



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

OCT 10 2013

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL
SECURITY SERVICE

SUBJECT: Safeguarding Unclassified Controlled Technical Information

The Department of Defense (DoD) is committed to protecting our unclassified controlled technical information against the threat of cyber intrusions that target the Department and our industrial base. Stolen data provides potential adversaries extraordinary insight into the United States' defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. Protection of this data is a high priority for the Department and is critical to preserving the intellectual property and competitive capabilities of our national industrial base and the technological superiority of our fielded military systems.

In order to ensure our unclassified controlled technical information is protected from cyber intrusions and that any consequences associated with loss of this information are minimized, I am directing the following actions which will augment our ongoing activities in this area:

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in coordination with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence (USD(I)), and the DoD Chief Information Officer (CIO), shall take immediate action to improve the protection of unclassified controlled technical information that resides on or passes through defense contractor systems or networks. This shall include necessary policy, guidance, and rulemaking activities, to include expansion of current cybersecurity information-sharing activities and programs. USD(AT&L) shall propose an amendment to the Defense Federal Acquisition Regulation Supplement for defense contractors to safeguard unclassified controlled technical information.

USD(AT&L), with the support of USD(I), USD(P), the Defense Intelligence Agency, the Joint Staff, U.S. Strategic Command (USSTRATCOM), and the Military Departments, shall



OSD071338-13

establish a joint analysis capability to assess technical information losses and determine consequences of those losses in order to inform requirements, acquisition, programmatic, and strategic courses of action.

The Military Departments, in coordination with the Joint Staff, USD(AT&L), and DoD CIO, shall identify critical acquisition and technology programs requiring higher levels of protection. USD(I) shall lead the Services in a review of the classification guidance for these programs to ensure adequate security protection is provided for technical information associated with these programs.

DoD CIO, along with the National Security Agency and the Defense Information Systems Agency, shall continue to identify technical standards for protecting unclassified information and align these standards with the DoD Joint Information Environment single security architecture. In coordination with the Components and DoD CIO, USSTRATCOM shall conduct an assessment of unclassified DoD-operated networks to determine their vulnerability to cyber attack, and, in collaboration with DoD CIO, provide risk mitigation action plans to reduce identified vulnerabilities to an acceptable level.

USD(AT&L) and DoD CIO shall monitor the effectiveness of these actions and recommend further actions, as needed.

These actions will ensure that the Department provides a cohesive, comprehensive, and cost-effective approach to protect priority investments and future defense capabilities while maintaining efficient business operations with our industrial partners.

Thank you.

*Cyber
HAGER*
/

cc:
DepSecDef