



ENERGY,
INSTALLATIONS,
AND ENVIRONMENT

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

3400 DEFENSE PENTAGON
WASHINGTON, DC 20301-3400

MAR 31 2016

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Managing Cyber Risks to Facility-Related Control Systems

REFERENCES: a) DoD Instruction (DoDI) 8500.01, *Cybersecurity* (March, 2014)
b) DoDI 8510.01, *Risk Management Framework (RMF)* (March, 2014)
c) DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (March, 2016)
d) Deputy Secretary of Defense Memo, *Mission Assurance Assessment Program Interim Implementation*, April 2015
e) National Institute of Standards and Technology Special Publication 800-82 revision 2, *Guide to Industrial Control Systems Security* (May, 2015)

Cyber-attacks on DoD Information Technology (IT) demonstrate the need for continuous vigilance and effective defensive measures. Per references (a) through (c), system owners and operators are accountable for system operational resilience and cybersecurity defense posture. To that end, your staffs shall develop plans identifying the goals, milestones and resources needed to identify, register, and implement cyber security controls on DoD facility-related control systems under your cognizance.

Plans shall be submitted to the point of contact listed below by December 31, 2016, and shall identify steps to obtain required resources and mitigate vulnerabilities per reference (b). The goal is to implement cybersecurity controls on the most critical facility-related control systems by the end of Fiscal Year 2019, giving priority to:

- 1) Supporting Defense Critical Assets and Tier 1 Task Critical Assets per reference (d); and
- 2) Those control systems that connect to the DoD Information Network, are Internet-facing and/or stand-alone, and require an authorization to operate.

Managing life-cycle cybersecurity risk to DoD IT, per reference (e) will require considerable collaboration among control systems stakeholders: installation/facility control engineers and operators; physical security, information network and system security expert(s); and when applicable, control system vendors and system integrators. Resources for implementing the RMF and registering facility-related control systems are available at the RMF Knowledge Service portal (<https://rmfks.osd.mil>). My point of contact is Mr. Daryl Haegley, daryl.r.haegley.civ@mail.mil or (571) 372-6857.



Peter Potochney

Deputy Assistant Secretary of Defense (Basing)
Performing the Duties of the Assistant Secretary of Defense
(Energy, Installations, and Environment)

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 COMMISSARY AGENCY (INFRASTRUCTURE SUPPORT)
DIRECTOR, DEFENSE LOGISTICS AGENCY (INSTALLATION SUPPORT)
DIRECTOR, MISSILE DEFENSE AGENCY (FACILITIES, MILITARY CONSTRUCTION AND ENVIRONMENTAL LIABILITIES)
DIRECTOR, NATIONAL SECURITY AGENCY (INSTALLATION LOGISTICS)
CHIEF, DEPARTMENT OF DEFENSE EDUCATION ACTIVITY (FACILITIES)
DIRECTOR, DEFENSE HEALTH AGENCY (PORTFOLIO PLANNING AND MANAGEMENT DIVISION)
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (FACILITIES SERVICES DIRECTORATE)

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 (OPNAV N46)
DIRECTOR, USACE CRITICAL INFRASTRUCTURE CYBER SECURITY
CHIEF, USACE INSTALLATION SUPPORT DIVISION DIRECTORATE OF MILITARY PROGRAMS