



DEPARTMENT OF THE NAVY
UNITED STATES NAVAL ACADEMY
121 BLAKE ROAD
ANNAPOLIS MARYLAND 21402-1300

USNAINST 8510.01
6/ITSD
20 Jan 2016

USNA INSTRUCTION 8510.01

From: Superintendent, United States Naval Academy

Subj: CYBERSECURITY RISK MANAGEMENT

Ref: (a) DoDI 8510.01 Risk Management Framework for DoD Information Technology
(b) FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems
(c) USNAINST 5230.1A Information Technology and Cybersecurity Policy and Standards
(d) Navy Authorizing Official and Security Control Assessor Risk Management Framework Process Guide, 31 Aug 2015
(e) Navy Higher Education Cybersecurity Concept of Operations dated 5 Dec 2014
(f) USNAINST 5321.1C Life Cycle Management Policy
(g) USNAINST 7320.10 USNA Management of Personal Property

1. Purpose. This instruction establishes the Cybersecurity Risk Management policy for the United States Naval Academy (USNA).

2. Authority. Per reference (a), all Department of Defense (DoD) Information Technology (IT) that receives, processes, stores, displays, or transmits DoD information including IT supporting research, development, test and evaluation, and IT operated by a contractor on behalf of the DoD shall be under the governance of a Cybersecurity program. Reference (b) applies to all federal information systems and information within the federal government, except as noted in the reference.

3. Policy. All IT resources and IT services as defined in reference (c), and all information transmitted by or created, processed, or stored on these IT resources and IT services,

20 Jan 2016

acquired by or for USNA or any USNA-supported entity, regardless of funding source or provenance, including cloud services and commercial Internet Service Provider (ISP) services, shall be managed with respect to Cybersecurity risk per references (a) through (g).

4. Responsibilities. Risk management responsibilities are defined in reference (d) and assigned by role as follows:

a. Per reference (e), the USNA Deputy for Information Technology/Chief Information Officer (CIO) is the delegated approval authority for granting or denying permission to operate USNA information systems, subsystems, and individual IT components. The Deputy for IT/CIO functions as the Authorizing Official (AO) per reference (d).

b. AO Cybersecurity Analysts support the Configuration Control Board, which makes risk-based recommendations as to security controls, benchmarks, checklists or mitigations to implement or apply, and conduct risk impact analysis for proposed and unexpected changes related to secure baseline configurations.

c. The Security Control Assessor (SCA) is the Information Technology Services Division (ITSD) Deputy Director for Cybersecurity, and maintains oversight of the risk assessment process.

d. The SCA Liaison is assigned by the AO. The SCA Liaison assists the SCA, provides guidance to validators, and is responsible for documenting the risk management process.

e. Validators are the members of the ITSD Cybersecurity Department who perform assessment of risk controls and participate in continuous risk monitoring.

f. Information System Owners (ISO) are ITSD Deputies, Division Directors, and others who manage business processes or

mission support information systems, who ensure configuration management policies and procedures are implemented and enforced for cognizant information systems. ISOs also participate in risk assessment.

g. Information Owners (IO) are USNA Cost Center Heads and others who manage information at the business process level. IOs define and convey information system functional requirements and participate in risk assessment.

h. The Information System Security Manager (ISSM) is designated in writing by the AO and is the primary Cybersecurity technical advisor to the AO. The ISSM monitors compliance, provides oversight to ISSO, ensures secure configuration of IT products and services prior to acceptance, and participates in risk assessment and security impact analysis.

i. Information System Security Officers (ISSO) are ITSD Associate Deputies, Department Chairs, and others who manage information at the information system component level (e.g., server, appliance). ISSOs manage implementation and enforcement of configuration management policies and procedures for cognizant information systems, perform configuration monitoring activities, and assist with risk assessment and security impact analysis.

j. Information System Security Engineers (ISSE) are USNA enterprise Software Developers and System Administrators in the Cybersecurity Workforce. Software Developers ensure configuration settings are built into developed applications per configuration management requirements, and assist with risk assessment, security impact analysis, and configuration monitoring. System Administrators implement baseline configurations and configuration changes, and assist with risk assessment, security impact analysis, and configuration monitoring.

20 Jan 2016

k. Privileged Users can install software or make changes to configuration settings and are responsible for obtaining required approval before making configuration changes.

l. Non-privileged Users assist with functional testing and are responsible for informed, secure IT operational behavior/cyber hygiene.

5. Action

a. The USNA Deputy for Information Technology/CIO shall issue directives, notes, memoranda, and/or standard operating procedures as required to implement the USNA Cybersecurity program.

b. All IT acquisition requests regardless of the funding source or provenance, shall be forwarded to ITSD per references (c), (f), and (g). For items under configuration management, approval is contingent upon favorable risk and financial determinations.

c. Existing ITs will transition Cybersecurity management from the Defense Information Assurance Certification and Accreditation Process policy framework to Risk Management Framework policy per reference (d) and additional guidance issued by the USNA Deputy for Information Technology/CIO.

d. All hands shall comply with the Cybersecurity policies and procedures issued by USNA's Deputy for Information Technology/CIO.


W. E. CARTER, JR

Distribution:
Non Mids (electronically)
Brigade (electronically)