DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5239.22
ASN (RD&A)
15 Nov 16

SECNAV INSTRUCTION 5239.22

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CYBERSECURITY SAFETY PROGRAM

Ref: (a) DoD Instruction 8500.01 of 14 March 2014
(b) SECNAVINST 5239.3C
(c) SECNAVINST 5400.15C CH-1
(d) SECNAVINST 5430.7Q
(e) DoD Instruction 5000.02 of 7 January 2015

1. Purpose. This instruction establishes policy and assigns responsibilities for the development, management, and implementation of the Department of the Navy (DON) Cybersecurity Safety (CYBERSAFE) Program. CYBERSAFE shall provide for enhancements and cybersecurity requirements and measures beyond those directed in references (a) and (b). This instruction is an original issue and should be reviewed in its entirety.

2. 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 U.S. Navy and U.S. Marine Corps organizations. Execution of CYBERSAFE responsibilities shall align to the relationships defined in references (c) and (d).

3. Policy. CYBERSAFE is distinct from, but highly integrated with, DON cybersecurity. The CYBERSAFE program shall provide maximum reasonable assurance of survivability and resiliency of mission critical information technology (IT), as defined in reference (e), in a contested cyber environment in order to maintain mission capabilities. CYBERSAFE will provide enhanced protection and resiliency to critical IT and include components and processes, material and software solutions, and procedures adequate to protect, defend, and restore those capabilities without abruptly or unexpectedly impacting mission.

a. CYBERSAFE shall apply to mission critical IT within the DON infrastructure to ensure mission assurance across the lifecycle; including in-service capabilities.

b. The CNO and CMC shall integrate and synchronize their CYBERSAFE programs.

4. Responsibilities

a. The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RD&A)) shall:

(1) In coordination with CNO, CMC, and Department of the Navy Chief Information Officer (DON CIO) establish a CYBERSAFE governance process.

(2) Coordinate and provide recommendations and resolutions to the CNO and CMC for CYBERSAFE investment, policy, and strategy.

b. The CNO and CMC shall:

(1) Establish Service CYBERSAFE programs at the Systems Command (SYSCOM) level that shall:

(a) Identify mission critical IT.

(b) Develop operational strategies to implement CYBERSAFE in a contested environment.

(c) Implement and ensure execution.

(2) Issue implementing directives to ensure effective and efficient execution and continuous improvement of the CYBERSAFE program.

(3) Oversee the execution of the Services' CYBERSAFE activities, plans, and strategies.

(4) In coordination with ASN(RD&A) and DON CIO, establish a CYBERSAFE governance process.

(5) Identify a Service CYBERSAFE responsible agent to implement and execute the CYBERSAFE program.

(6) Establish policy to incorporate CYBERSAFE into leadership briefings such as Resources and Requirements Review Boards and Operational Test Readiness Reviews.

c. The DON CIO shall:

(1) Participate in the CYBERSAFE governance process.

(2) In coordination with the Services' CYBERSAFE programs, establish policy to strengthen authority, accountability, and rigor in cybersecurity.

d. The Deputy Under Secretary of the Navy for Policy shall participate in the CYBERSAFE governance process to align DON CYBERSAFE efforts with Department of Defense/Joint Chiefs of Staff overarching cybersecurity and/or mission assurance initiatives.

e. The Assistant Secretary of the Navy for Energy, Installations & Environment shall participate in the CYBERSAFE governance process.

f. Program Executive Offices shall implement the CNO/CMC CYBERSAFE programs in coordination with the appropriate SYSCOM(s).

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

RAY MABUS

Distribution:
Electronic only, via DON Issuances Website
http://doni.documentservices.dla.mil/default.aspx