



ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

FEB 18 2020

SUSTAINMENT

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Managing Cyber Risks to Facility-Related Control Systems

REFERENCES: (a) Department of Defense (DoD) Instruction 8500.01, "Cybersecurity," March 2014
(b) DoD Instruction 8510.01, "Risk Management Framework," March 2014
(c) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 2017
(d) Deputy Secretary of Defense Memorandum, "Enhancing Cybersecurity Risk Management for Control Systems Supporting DoD-Owned Defense Critical Infrastructure," July 19, 2018
(e) Chief Information Officer Memorandum, "Control Systems Cybersecurity," December 18, 2018

Cyber vulnerabilities continue to jeopardize critical infrastructure that enables DoD operations. Unsecured control systems can lead to mission failure, decreased operational effectiveness, and physical damage to critical infrastructure. Additionally, they can expose connected DoD information networks to risk. Per references (a) through (c), system owners and operators are accountable for system operational resilience and cybersecurity defense posture.

In response to references (d) and (e), the Department increased initiatives to cyber-secure mission-critical Facility-Related Control Systems (FRCS). As part of this Department-wide effort, I request that Components and Defense Agencies provide updated FRCS Cybersecurity Plans that cover Fiscal Years 2020-2026. Components should prioritize the completion of cybersecurity plans for FRCS that:

- 1) Support Defense Critical Assets and Tier 1 Task Critical Assets; and
- 2) Systems that connect to the DoD Information Network, are internet-facing and/or stand-alone, and require an Authorization to Operate.

Please use the attached guidance and template in developing your FRCS Cybersecurity Plans. Plans submitted in other formats will not be accepted. Please submit your plans by April 30, 2020, to my point of contact, Ms. Teria Cason, teria.b.cason.civ@mail.mil, or 571-256-0793.

Thank you for your continued support to improve the Department's FRCS resilience and security posture.



Peter J. Potochney
Acting

Attachments:
As stated

DISTRIBUTION:

ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS, ENERGY AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE NAVY (ENERGY, INSTALLATIONS AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (INSTALLATIONS, ENVIRONMENT AND ENERGY)
DIRECTOR, DEFENSE LOGISTICS AGENCY (INSTALLATION SUPPORT)
DIRECTOR, MISSILE DEFENSE AGENCY (FACILITIES, MILITARY CONSTRUCTION AND ENVIRONMENTAL LIABILITIES)
CHIEF, NATIONAL SECURITY AGENCY (INSTALLATION LOGISTICS)
CHIEF, DEFENSE HEALTH AGENCY (FACILITIES DIVISION)
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (FACILITIES SERVICES DIRECTORATE)
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (SECURITY AND INSTALLATIONS DIRECTORATE)
PROGRAM MANAGER, DEFENSE INTELLIGENCE AGENCY (INDUSTRIAL CONTROL SYSTEMS)
DIRECTOR, DEFENSE COMMISSARY AGENCY (INFRASTRUCTURE SUPPORT)
CHIEF, DEPARTMENT OF DEFENSE EDUCATION ACTIVITY (FACILITIES)

COPY TO:

DOD CHIEF INFORMATION OFFICER
COMPONENT CIOs
JOINT STAFF/J-3/J-6
DEPUTY COMMANDER, US CYBER COMMAND
DEPUTY COMMANDER, STRATEGIC COMMAND
ASSISTANT CHIEF OF STAFF FOR INSTALLATION MANAGEMENT, ARMY
DIRECTOR OF CIVIL ENGINEERS, AIR FORCE
COMMANDER, U.S. ARMY CORPS OF ENGINEERS
COMMANDER, NAVAL FACILITIES ENGINEERING COMMAND
DIRECTOR, SHORE READINESS (OPNA V N46)
DIRECTOR, USACE CRITICAL INFRASTRUCTURE CYBER SECURITY
CHIEF, USACE INSTALLATION SUPPORT DIVISION DIRECTORATE OF MILITARY PROGRAMS