SECNAVINST 5239.3C
DUSN (M) (DON CIO)
2 May 16

SECNAV INSTRUCTION 5239.3C

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CYBERSECURITY POLICY

Ref: See enclosure (1).

Encl: (1) References
       (2) Responsibilities

1. Purpose. This instruction:

    a. Establishes Department of the Navy (DON) policy for cybersecurity (CS) consistent with national and Department of Defense (DoD) CS policy directives and instructions.

    b. Per references (a) and (b), designates the DON Chief Information Officer (DON CIO) as the official responsible for managing the DON's CS program and ensuring compliance with references (a), (b), and (c).

    c. Assigns responsibilities in the DON for developing, implementing, managing, and evaluating DON CS programs, policies, procedures, and controls per reference (c).

2. Cancellation. SECNAVINST 5239.3B

3. Definitions. See references (a), (c), and (d).

4. Applicability. This instruction applies to the offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all subordinate U.S. Navy and U.S. Marine Corps organizations.

    a. This instruction and the accompanying policy manual, reference (e), apply to all DON owned or controlled Information Technology (IT), including IT operated by a contractor or other entity on behalf of the DON.

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

c. This policy shall not alter or supersede the existing authorities and policies of the Director of Naval Intelligence or the Director, National Security Agency regarding the protection of Communications Security (COMSEC), sensitive compartmented information, and special access programs for intelligence that fall under the purview of reference (f).

d. This policy shall not alter or supersede the existing authorities and policies of the Director, Naval Criminal Investigative Service (NCIS) regarding the conduct of counterintelligence and law enforcement investigations, operations, and analysis in the cyber domain pursuant to references (g) and (h).

5. Policy. It is DON policy that:

a. CS Program. The DON Information Assurance Program is renamed the DON Cybersecurity Program. DON CIO will maintain and update reference (e) as necessary to align with this instruction and account for changes in the CS environment.

b. CS Workforce. The DON will employ a trained workforce to achieve the CS capabilities needed to protect DON information. The DON will identify and manage CS workforce functions, and ensure personnel performing CS functions are qualified per references (i), (j), and (k). Dedicated organizations, integrated and coordinated processes, and trusted technologies are vital to an effective CS workforce.

c. Defense-in-Depth/Defense-in-Breadth. DON organizations shall implement a defense-in-depth/defense-in-breadth CS strategy to mitigate information security risks throughout the entire life cycle of a system or network per references (c) and (d). Additionally, commanders of DON organizations must maintain CS situational awareness and ensure compliance with CS policy.

d. Acquisition CS Management

(1) All DON IT must comply with the acquisition guidance in references (l) and (m). DON systems must develop and implement plans to achieve security control objectives as stated in references (c) and (d), and ensure that CS is fully integrated into all phases of acquisition, upgrade, or modification programs, including initial design, development, engineering technical reviews, testing, fielding, and operation.

(2) The DON will employ commercial CS technology in conjunction with government CS technology to meet future DON requirements and deploy CS solutions that support IT interoperability and integration in the DoD.

e. IT Assessment and Authorization

(1) System Categorization. Per reference (c), DON program managers will categorize all DON IT and enter those categorizations into authoritative databases, as directed. A categorization will be determined by the importance of the information in the system to DON missions (particularly the warfighter mission) and not by the cost of CS factors associated with a particular categorization.

(2) Assessment and Authorization. DON organizations shall continually assess the effectiveness of their CS programs and report changes in CS posture to the relevant authorities throughout the life cycle of the system. They should mitigate or remediate emergent CS issues, document changes, and notify appropriate CS stakeholders per references (d), (l), and organizational processes and procedures. This includes, but is not limited to the acquisition, design, development, authorization, operational testing, deployment, and decommission processes. All DON IT shall be assessed and authorized per references (c) and (d). All DON IT must have assigned Authorizing Officials (AOs) and achieve and maintain authorization as defined in reference (d).

(3) Annual Reviews and Tests. All IT must undergo security assessments with annual CS reviews or an approved continuous monitoring strategy per references (a) and (c). Annual reviews must be noted in a system's Federal Information System Modernization Act (FISMA) section of the Department of

Defense Information Technology Portfolio Repository-Department of the Navy (DITPR-DON) and occur within 12 months of the previous completion date. If the AO awards an Authorization to Operate during the year, this suffices for the annual review. However, in succeeding years, the program managers must review the system for any changes that could affect the authorization and take immediate corrective action to address shortfalls, document changes to the system, and notify appropriate CS stakeholders according to organizational processes and procedures. If immediate corrective actions cannot be taken, the program manager must update the IT security plan of action and milestones to include future corrections, and if applicable, initiate appropriate reauthorization actions.

    f. <u>COMSEC</u>

      (1) The DON shall use COMSEC measures and procedures to protect the confidentiality and integrity of Classified National Security Information (CNSI) and Controlled Unclassified Information (CUI) that has not been approved for public release. DON organizations shall execute COMSEC policy and procedures established by DoD and the Committee on National Security Systems (CNSS), per references (n) and (o).

      (2) The DON shall use COMSEC monitoring and CS readiness testing to assess the contents and value of government information subject to loss or exploitation activities, in compliance with reference (p).

    g. <u>Information Security</u>. DON organizations shall properly classify, mark, safeguard, transmit, destroy, and ensure prompt management action and reporting of all security incidents for CNSI and CUI, including Personally Indentifiable Information breaches per references (f) and (q) through (v).

    h. <u>Operations Security (OPSEC)</u>. DON organizations shall establish OPSEC programs focused on command involvement, assessments, surveys, training, education, vulnerability, threat, resourcing, awareness, and monitoring, per reference (w).
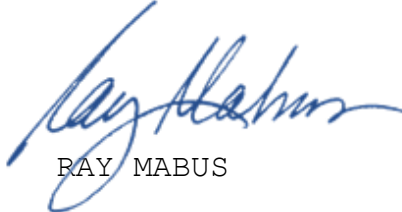
    i. <u>Insider Threat</u>. The DON shall establish an integrated set of policies and procedures to deter, detect, and mitigate

insider threats before damage is done to national security, personnel, resources and/or capabilities, as defined in reference (x).

6. <u>Responsibilities</u>. See enclosure (2).

7. <u>Records Management</u>. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012.

8. <u>Reports</u>. The reporting requirements contained in paragraphs 5g and 5h of the instruction, and enclosure (2) paragraphs 1b, 1f, 1g, 1k, and 1o are exempt from reports control per SECNAV M-5214.1 of December 2005, Part IV, paragraphs e, g, and o.

RAY MABUS

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

REFERENCES

a. 44 U.S.C. Chapter 35, Subchapter II
b. SECNAVINST 5430.7Q
c. DoD Instruction 8500.01 of 14 March 2014
d. DoD Instruction 8510.01 of 12 March 2014
e. SECNAV M-5239.1, Department of the Navy Information Assurance Manual
f. DoD Instruction 5200.01, Change 1 of 13 June 2011
g. SECNAVINST 5430.107
h. SECNAVINST 3850.2C
i. SECNAVINST 5239.20
j. DoD Directive 8570.01 of 15 August 2004
k. DoD 8570.01-M, Information Assurance Workforce Improvement Program Manual, December 2005
l. SECNAVINST 5000.2E
m. DoD Instruction 5000.02 of 7 January 2015
n. CNSSI No. 4005, Safeguarding COMSEC Facilities and Materials of 22 August 2011
o. DoD Instruction 8523.01 of 22 April 2008
p. DoD Instruction 8560.01 of 9 October 2007
q. SECNAV M-5510.36, Department of the Navy Information Security Program
r. DoDM 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification of February 2012
s. DoDM 5200.01, Volume 2, DoD Information Security Program: MARKING OF CLASSIFIED INFORMATION of February 2012
t. DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information of February 2012
u. DoDM 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI) of February 2012
v. SECNAVINST 5211.5E
w. DoD Directive 5205.02E of 20 June 2012
x. SECNAVINST 5510.37
y. NIST SP 800-37, Guide for Applying the Rise Management Framework to Federal Information Systems: A Security Life Cycle Approach of February 2010
z. DoD Directive 8521.01E of 21 February 2008
aa. SECNAVINST 5000.36A
ab. CJCSM 6510.01B, Cyber Incident Handling Program of 10 July 2012
ac. SECNAVINST 5239.19
ad. DoD Instruction O-8530.2 of 9 March 2001

ae. SECNAV M-5510.30, Department of the Navy Personnel Security
    Program
af. CNSSP-8 of 1 August 2012
ag. DoD Directive 5230.20 of 22 June 2005
ah. DoD Memorandum, Cross Domain Support Element (CDSE)
     Responsibilities, of 11 October 2011

RESPONSIBILITIES

1. The DON CIO shall:

    a. Carry out the CS responsibilities assigned by reference (a) to the head of each federal agency per reference (c). Accordingly, the DON CIO shall ensure DON compliance with the CS requirements of references (a), (b), (c), and related policies, procedures, standards, and guidelines.

    b. Maintain situational awareness and report CS/Computer Network Defense (CND) issues and significant incidents as necessary to the SECNAV per reference (a).

    c. Designate a DON Senior Information Security Officer (SISO) (formerly Senior Information Assurance Officer) to manage the DON CS program per references (a) and (d).

    d. Designate AOs for DON IT and ensure compliance with Risk Management Framework (RMF) requirements per references (c) and (d).

    e. Ensure implementation of DON Insider Threat Program requirements as defined in reference (x).

    f. Ensure DON officials provide CS protections for DON IT that supports operations and assets, including Industrial Control Systems. These CS protections shall include assessment, determining appropriate levels of CS, implementing policies and procedures to cost-effectively reduce risks to an acceptable level, and periodic testing and evaluation of CS controls and techniques to ensure effective implementation.

    g. Immediately refer to the NCIS any incidents of actual, suspected, or alleged criminal offenses; including espionage, acts of terrorism, and all instances of suspicious activities or anomalies that might indicate the involvement of a foreign government or terrorist organization. Referrals must be made prior to any substantive investigation by the command unless investigative actions are necessary to protect life or property, or to prevent the destruction of evidence. The requirement for immediate referral shall not preclude efforts by first responders to safeguard personnel, secure crime scenes, or take other appropriate action.

h. Set DON standards and policy for CS workforce education, training (including user awareness), certification, and management requirements commensurate with responsibilities regarding DON IT.

i. Collaborate with appropriate stakeholders on the integration of CS requirements with DON strategic and operational planning and with the DON acquisition management process.

j. Ensure coordination of CS/CND issues within the DON, and externally with other Military Departments, Defense Agencies, and the DoD.

k. Evaluate annually the effectiveness of the DON CS Program per reference (a) and provide input to the DoD CIO for a collective report on CS as part of the annual FISMA report.

l. Define DON CIO reportable metrics in coordination with DON Services and organizations. Metrics must illustrate the adequacy of DON CS/CND efforts.

m. Coordinate with the DON Auditor General for recommendations for CS audits and reviews.

n. Review CS strategies for major defense acquisition programs and major automated information systems, per reference (l).

o. Report periodically, in coordination with other senior officials, to the SECNAV on the effectiveness of the DON CS Program.

p. Ensure compliance with DoD identity management policy, timelines, and processes throughout the DON.

q. Ensure coordination of risk management across DON Services and organizations by balancing threat against system and/or data criticality to identify and implement practical solutions.

r. Mandate a robust program within the DON for conducting vulnerability assessments, threat modeling, penetration testing, and lessons learned, including effective use of red team exercises.

s. Participate in the DoD Cybersecurity Enterprise Capabilities Steering Group (formerly Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group) process, as defined in reference (c), to ensure capabilities acquired or developed support CS objectives and organizational requirements.

t. Provide management, oversight, and direction for the DON High Risk Escalation Process and provide approval for systems that have a High or Very High level of risk per reference (d).

u. Coordinate with the Assistant Secretary of the Navy (ASN), Research, Development and Acquisition (RD&A) to ensure CS responsibilities are integrated into processes for DON acquisition programs, including research and development.

v. Coordinate with the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate to ensure CS policies and capabilities are aligned with and mutually supportive of personnel, physical, industrial, information, and OPSEC policies and capabilities.

2. The DON SISO shall:

a. Ensure all enterprise-wide systems comply with requirements of applicable DON, DoD, and Federal policies and mandates, such as references (a) through (d).

b. Serve as a single CS coordination point for DON organizations responsible for Joint or Defense-wide programs implemented on DON enterprise networks.

c. Establish a reporting relationship between the DON CIO and the Navy and Marine Corps to ensure coordination on CS.

d. Implement and enforce the RMF for DoD IT within the DON CS Program.

e. Track the RMF Assessment and Authorization status of information systems governed by the DON CS Program via automated tools.

f. Formally delegate Security Control Assessor duties.

g. Ensure CS assessment quality, capacity, visibility, and effectiveness by providing oversight and approval to DON organizations' implementation of and process for the RMF.

h. Facilitate a consistent application of CS policies, processes, responsibilities, and procedures throughout the DON.

i. Ensure consistent application of CS related waiver standards and request processing among DON enterprise networks.

j. Establish and chair a DON-level enterprise CS governance board responsible for carrying out the Risk Management Executive function per reference (y).

k. Designate DON Deputy SISOs (Service SISOs) as warranted and provide authority to appoint Service AOs and Service Security Control Assessors after coordination with DON CIO.

3. ASN (RD&A) shall:

a. Issue DON acquisition policies providing implementation details and procedures to support CS.

b. In collaboration with DON CIO and other appropriate entities, ensure the integration of CS requirements into acquisition management of all DON acquisition programs throughout their life cycle per reference (c).

c. Maintain science and technology efforts in CS, per reference (a).

d. Ensure all new acquisitions or upgrades of electronic biometric collection systems conform to the Federal and DoD electronic biometric transmission specification per reference (z).

4. ASN, Manpower and Reserve Affairs shall issue DON manpower and personnel policies and ensure accurate authoritative manpower data supports CS.

5. DUSN (P) Security Directorate shall collaborate on the development and implementation of DON CS policy, guidance, procedures, and controls where an integration of requirements are required for traditional security related to personnel, physical, industrial, information, insider threat, and operation security.

6. The DON/Assistant for Administration, CNO, and CMC shall:

    a. Require that qualifying IT systems be registered in DITPR-DON, per references (l) and (aa) and periodic DITPR-DON guidance issued by the DON CIO.

    b. Ensure that CS/CND is implemented throughout the life cycle of all DON IT assets, including design, acquisition, installation, operation, upgrade, replacement, or retirement.

    c. Establish and validate CS/CND requirements and coordinate CS requirements that cross boundaries per reference (c).

    d. Ensure CS/CND costs are budgeted in DON IT programs and IT system acquisitions, per reference (l).

    e. Provide for CS vulnerability assessment, vulnerability mitigation, and incident response and reporting per references (c), (ab), (ac), and (ad).

    f. Ensure procurement and use of identity and access management capabilities, e.g., Common Access Card, Public Key Infrastructure, and biometrics, compliant with DoD policy, standards, and specifications as cited in reference (c), to include interoperability.

        (1) Ensure all information systems, including networks, e-mail, and web servers that host information not approved for public release implement person and non-person entity identity standards, i.e., device, services, authentication, per reference (c) and its references.

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

(b) Enforce encryption of e-mail or web server transactions containing CUI and Controlled Technical Information, per requirements in reference (u).

(2) Ensure all new acquisitions or upgrades of electronic biometric collection systems conform to the Federal and DoD electronic biometric transmission specification per reference (z).

g. Ensure notification to 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, per reference (p).

h. Ensure individual and organization accountability under their purview, including:

(1) Holding Commanders, Information System Owners, AOs, Information Systems Security Managers, Information System Security Managers, Program Managers, Project and Application Leads, Supervisors, and System Administrators responsible and accountable for the implementation of DoD security requirements per this instruction and supplemental DoD and DON guidance.

(2) Ensuring military and civilian personnel are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk DoD and DON information by not ensuring implementation of DoD and DON security requirements per this instruction, other DoD 8500 series directives and instructions, DoD 5200 series instructions and publications, and supplemental DON policies and procedures.

7. In addition to responsibilities above, CNO and the CMC shall:

a. Develop and implement CS/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 organization.

b. Identify, train, and certify all personnel performing CS functions, regardless of job series or military specialty.

(1) Implement DoD CS awareness training. Ensure all authorized users of DON information systems and networks receive initial CS awareness orientation as a condition of access and, thereafter, complete annual refresher training to maintain CS awareness.

(2) Monitor and report workforce CS 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 CS workforce; and use, to the extent possible, existing databases and tools to satisfy these CS reporting requirements.

(3) Develop CS training consistent with the minimum standards published in references (j) and (k), to specific job roles and functions.

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

c. Set policies and procedures to control access by foreign nationals to classified and unclassified information, and local area networks and information assets, consistent with references (c), (ae), (af), and (ag).

d. Implement standard formats to identify foreign nationals and contractors in all forms of communications, including e-mail, per reference (c).

e. Mandate penetration, internal hunting, and staff assist Computer Defense operations within DON organizations. Ensure results are reported to AOs, DON CIO, and other organizational CS stakeholders.

f. Review Service CS/CND status annually to ensure it is fully consistent with the DON CS policy. Report these findings to the DON CIO.

g. Establish a Cross Domain (CD) Support Element (CDSE) to coordinate enterprise CD activities with the Unified Cross Domain Services Management Office (UCDSMO) per DoD CIO Memorandum (Reference (ah)), and ensure transition from using Cross Domain Solutions (CDSs) on the UCDSMO-managed CDS Sunset List to using CDSs on the UCDSMO-managed CDS Baseline List.

h. Ensure CS efforts are aligned with and informed by DoD Mission Assurance efforts.

i. Serve as the resource sponsor for cryptographic requirements, following the guidelines of reference (o), based on DON priorities.

8. Program Executive Officer for Command, Control, Communications, Computers, and Intelligence (PEO C4I) is the central DON procurement authority for all DON high assurance COMSEC and key management infrastructure.

9. The Director, NCIS, shall:

a. Conduct all felony-level investigations, operations and analysis of criminal or foreign intelligence related cyber incidents, and targeting involving DON IT assets and/or personnel. This includes root level intrusions, user level intrusions, denial of service, malicious logic incidents, and aforementioned suspected incidents per reference (ab). Provide recommendations based on analysis of forensics to the DON CIO for incorporation into potential CS/CND policy.

b. Collect, track, and report criminal and foreign intelligence entity threats to DON IT assets and disseminate this information to other law enforcement agencies, DoD, DON, DON CIO, CMC, CNO, and other national agencies as appropriate.

c. Train and maintain a multidisciplinary staff skilled in tactics, techniques, and procedures associated with activities above, to include digital forensics and technical support to operations, investigations, and analysis. Identify resource

requirements to NCIS resource sponsor(s) to ensure handling of multiple major incidents and in response to growing demands of the DON.