certificates, when improperly installed, stored, or maintained, may introduce vulnerabilities to DON networks. For this reason, software certificates are being phased out, and their use should be avoided whenever a PKI hardware token alternative exists. DoD PKI software based certificates may be used only when deemed mission essential and authorized, in writing, by the DON Deputy CIO (Navy or Marine Corps). 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.

<u>2</u>. Digital Signatures. Commanders of DON organizations shall ensure e-mail messages requiring either message integrity or non-repudiation are digitally signed using DoD PKI. All e-mail containing an attachment or embedded active content must be digitally signed.

13

<u>3</u>. Encryption. Commanders of DON organizations shall ensure that CUI contained in either e-mail or Web server transactions is encrypted using DoD PKI. Examples of this are attachments that contain personal identity or budget information.

(c) Biometrics. Commanders of DON organizations shall ensure that all new acquisitions or upgrades of electronic biometric collection systems used by DON components conform to the DoD standards, per reference (qq). Based on the criticality and sensitivity of the system, biometrics can be combined in an IA defense-in-depth strategy to provide an additional layer of user authentication.

(11) Internet Security. Commanders of DON organizations shall manage all interconnections of DON information systems, both internal and external, to minimize community risk.

(a) Physical or technical means, such as an approved boundary protection product, PKI, or the integration of systems into a DoD Non-Classified Internet Protocol Router Network (NIPRNet) DMZ, shall be used to protect DON information systems that allow open, unrestricted access to the public. A DMZ may be used to host all Internet-facing DoD servers and applications. These are the public servers and applications that must be accessible from the Internet and will provide separation between the public and private servers by segmenting the public servers within the controlled environment of the DoD DMZ. Establishing DoD DMZs at the Internet–NIPRNet boundary and migrating publicly accessible servers to these DoD DMZs will protect private DoD information from Internet access and rigidly control DoD public information access from the Internet while still enabling information sharing.

(b) Private servers are the NIPRNet-only servers and applications that must not be accessible from the Internet. Access to private servers and applications will be blocked such that access directly from the Internet to these servers and applications will not be possible. Additionally, all DON private/restricted Web servers shall be issued DoD PKI server certificates and shall use the certificates for server authentication via the appropriate cryptographic protocol (e.g., transport layer security protocol) and require client side

authentication, per reference (oo). Possession of a valid PKI certificate does not confirm "need-to-know," therefore additional access control measures are required to protect CUI.

(12) Physical Security. Commanders of DON organizations shall ensure the protection of DON IT resources (e.g., installations, personnel, equipment, electronic media, documents, etc.) from damage due to malicious activities, natural disasters, loss, theft, or unauthorized physical access. References (x) and (y) provide amplifying requirements and information related to information security.

(13) Contingency Planning. Commanders of DON organizations shall develop, test, and evaluate Contingency Plans (CPs) in accordance with reference (f) to describe the interim measures used to recover and restore IT systems and service operations following an emergency or system disruption.

(a) System owners must develop a CP in accordance with reference (rr) for every information system, 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.

(b) CPs must name the system in the plan to match the name that is registered in DITPR-DON and the applicable C&A documentation.

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

(d) CPs shall be exercised at least annually in accordance with reference (f). Exercises should be realistic; however, a desktop exercise can be used in place of an actual physical exercise. Exercise performance must be documented, signed, and dated, and specifically state what was tested and the results. Shortfalls shall be documented and approved via a Plan of Action and Milestones (POA&M). The POA&M shall be maintained to track progress and resolution of identified shortfalls.

(14) Information Operations Conditions (INFOCONs). To ensure adequate incident response, commanders of DON organizations shall develop, implement, and manage INFOCONs as required in reference (ss). Specific requirements of INFOCON levels across the DON should be consistent. Although USSTRATCOM of JTF-GNO normally prescribe INFOCONs, commanders of DON organizations have the authority to increase INFOCONs in their area of responsibility when the circumstances dictate. This increased security posture is one more tool available in the defense-in-depth architecture.

(15) Information Assurance Vulnerability Management (IAVM). The IAVM process is designed to provide positive control of the vulnerability notification and corrective action process in the Department of Defense. Commanders of DON organizations shall comply with the IAVM process and report compliance to the appropriate combatant commander and the NCDOC or MCNOSC per references (o), (gg), and (ii). Commanders of DON organizations must monitor that patches deployed have been implemented and reported.

c. Mission Assurance Categories (MAC). Per reference (f), program managers, acting for the Chief of Naval Operations or the Commandant of the Marine Corps, shall assign a MAC to each DON information system and enter that data in the FISMA section of DITPR-DON. The MAC must be selected based on the importance of the information in the system relative to the achievement of DON goals and objectives; particularly the warfighter mission, not the cost of IA factors associated with a particular MAC.

d. IA Assessments

(1) Commanders of DON organizations shall assess the effectiveness of their defense-in-depth/defense-in-breadth IA strategy implementations. Program managers shall also assess their IA strategy during development and testing. There are a wide variety of programs and services to evaluate the vulnerability of IT including: online surveys, self-assessment checklists, training assist visits, vulnerability assessments, threat monitoring, and outside audits.

(2) Other DON components, e.g., MCNOSC and NCDOC, conduct vulnerability assessments in accordance with their procedures.

(3) Service and secretariat DAAs shall report to the DON CIO any critical issues that may impact DON network security.

e. Certification and Accreditation (C&A). DON information systems shall have an assigned DAA and obtain C&A per references (e), (f), and (tt).

(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 analysis of IA controls for use by the DAA to issue an accreditation decision.

(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. Full accreditation with an Authorization to Operate (ATO) is always the goal for operational systems. Reference (tt) describes accreditation types and criteria for issuance.

(3) Reference (tt) provides the requirements for C&A of DON systems and networks. In amplification of this reference:

(a) An Interim Authorization to Operate (IATO) associated with ships and aircraft under construction may be renewed only until the unit is commissioned, tested, and accepted for unrestricted operations.

(b) The Department of the Navy goal for system accreditation for systems requiring C&A is 100 percent either fully accredited (ATO) or with at least an IATO accompanied by a POA&M. These goals reflect the requirements of the President's Management Agenda.

(4) The Service DAA shall ensure secure operation of all information systems and networks in his or her area of responsibility. The appropriate DAA shall formally authorize a system to operate when an acceptable level of risk has been achieved through application of appropriate risk mitigation in accordance with references (l) and (tt). DAAs shall accredit

DON information systems that meet the requirements of references (e), (f), and (tt) per the C&A process, and in coordination with the DON Senior IA Officer (SIAO) per with reference (uu).

(5) POA&Ms. Commanders of DON organizations and program managers shall develop IT security POA&Ms to delineate the tasks and schedule necessary to successfully resolve identified security weaknesses. The purpose of the POA&M is to assist DON organizations in identifying, assessing, prioritizing, and monitoring the progress to resolve identified security weaknesses in programs and systems. IT security POA&Ms shall be maintained and managed in accordance with references (jj) and (tt). The respective DAAs are responsible for monitoring and tracking overall execution of system-level IT security POA&Ms, per reference (tt). The DON Deputy CIOs will monitor and track overall execution of system-level IT security POA&Ms and report status of system-level IT security POA&Ms on a quarterly basis to the DON CIO per reference (tt). POA&Ms are especially important for systems for which a capital asset plan and business case (exhibit 300) is submitted per reference (vv).

f. Annual Reviews and Tests

(1) All information systems must undergo annual information security reviews per references (a) and (f). Corrective action shall be taken to immediately address shortfalls identified. If corrective actions cannot be immediately implemented, the IT security POA&M will be updated to include future corrections. 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) The applicable security controls for information systems requiring C&A and reported for FISMA purposes must be tested at least annually per reference (f). 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.

g. Acquisition Management. Commanders of DON organizations and program managers shall implement a defense-in-depth/defense-

in-breadth strategy throughout the life cycle of the IT asset.
This applies to all DON information systems used to enter,
process, store, display, or transmit information.

(1) Per reference (g), a contract to acquire a mission-
critical, mission-essential, or mission support IT asset cannot
be awarded until the asset is registered in the DITPR-DON.
Further, major acquisition programs require an acquisition IA
strategy as defined in reference (g).

(2) Per reference (ww), commanders of DON organizations
and program managers, in coordination with ASN(RD&A), shall
identify and implement a plan to achieve security control
objectives, and ensure that IA is fully integrated into all
phases of their acquisition, upgrade, or modification programs,
including initial design, development, testing, fielding, and
operation. Further, they shall ensure that IA is integrated
into the systems engineering technical review process in
accordance with reference (xx). IA requirements include:

(a) Appointment of an IAM;

(b) Determination of a system MAC, mission
criticality, and confidentiality level; and

(c) Planning and execution of the C&A process per
references (e), (f), and (tt).

(3) Commanders of DON organizations and program managers
shall acquire and use National Information Assurance Partnership
evaluated or validated government-off-the-shelf or commercial-
off-the-shelf IA and IA-enabled IT products for all IT systems
as long as the validated products meet mission requirements, per
reference (f). All incorporated IA products and IA-enabled IT
products shall comply with the requirements of reference (yy),
as outlined in reference (f).

(4) The Department of the Navy shall acquire COMSEC
products and services to protect classified systems and networks
per references (f) and (zz), as appropriate. The program
executive officer for command, control, communications,
computers, and intelligence is designated as the central DON
procurement authority for all DON high assurance COMSEC and key
management infrastructure.

(5) Commanders of DON organizations and program managers shall include requirements to protect classified and CUI in contracts and monitor contractors for compliance per references (ww) and (aaa).

(6) Commanders of DON organizations and program managers shall assess the risk of allowing foreign nationals to compose code for or access DON information systems and networks, per references (e), (f), and (u). The result of the risk assessment shall guide access restrictions and security requirements for the contract.

(7) Commanders of DON organizations shall implement those steps necessary to ensure acquisition managers address IA requirements for all FISMA-defined National Security Systems (NSS), per references (a), (e) through (g), and (ww).

h. <u>Operations Security (OPSEC)</u>. Commanders of DON organizations shall establish an OPSEC program focused on command involvement, assessments, surveys, training, education, vulnerability, threat, resourcing, awareness, and monitoring in accordance with reference (bbb).

i. <u>COMSEC</u>

(1) The ability to maintain the confidentiality and integrity of DON classified information and unclassified information that has not been approved for public release during transmission is of paramount importance for an effective DON security posture. The Navy and Marine Corps shall protect this information through COMSEC measures and procedures, and conduct COMSEC monitoring activities only as necessary and in accordance with references (zz) and (ccc), to determine the degree of security provided to telecommunications and automated information systems.

(2) IA and COMSEC monitoring activities are done only as necessary to determine the degree of security provided to telecommunications and DON IT and to aid in countering vulnerabilities. Commanders of DON organizations shall ensure that such activities are conducted in strict compliance with reference (ccc).

j. Research and Development. The Department of the Navy shall leverage commercial IA technology in conjunction with government IA technology to meet future DON requirements. The Department of the Navy shall deploy IA solutions that support interoperability and integration of IT activities across the Department of Defense.

8. Responsibilities

a. The DON CIO shall:

(1) Carry out the IA responsibilities assigned by reference (a) to the head of each Federal agency, and by reference (b). Accordingly, the DON CIO shall ensure DON compliance with the IA requirements of references (a), (e), and (f) and related IA policies, procedures, standards, and guidelines.

(2) Report (as required) to the Secretary of the Navy (SECNAV) IA/CND issues and significant incidents.

(3) Develop information security policies sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the Department of the Navy.

(4) Designate a DON SIAO who reports to the DON CIO on DON IA policies per section 3544(a)(3) of reference (a).

(5) Designate a DON Deputy SIAO for CND who reports to the DON SIAO per references (uu) and (ddd). The DON Deputy SIAO for CND is responsible for maintaining unified and enhanced DON CND processes, establishing policy, and providing appropriate oversight of the processes. The DON Deputy SIAO for CND will collaborate with the ODAAs and representatives of the DON Deputy CIO (Navy and Marine Corps) to coordinate on DAA issues, ensure consistent guidance is provided, and discuss and resolve problem areas.

(6) Ensure senior DON officials provide IA protections for DON information and information systems that support operations and assets. These IA protections include assessment, determining appropriate levels of IA, implementing policies and

procedures to cost-effectively reduce risks to an acceptable level, and periodically testing and evaluating IA controls and techniques to ensure effective implementation.

(7) Set DON standards and policy for IA workforce education, training (including user awareness), certification, and management requirements commensurate with their respective responsibilities regarding information and information systems, and including Internet security and DAA training.

(8) Incorporate IA and CND tenets within the DON information management and IT strategy.

(9) Collaborate the integration of IA requirements with DON strategic and operational planning, and with the DON major system acquisition management process.

(10) Ensure coordination of IA/CND issues with other military departments, defense agencies, and the Department of Defense.

(11) Evaluate annually the effectiveness of the DON IA program per reference (a) and provide input to the DoD CIO for a collective report on information security, as part of the annual FISMA report.

(12) Define and cause to be reported metrics to describe the adequacy of DON IA/CND efforts.

(13) Coordinate with the DON Auditor General for recommendations for IA audits and reviews.

(14) Review IA strategies for major defense acquisition programs and major automated information systems per reference (g) as part of the process for managing IT investments.

(15) Report periodically, in coordination with other senior officials, to the SECNAV on the effectiveness of the DON IA program, including progress on remedial actions.

(16) Ensure compliance with DoD identity management policy, timelines, and processes throughout the Department of the Navy through process synchronization and strategy alignment.

(17) Coordinate risk management across the Department of the Navy by balancing threat against system/data criticality to identify and implement practical solutions.

(18) Mandate a robust program within the Department of the Navy for vulnerability assessments, threat modeling, and penetration testing, including effective use of red team exercises. Mandate sharing of lessons learned and best practices across the Navy and Marine Corps.

b. The DON SIAO shall:

(1) Ensure all enterprise-wide systems comply with requirements of applicable DON, DoD, and Federal policies and mandates such as references (a), (b), (e), (f), and (tt);

(2) Serve as the single IA coordination point with the DON Service DAAs for implementation and accreditation of Joint or Defense-wide applications on DON enterprise networks or to DoD component enclaves;

(3) Establish a reporting relationship and ensure alignment between the Navy and Marine Corps DAAs;

(4) Track the C&A status of information systems that are governed by the DON IA program via an automated C&A tool;

(5) Formally delegate certifying authority duties;

(6) Ensure certification quality, capacity, visibility, and effectiveness;

(7) Facilitate a consistent application of IA policies, processes, responsibilities, and procedures across the DON;

(8) Ensure communication between the DON SIAO, Service-level DAAs, and network operations of the Services;

(9) Establish and enforce the C&A process for applications residing on DON enterprise networks; and,

(10) Ensure the consistent application of waiver request standards and processing across DON enterprise networks.

d. ASN(RD&A) shall:

(1) Issue DON acquisition policies providing implementation details and procedures to support IA.

(2) Collaborate the integration of IA requirements into acquisition management of all DON acquisition programs throughout their life cycle per reference (f), and collaborate with DON CIO in the integration of IA into DON major system acquisition management process.

(3) Maintain a science and technology program in IA, per reference (a).

e. The Assistant for Administration/Office of the Under Secretary of the Navy (AA/USN) shall:

(1) Function as the DAA for secretariat IT assets.

(2) Set policies and procedures to control access by foreign nationals to information systems via networks owned or operated at the SECNAV level, per references (e), (f), and (u) through (aa).

(3) Implement standard formats specified in reference (f) to identify foreign nationals and contractors in all forms of communications owned and operated at the SECNAV level, including e-mail, per reference (e).

(4) Require that qualifying IT investments under the purview of AA/USN be registered in DITPR-DON, per references (g) and (h), and periodic DITPR-DON guidance issued by the DON CIO.

f. The Chief of Naval Operations and the Commandant of the Marine Corps shall:

(1) Ensure the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems and networks supporting their respective operations and assets.

(2) Develop and implement IA/CND programs, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting

from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for their respective Service. Service IA programs shall contain the elements of a DoD Component IA program in reference (f).

(3) Ensure that IA/CND is practiced throughout the life cycle of their respective Service IT assets, including design, acquisition, installation, operation, upgrade, or replacement.

(4) Establish and validate Service IA/CND requirements and coordinate IA requirements that cross Service boundaries with the Joint Staff per reference (e).

(5) Ensure IA/CND costs are budgeted in DON IT programs and IT system acquisitions, in accordance with reference (g) and the annual DON CIO IT policy guidance memorandum.

(6) Serve as the resource sponsor for their respective Service cryptographic requirements, following the guidelines of reference (zz), based on DON priorities.

(7) Designate Service DAAs for information systems under their Service authority and ensure compliance with the C&A requirements per references (e), (f), and (tt).

(8) Require that qualifying Service IT systems be registered in DITPR-DON, per references (g) and (h), and periodic DITPR-DON guidance issued by the DON CIO.

(9) Identify, train, and certify all personnel performing IA functions, regardless of job series or military specialty.

(a) Implement DoD IA awareness training. Ensure all authorized users of DON information systems and networks receive initial IA awareness orientation, located on the Navy Knowledge Online Web site, as a condition of access, and, thereafter, complete annual refresher training to maintain IA awareness.

(b) Monitor and report workforce IA training and workforce status to the DON CIO to meet DoD reporting requirements and the annual FISMA Report. Maintain supporting records to include the methodology and processes used to

identify and track the IA workforce; and use, to the extent possible, existing databases and tools to satisfy these IA reporting requirements.

(c) Develop IA training to be consistent with the minimum standards published in references (m) and (n), as applicable, to specific job roles and functions.

(d) Ensure training organizations include appropriate IA content in professional military education to develop leadership understanding of the critical importance of IA to the successful execution of the DON mission.

(10) Set policies and procedures to control access by foreign nationals to DON-owned classified and unclassified information, and DON-owned and operated local area networks and information assets, consistent with references (e), (f), and (u) through (aa).

(11) Implement standard formats specified in reference (f) to identify foreign nationals and contractors in all forms of communications owned or operated by their respective Service, including e-mail, per reference (e).

(12) Provide for IA vulnerability assessment, vulnerability mitigation, and incident response and reporting in accordance with references (f), (o), (hh), and (ii).

(13) Mandate red and blue team operations within Service organizations. Ensure results are reported to the Service DAAs, DON Deputy CIOs, and DON CIO.

(14) Review their Service IA/CND status annually to ensure it is fully consistent with the DON IA policy. Report these findings to the DON CIO.

(15) Ensure DON CIO is provided, within 3 working days, a copy of all formal reports of security incidents and analyses reported via the operational chain of command.

(16) Ensure the efficient and effective use of identity management capabilities and implementation (CAC, PKI, and biometrics) for their service.

(a) Ensure any procurement of user identity smart card technology, other than the CAC, has DON CIO review and approval, and conforms to requirements established by references (j) and (k).

(b) Ensure all Service information systems, including networks, e-mail, and Web servers are properly Public Key (PK)-enabled, including the use of secondary access controls to enforce need to know and data segregation requirements where appropriate.

    1. Enforce digital signature of all DON-originated e-mail messages which require message integrity and non-repudiation.

    2. Enforce encryption of all e-mail or Web server transactions containing CUI or sensitive information.

(c) Ensure all new acquisitions or upgrades of electronic biometric collection systems used within their respective Service conform to the Federal and DoD electronic biometric transmission specification per reference (qq).

(17) Ensure the Service DAAs report to the DON CIO any critical issues that impact network security, including results of red team activity analysis on DON networks.

(18) Notify the General Counsel of the Navy of actions taken to notify users of official DON telecommunications systems and IT, that such systems are subject to COMSEC monitoring at all times and that use of such systems constitutes consent to COMSEC monitoring, in accordance with reference (ccc).

  g. The Director, NCIS, shall:

(1) Conduct all investigations regarding operations, proactive programs, and related analyses of cyber incidents and targeting involving DON IT assets.

(2) Collect, track, and report threats to DON IT assets and disseminate this information to other law enforcement agencies, Department of Defense, Department of the Navy, DON CIO, and other national agencies, as needed.

(3) Conduct cyber-related criminal investigations regarding root level intrusions, user level intrusions, denial of service, malicious logic incidents, and aforementioned suspected incidents (Categories 1, 2, 4, and 7). Provide recommendations based on analysis of forensics to the DON CIO for incorporation into potential IA/CND policy

(4) Investigate fraud, waste, abuse, and other criminal violations involving DON IT.

(5) Maintain a staff skilled in the investigation of computer crime. The staff should be sufficient in size to handle multiple major incidents and respond to increasing demands of the Department of the Navy.

9. <u>Action</u>. All DON commands, activities, and organizations shall implement this policy.

10. <u>Records Management</u>. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with reference (jj).

11. <u>Reports</u>. The reports referred to in this instruction are exempt from reports controlled by SECNAV Manual 5214.1.
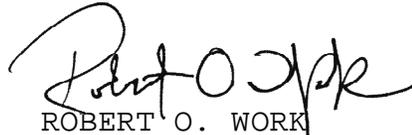
ROBERT O. WORK
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances Web site
http://doni.daps.dla.mil/

REFERENCES (continued)

(g) SECNAVINST 5000.2D, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, of 16 Oct 08

(h) SECNAVINST 5000.36A, Department of the Navy Information Technology Applications and Data Management, of 19 Dec 05

(i) DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, 9 Oct 08

(j) Homeland Security Presidential Directive–12(HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, of 27 Aug 04

(k) National Institute of Standards and Technology, Federal Information Processing Standards Publication (FIPS 201-1),Personal Identity Verification (PIV) of Federal Employees and Contractors, Mar 06

(1) SECNAV Manual M-5239.1, Department of the Navy Information Assurance Program, of Nov 05

(m) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, of 15 Aug 04

(n) DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 Dec 05

(o) Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01, CH 3 of 8 Mar 06, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND) (NOTAL)

(p) CJCS Instruction 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities, of 9 Jul 08

(q) SECNAVINST 5211.5E, DON Privacy Act (PA) Program, of 28 Dec 05

(r) SECNAVINST 5720.47B, Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites, of 28 Dec 05

(s) DoD memo, Policy on Use of DoD Information Systems – Standard Consent Banner and User Agreement, of 9 May 08

(t) DON CIO Washington DC 161108Z JUL 05, Effective Use of Department of the Navy Information Technology Resources

(u) SECNAV M-5510.30, Department of the Navy Personnel Security Program Manual, of Jun 06

(v) ASD (NII) memo, Access to Unclassified DoD Networks by Foreign Government Organizations, of 2 Aug 04

(w) SECNAVINST 5510.30B, Department of the Navy (DON) Personnel Security Program (PSP) Instruction, 6 Oct 06

(x) SECNAV-M 5510.36, DON Information Security Program
    Manual, of Jun 06
(y) SECNAVINST 5510.36A, Department of the Navy (DON)
    Information Security Program Instruction, of 6 Oct 06
(z) SECNAVINST 5510.34A, Disclosure of Classified Military
    Information to Foreign Governments, International
    Organizations, and Foreign Representatives, of 8 Oct 04
(aa) DoD Directive 5230.20, Visits, Assignments, and Exchanges
     of Foreign Nationals, of 12 Aug 98
(bb) OMB memo M-06-16, Protection of Sensitive Agency
     Information, of 23 Jun 06
(cc) DoD CIO memo, Department of Defense (DoD) Guidance on
     Protecting, Personally Identifiable Information (PII),
     of 18 Aug 06
(dd) USD(P&R) memo, Department of Defense (DoD) Telework
     Policy and Guide, of 22 Oct 01
(ee) DoD CIO memo, Encryption of Sensitive Unclassified Data
     at Rest on Mobile Computing Devices and Removable Storage
     Media, of 3 Jul 07
(ff) DON CIO Washington DC 291652Z FEB 08, Loss of Personally
     Identifiable Information (PII) Reporting Process
(gg) DoD Directive O-8530.1, Computer Network Defense (CND),
     of 8 Jan 01
(hh) SECNAVINST 5239.19, Department of the Navy Computer
     Network Incident Response and Reporting Requirements, of
     18 Mar 08
(ii) DoD Instruction O-8530.2, Support to Computer Network
     Defense, of 9 Mar 01
(jj) SECNAV Manual 5210.1, Department of the Navy Records
     Management Manual, 11 Nov 07
(kk) DoD Instruction 8552.01, Use of Mobile Code Technologies in
     DoD Information Systems, of 23 Oct 06
(ll) DoD Directive 8190.3, Smart Card Technology, of 31 Aug 02
(mm) DoD 5200.08-R, Physical Security Program, of 9 Apr 07
(nn) DoD Instruction 8520.2, Public Key Infrastructure (PKI) and
     Public Key (PK) Enabling, of 1 Apr 04
(oo) DON CIO Washington DC 061525Z OCT 04, DON Public Key
     Infrastructure (PKI) Implementation Guidance
(pp) DoD Policy memo, Compliance and Review of Logical Access
     Control in Department of Defense (DoD) Processes,
     of 24 Jan 07
(qq) DoD Directive 8521.01E, Department of Defense Biometrics,
     of 21 Feb 08

(rr) National Institute of Standards and Technology (NIST) Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, of Jun 02

(ss) STRATCOM Strategic Directive SD-527-1, Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures, of 27 Jan 06

(tt) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of 28 Nov 07

(uu) DON CIO Memorandum, Senior Information Assurance Officer Alignment and Responsibilities for Information Assurance and Certification and Accreditation Processes, 18 Dec 08

(vv) OMB Circular A-11, Preparation, Execution, and Submission of the Budget, Jul 03 (NOTAL)

(ww) DoD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System, of 9 Jul 04

(xx) ASN(RD&A) memo, Systems Engineering Technical Review Process for Naval Acquisition Programs, of 13 Jun 08

(yy) NSTISSP No. 11 Revised Fact Sheet, National Information Assurance Acquisition Policy, of Jul 03

(zz) DoD Instruction 8523.01, Communications Security (COMSEC) (U), of 22 Apr 08

(aaa) DoD Manual 5220.22, National Industrial Security Program Operating Manual (NISPOM), of Feb 06

(bbb) DoD Directive 5205.02, DoD Operations Security (OPSEC) Program, of 6 Mar 06

(ccc) DoD Instruction 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing, of 9 Oct 07

(ddd) DON CIO memo, Roles and Responsibilities of the Department of the Navy Deputy Senior Information Assurance Officer for Computer Network Defense (DON Deputy SIAO for CND), of 27 Sep 07

Reference Location Table

Ref	Subject	Location
a	FISMA, in E-Government Act of 2002	http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
b	SECNAVINST 5430.7P, Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy	http://doni.daps.dla.mil/allinstructions.aspx
c	CNSS Instruction 4009, National Information Systems Security Glossary	http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
d	Joint Publication 1-02, DoD Dictionary of Military and Associated Terms	http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf
e	DoD Directive 8500.01E, Information Assurance (IA)	http://www.dtic.mil/whs/directives/
f	DoD Instruction 8500.2, IA Implementation	http://www.dtic.mil/whs/directives/
g	SECNAVINST 5000.2D, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System	http://doni.daps.dla.mil/allinstructions.aspx
h	SECNAVINST 5000.36A, Department of the Navy Information Technology Applications and Data Management	http://doni.daps.dla.mil/allinstructions.aspx
i	DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information	http://www.dtic.mil/whs/directives/
j	Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors	https://www.dmdc.osd.mil/smartcard/owa/ShowPage?p=HSPD12
k	National Institute of Standards and Technology, Federal Information Processing Standards Publication (FIPS 201)	http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

l	SECNAV Manual M-5239.1, Department of the Navy Information Assurance Program	http://doni.daps.dla.mil/secnavmanuals.aspx
m	DoD Directive 8570.1, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/
n	DoD 8570.01-M, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/directives/
o	CJCS Manual 6510.01, CH 3, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)	http://www.dtic.mil/cjcs_directives/cjcs/manuals.htm (LIMITED ACCESS)
p	CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf
q	SECNAVINST 5211.5E, DON Privacy Act Program	http://doni.daps.dla.mil/allinstructions.aspx
r	SECNAVINST 5720.47B, DON Policy for Content of Publicly Accessible World Wide Web Sites	http://doni.daps.dla.mil/allinstructions.aspx
s	DoD Memo of May 9, 2008, Policy on Use of DoD Information Systems – Standard Consent Banner and User Agreement	http://www.doncio.navy.mil/uploads/GRIMES_Banner_and_User_Ack_memo_May2008.pdf
t	DON CIO message 161108Z JUL 05, Effective Use of DON Information Technology Resources	http://www.doncio.navy.mil/PolicyView.aspx?ID=346
u	SECNAV M-5510.30, DON Personnel Security Program Manual	http://doni.daps.dla.mil/secnavmanuals.aspx
v	ASD (NII) memo of 2 Aug 04, Access to Unclassified DoD Networks by Foreign Government Organizations	http://www.doncio.navy.mil/uploads/DOD Policy on FN – DMZs.pdf
w	SECNAVINST 5510.30B, DON Personnel Security Program (PSP) Instruction	http://doni.daps.dla.mil/allinstructions.aspx
x	SECNAV M-5510.36, DON Information Security Program Manual	http://doni.daps.dla.mil/secnavmanuals.aspx

y	SECNAVINST 5510.36A, Department of the Navy (DON) Information Security Program Instruction (ISP)	http://doni.daps.dla.mil/allinstructions.aspx
z	SECNAVINST 5510.34A, Disclosure of Classified Military Information to Foreign Governments, International Organizations, and Foreign Representatives	http://doni.daps.dla.mil/allinstructions.aspx
aa	DoD Directive 5230.20, Visits, Assignments, and Exchanges of Foreign Nationals	http://www.dtic.mil/whs/directives/
bb	OMB Memo M-06-16 of 23 Jun 06, Protection of Sensitive Agency Information	http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2006/m06-16.pdf
cc	DoD CIO memo of 18 Aug 06, Department of Defense (DoD) Guidance on Protecting, Personally Identifiable Information (PII)	DISA Web site: http://iase.disa.mil/policy-guidance/pii-signed-memo-08182006.pdf
dd	USD(P&R) memo of 22 Oct 01, Department of Defense (DoD) Telework Policy and Guide	http://www.cpms.osd.mil/telework.aspx
ee	DoD CIO memo of 3 Jul 07, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media	http://www.doncio.navy.mil/PolicyView.aspx?ID=358
ff	DON CIO message 291652Z FEB 08, Loss of Personally Identifiable Information (PII) Reporting Process	http://www.doncio.navy.mil/PolicyView.aspx?ID=610
gg	DoD Directive O-8530.1, Computer Network Defense (CND)	DISA Web site: http://iase.disa.mil/policy-guidance/index.html#cnd
hh	SECNAVINST 5239.19, DON Computer Network Incident Response and Reporting Requirements	http://doni.daps.dla.mil/allinstructions.aspx

ii	DoD Instruction O-8530.2, Support to CND	DISA Web site: http://iase.disa.mil/policy-guidance/index.html#cnd
jj	SECNAV Manual 5210.1, Department of the Navy Records Management Manual	http://doni.daps.dla.mil/secnavmanuals.aspx
kk	DoD Instruction 8552.01, Use of Mobile Code Technologies in DoD Information Systems	http://www.dtic.mil/whs/directives/
ll	DoD Directive 8190.3, Smart Card Technology	http://www.dtic.mil/whs/directives/
mm	DoD 5200.08-R, Physical Security Program	http://www.dtic.mil/whs/directives/
nn	DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/
oo	DON CIO message 061525Z OCT 04, DON Public Key Infrastructure (PKI) Implementation Guidance	http://www.doncio.navy.mil/PolicyView.aspx?ID=374
pp	DoD Policy Memo of 24 Jan 07, Compliance and Review of Logical Access Control in Department of Defense (DoD) Processes	http://www.doncio.navy.mil/PolicyView.aspx?ID=872
qq	DoD Directive 8521.01E, Department of Defense Biometrics	http://www.dtic.mil/whs/directives/
rr	NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems	http://csrc.nist.gov/publications/PubsSPs.html
ss	STRATCOM Strategic Directive SD-527-1, Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures	DISA Web site: http://iase.disa.mil/policy-guidance/index.html#stratcom
tt	DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP)	http://www.dtic.mil/whs/directives/
uu	DON CIO Memo of 18 Dec 08, Senior Information Assurance Officer Alignment and	http://www.doncio.navy.mil/PolicyView.aspx?ID=825

	Responsibilities for IA and C&A Processes	
vv	OMB Circular A-11, Preparation, Execution, and Submission of the Budget	http://www.whitehouse.gov/omb/search/?keywords=A-11
ww	DoD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System	http://www.dtic.mil/whs/directives/
xx	ASN(RD&A) Memo of 13 Jun 08, Systems Engineering Technical Review Process for Naval Acquisition Programs	http://www.doncio.navy.mil/uploads/ASN_RDA_SETR_Memo_JUN08.pdf
yy	NSTISSP No. 11 Revised Fact Sheet, National Information Assurance Acquisition Policy	http://www.niap-ccevs.org/cc-scheme/nstissp11_factsheet.pdf
zz	DoD Instruction 8523.01, Communications Security (COMSEC) (U)	http://www.dtic.mil/whs/directives/
aaa	DoD M-5220.22, National Industrial Security Program Operating Manual	http://www.dtic.mil/whs/directives/
bbb	DoD Directive 5205.02, DoD Operations Security (OPSEC) Program	http://www.dtic.mil/whs/directives/
ccc	DoD Instruction 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing	http://www.dtic.mil/whs/directives/
ddd	DON CIO Memo of 27 Sep 07, Roles and Responsibilities of the Department of the Navy Deputy Senior Information Assurance Officer for Computer Network Defense (DON Deputy SIAO for CND)	http://www.doncio.navy.mil/Policy.aspx?ID=563

Definitions

Standard definitions are contained in references (c) through (g).

Other and expanded definitions:

1. <u>Computer Network Defense (CND)</u>. Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation or access to computer networks, information systems or their contents or theft of information. CND protection activity employs IA protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND services, intelligence, counterintelligence and law enforcement. CND response can include recommendations or actions by network operations (including IA), restoration priorities, law enforcement, military forces and other US Government agencies. (Reference (gg))

2. <u>Confidentiality Level</u>. Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and "need-to-know" determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels: classified, sensitive, and public. (Reference (f))

3. <u>Contingency Plan (CP)</u>. CPs describe the interim measures used to recover and restore IT systems and service operations following an emergency or system disruption. (Reference (rr))

4. <u>Controlled Unclassified Information (CUI)</u>. Unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended,

but is pertinent to the national interests of the United States
or to the important interest of entities outside the U.S.
Federal Government, and under law or policy, requires protection
from unauthorized disclosure, special handling safeguards, or
prescribed limits on exchange or dissemination. CUI is a generic
term for unclassified information that requires protection,
safeguarding, and access/dissemination control because it is
required to be withheld from public disclosure. The term "CUI"
itself is not a new marking. The proposed new Federal marking
and dissemination framework (aka CUI Framework) will replace
existing unclassified markings (e.g., For Official Use Only
(FOUO)) with new, standard CUI markings. Types of CUI include:

   a. <u>PII</u> Information about an individual that identifies,
relates, or is unique to, or describes him or her (e.g., social
security number, age, military rank, civilian grade, marital
status, race, salary, home/office phone numbers, mother's maiden
name, biometric, personal, medical, financial, and other
demographic data, including any other personal information which
is linked or linkable to a specified individual). (Reference
(cc))

   b. <u>FOUO</u>. In accordance with DoD 5400.7-R of 4 September
1998, DoD information exempted from mandatory public disclosure
under the Freedom of Information Act.

   c. <u>DoD Unclassified Controlled Nuclear Information</u>.
Unclassified information on security measures (including
security plans, procedures, and equipment) for the physical
protection of DoD special nuclear material, equipment, or
facilities in accordance with DoD Directive 5210.83 of 15
November 1991.

   d. <u>Unclassified Technical Data</u>. Data that is not
classified but is subject to export control and is withheld from
public disclosure according to DoD Directive 5230.25 of 6
November 1984.

   e. <u>National Allied Treaty Organization (NATO) or Foreign
Government RESTRICTED Information</u>. Information originated by
NATO or foreign government that is not classified, but requires
protection per reference (x).

f. Department of State Sensitive But Unclassified (DoS SBU). Information that originated from the DoS that has been determined to be SBU under appropriate DoS information security polices.

g. National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION Information. A caveat used by the NGA to identify a select group of sensitive but unclassified imagery or geospatial information, and data created or distributed by NGA or information, data, and products derived from such information.

h. Drug Enforcement Administration (DEA) Sensitive Information. Information that is originated by DEA and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

5. Data at Rest (DAR). Refers to all data in computer storage while excluding data that is traversing a network (data in transit) or temporarily residing in computer memory to be read or updated. DAR can be archival or reference files that are changed rarely or never, or data that is subject to regular but not constant change.

6. Defense-in-Depth/Defense-in-Breadth

a. Defense-in-Depth. The DoD approach for establishing an adequate IA posture in a shared risk environment that allows for shared mitigation through: the integration of people, technology and operations; the layering of IA solutions within and among IT assets; and the selection of IA solutions based on their relative level of robustness. This approach takes the strategic, organization-wide approach, considers the total life cycle of DON IT, and integrates people, technology, and operations to establish variable barriers across multiple layers and dimensions of networks. (Reference (e))

b. Defense-in-Breadth. To mitigate risk from the supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide defense-in-breadth approach. A defense-in-breadth approach helps to protect information systems (including the IT products that compose those systems) throughout the system

development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

8. <u>Demilitarized Zone (DMZ)</u>. Perimeter network that adds an extra layer of protection between internal and external networks by enforcing the internal network's IA policy for external information exchange. A DMZ, also called a "screened subnet," provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. (Reference (f))

9. <u>Designated Accrediting Authority (DAA)</u>. The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with "designated approval authority" and "delegated accrediting authority." (Reference (tt))

10. <u>Global Information Grid (GIG)</u>. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes NSS as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, national security, and related intelligence community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria: (Reference (f))

a. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

b. Provides retention, organization, visualization, IA, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

c. Processes data or information for use by other equipment, software, and services.

11. <u>Information Assurance Manager (IAM)</u>. The individual responsible for the IA program of a DoD information system or organization. While the term "information assurance manager" is favored within the Department of Defense, it may be used interchangeably with the IA title "information systems security manager." (Reference (f))

12. <u>Information Assurance Officer</u>. An individual responsible to the IAM for ensuring the appropriate operational IA posture is maintained for a DoD information system or organization. While the term "information assurance officer" is favored within the Department of Defense, it may be used interchangeably with other IA titles, e.g. "information systems officer," or "terminal area security officer." (Reference (f))

13. <u>Information Operations Condition (INFOCON)</u>. INFOCON is a defense posture and response system for DoD information systems and networks. Note: INFOCON levels are: INFOCON 5- Normal readiness procedures; INFOCON 4 – Increased military vigilance procedures; INFOCON 3 – Enhanced readiness procedures; INFOCON 2 – Greater readiness procedures; and INFOCON 1 – Maximum readiness procedures. (Reference (ss))

14. <u>Interconnection Security Agreement</u>. Written management authorization to interconnect agreement information systems based upon acceptance of risk and implementation of established controls. (Reference (c))

15. <u>Mission Assurance Category (MAC)</u>. Applicable to DoD information systems, the MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MACs

are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined MACs: (Reference (f))

a. <u>MAC I</u>. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

b. <u>MAC II</u>. Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

c. <u>MAC III</u>. Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

16. <u>Mission Critical Information System</u>. A system that meets the definitions of "information system" and "national security system," the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical shall be made by a component head, a combatant commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary

of Defense – Comptroller (USD(Comptroller)). A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System.") (Reference (ww))

17. <u>Mission Essential Information System</u>. A system that meets the definition of "information system", that the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential shall be made by a component head, a combatant commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(Comptroller). A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System.") (Reference (ww))

18. <u>National Security System (NSS)</u>. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which:

    a. Involves intelligence activities;

    b. Involves cryptologic activities related to national security;

    c. Involves command and control of military forces; and

    d. Involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military; or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). Reference (c) quoting section 3542 of title 44, U.S. Code, FISMA of 2002.

19. <u>Operations Security (OPSEC)</u>. Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and

protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: 1) identification of critical information, 2) analysis of threats, 3) analysis of vulnerabilities, 4) assessment of risks, and 5) application of appropriate countermeasures. (Reference (c))

20. <u>Personal Identifiable Information (PII)</u>. Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. (Reference (q))

21. <u>Platform IT</u>. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems including, but not limited to, weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electricity. (Reference (f))

22. <u>Platform IT Interconnection</u>. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Examples of platform IT interconnections that impose security considerations include: communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. (Reference (f))

23. <u>Public Key Infrastructure (PKI)</u>. Framework established to issue, maintain, and revoke PK certificates accommodating a variety of security technologies, including the use of software. (Reference (c))

24. <u>Remote Access</u>. Enclave-level access for authorized users external to the enclave that is established through a controlled access point (e.g., a remote access server or communications server) at the enclave boundary. (Reference (f))

25. <u>Senior Information Assurance Officer (SIAO)</u>. The official responsible for directing an organization's IA program on behalf of the organization's CIO. (Reference (tt))

ACRONYMS

AA/USN	Assistant for Administration/Office of the Under Secretary of the Navy
AIS	Automated Information System
ASN(RD&A)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ATO	Authorization to Operate
C&A	Certification and Accreditation
CAC	Common Access Card
CIO	Chief Information Officer
CND	Computer Network Defense
CNSS	Committee on National Security Systems
COMSEC	Communications Security
CP	Contingency Plan
CUI	Controlled Unclassified Information
DAA	Designated Accrediting Authority
DAR	Data at Rest
DEA	Drug Enforcement Administration
DITPR-DON	DoD Information Technology Portfolio Repository-Department of the Navy
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DoD	Department of Defense
DON	Department of the Navy
DoS	Department of State
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
GCCS	Global Command and Control System
GIG	Global Information Grid
HIPS	Host Intrusion Prevention System
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAM	Information Assurance Manager
IATO	Interim Authorization to Operate
IAVM	Information Assurance Vulnerability Management
IDS/IPS	Intrusion Detection System/Intrusion Protection System
INFOCON	Information Operations Condition
IT	Information Technology
JTF-GNO	Joint Task Force-Global Network Operations

JWICS	Joint Worldwide Intelligence Communications System
MAC	Mission Assurance Category
MAIS	Major Acquisition Information System
MCNOSC	Marine Corps Network Operations and Security Center
NATO	National Allied Treaty Organization
NCDOC	Navy Cyber Defense Operations Command
NCIS	Naval Criminal Investigative Service
NGA	National Geospatial-Intelligence Agency
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
NSTISSP	National Security Telecommunications and Information Systems Security Policy
ODAA	Operational Designated Accrediting Authority
OMB	Office of Management and Budget
OPSEC	Operations Security
PII	Personally Identifiable Information
PK	Public Key
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
SBU	Sensitive But Unclassified
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SIAO	Senior Information Assurance Officer
SIPRNet	Secret Internet Protocol Router Network
SSIC	Standard Subject Identification Code
USSTRATCOM	U.S. Strategic Command
VPN	Virtual Private Network
WiFi	Public Wireless Fidelity