



OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION,
TECHNOLOGY,
AND LOGISTICS

MAR 19 2014

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Real Property-related Industrial Control System Cybersecurity

The Department's computer networks and systems are under incessant cyber attack, and specific steps are underway to implement trustworthy cybersecurity practices. Recognizing the increased threats, vulnerabilities, and risks the Department recently updated the Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity* on March 14, 2014, and the DoDI 8510.01, *Risk Management Framework* on March 12, 2014. For the first time, these instructions mandate that Industrial Control Systems (ICS) be made secure against cyber attacks by implementing a Risk Management Framework (RMF).

Real property-related ICS includes, but is not limited to, building automation systems, energy/utility monitoring and control systems, computerized controllers on heating, ventilation and air conditioning equipment, smart meters, etc. Damage to or compromise of any ICS may be a mission disabler. For example, disruption of a computerized chiller controller could deleteriously impact critical military operations and readiness. A more serious mission disabling event could occur if the ICS was used as a gateway into the installation's Information Technology system or possibly the Department's broader information networks.

Implementing specific tailored real property-related ICS cybersecurity controls within the RMF envisioned in DoDI 8510.01 can mitigate cyber risks. Your team's cybersecurity efforts can be validated using a standard assessment tool, such as the Department of Homeland Security's Cyber Security Evaluation Tool. The tool can be downloaded from: <http://ics-cert.us-cert.gov/Downloading-and-Installing-CSET>.

To strengthen our engineering standards, we established a new Unified Facilities Criteria working group tasked to publish design criteria for real property-related ICS equipment and systems. Your team's involvement in this working group would be appreciated, and we request your ICS expert contact our Point of Contact (POC) for details. Our POC is Mr. Daryl Haegley and may be reached at daryl.r.haegley.civ@mail.mil or 571-232-2754.

John Conger
Acting Deputy Under Secretary of Defense
(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 LOGISTICS)
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 & MANAGEMENT DIVISION)
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (FACILITIES SERVICES DIRECTORATE)

COPY TO:

DOD CHIEF INFORMATION OFFICER
JOINT STAFF/J-3
DEPUTY COMMANDER, US CYBER COMMAND
DEPUTY COMMANDER, STRATEGIC COMMAND
ASSISTANT CHIEF OF STAFF FOR INSTALLATIONS MANAGEMENT
THE AIR FORCE CIVIL ENGINEER
COMMANDER, U.S. ARMY CORPS OF ENGINEERS
COMMANDER, NAVAL FACILITIES ENGINEERING COMMAND