



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

NOV 18 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
COMMANDERS OF THE COMBATANT
COMMANDS
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES
ATTN: COMPONENT ACQUISITION EXECUTIVES

SUBJECT: Cyber Security in Defense Acquisition Programs

The Department of Defense (DoD) and the Defense Industrial Base (DIB) face enormous challenges in protecting sensitive or controlled unclassified information developed and used in support of DoD acquisition programs. In particular, the increased reliance on the internet as a vehicle for sharing and storing information has exposed DoD and DIB unclassified networks to unprecedented risks to our information security. The DoD and the DIB must collaborate more effectively to address these risks and to secure our current and future warfighting capabilities.

The DoD has adopted a phased approach to engaging with the DIB to improve protections for defense program information (DPI). DoD initiated improved communications with the DIB under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) to address the critical need to improve information sharing regarding security of unclassified networks. Specific information sharing procedures have been implemented through the DIB Cyber Security Task Force (DIBCS-TF) Framework Agreements (FA), or through individual program contracts.

Given the seriousness of the threat, we must now move to the next phase of our collaborative effort to improve DoD-DIB cyber security. Acquisition Executives must engage their Program Executive Offices (PEOs) and Program Managers (PMs) to take immediate steps to ensure that DPI is appropriately identified and protected in all DoD acquisition programs. The following principles will guide our near term approach:



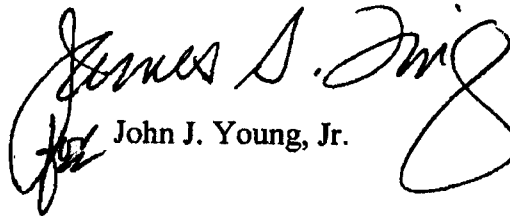
a. PMs must develop and implement information security requirements that are appropriate for the sensitivity of the information in their programs. At the next available opportunity, PMs will engage with their DIB partners to ensure that information security requirements included in contracts appropriately address the need to report any compromise, loss, or exfiltration of DPI, to participate in information sharing processes, and to provide adequate cyber security as a standard practice. PMs must also ensure a clear assignment of responsibility within the government for reviewing information security planning and monitoring compliance with contract information security requirements.

b. PMs must take advantage of the most current available information regarding cyber security threats, vulnerabilities, and best practices. Information on basic security practices and incident reporting is provided in the attachment. A snapshot collection of current best practices, however, may be insufficient to address constantly evolving cyber threats. The DoD and the DIB should continuously share available information and collaborate to incorporate improved methods and evolving technologies into their information security practices as soon as they become available.

c. PMs must leverage shared DoD cyber security resources. For example, all intrusions or incidents involving the potential compromise, exfiltration or other loss of any DPI on a DIB information system should be reported to the Office of DoD-DIB Collaborative Information Sharing Environment (ODCISE). I have also established the Damage Assessment Management Office (DAMO) to support the evaluation of impact to defense programs due to any such information loss and to identify necessary countermeasures and remediation.

I have established a DIB Cyber Acquisition Joint Analysis Team (JAT) to serve as a focal point to assess the overall effectiveness and impact of these activities. Within 90 days, PMs for all Acquisition Category I programs (through their Component Acquisition Executives) will provide the JAT with an overview of the implementation of cyber security requirements in their programs, along with any recommendations for implementing similar requirements across the DoD and DIB. The JAT will use this information to support the next phase of this effort: the incorporation of more detailed cyber security guidance and requirements into the Defense Federal Acquisition Regulation Supplement (DFARS). I direct that a DFARS case be opened immediately to support this critical requirement to protect our information.

I encourage you to take immediate action with your DIB partners to improve cyber security efforts in all DoD acquisition programs. My point of contact is Ms. Kristen Baldwin, kristen.baldwin@osd.mil, 695-6364.


John J. Young, Jr.

Attachment:
As stated

Attachment A
Basic Information Security Practices and Incident Reporting for
Defense Industrial Base Cyber Security

PEO/PMs will leverage the recommended practices and resources below in developing, implementing, and assessing the adequacy of program and contractor information security practices.

I. Definitions

- a. "Controlled unclassified information" or "CUI" means information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interests of the United States or to the important interests of entities outside the U.S. Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (Source: Presidential Memorandum "Designation and Sharing of Controlled Unclassified Information," May 9, 2008. Note that the use of the term CUI in this guidance does not authorize DoD components to use the new CUI markings outlined in the Presidential Memorandum until the DoD transition plan is completed and the DoD-level implementation guidance is issued.)
- b. "Defense program information" or "DPI" means CUI that is developed, used, or shared in support of a DoD program. This term includes, but is not limited to:
- Technical data governed by DoDD 5230.24, Distribution Statements on Technical Documents, or DoDD 5230.25, Withholding of Unclassified Technical Data from Public Disclosure.
 - Data subject to export control under International Traffic in Arms Regulations (ITAR) or the Export Administration Regulation (EAR).
 - Data pertaining to items on the Commerce Control List (CCL) or the U.S. Munitions List (USML).
 - Data designated as Critical Program Information (CPI) in accordance with DoD Directive 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection.
- c. "Information system" means computer networks and equipment as well as electronic information processing and storage facilities belonging to, or operated by or for, a contractor or subcontractor used to collect, develop, store, use, receive or transmit DPI.

II. Protection of Defense Program Information (DPI)

1. PMs must ensure that information security requirements included in contracts appropriately address the need for contractors to provide protection appropriate to the sensitivity of the DPI stored, processed, transported, or displayed on any information system that it owns, operates, or controls, and to implement basic information security guidelines in their project, enterprise, or company-wide information security planning. PMs must also clarify applicable requirements for contractor information security planning. For example, a PM may require that contractor information security planning address the specific systems, processes, and practices that will be implemented to meet the contract information security requirements. These requirements must be applied also to lower tier subcontracts as appropriate.

2. PMs must implement training and procedures for DoD personnel to ensure appropriate management and safeguarding for any sensitive or proprietary information provided to DoD by a contractor related to the compromise, exfiltration or loss of DPI. Such information must be protected against any unauthorized use or disclosure, in accordance with law, regulations, and by mutual agreement with the contractor or subcontractor.

3. Basic guidelines for the protection of DPI:

- Employ computer security measures to appropriately protect DPI from loss, compromise or exfiltration. Security planning should be tailored in scope and depth appropriate to the effort and the specific DoD information. Multiple sources of best practices should be considered. A comprehensive computer security program is described in the DIB Cyber Security Capabilities Benchmark, Additional sources for such measures include, NIST (<http://csrc.nist.gov/index.html>), the CERT Coordination Center at the Software Engineering Institute (<http://www.cert.org/>), ISO/IEC 27002:2005 (<http://www.iso.org/>), the Information Security Forum (<https://www.securityforum.org/index.htm>), and the SANS Institute (<http://www.sans.org/score/checklists.php>).
- Comply with extant federal information protection or reporting requirements for specified information, e.g., FISMA, HIPAA, Privacy Act.
- Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks, hotel business centers, or the like), or computers that do not have access control.
- Minimize computer screen exposure to unauthorized persons.
- Protect DoD information by at least one physical or electronic barrier when not under direct individual control.

- Sanitize media by commonly accepted industry standards (e.g.” over-writing IAW DOD 5200.22-M, 1 May 2000”, "National Industrial Security Program Operating Manual,") before sale, transfer, or reassignment to those not authorized and requiring access to data stored thereon.
- *Electronic Data Transmission:* Transmit email, text messages, and similar data communications containing DPI with technology/processes such as closed networks, virtual private networks (VPN), and PKI. Encrypt all wireless external data connections.
- *Voice and Fax Transmissions:* Do not transmit unless sender has a reasonable assurance that only authorized recipients will have access to the transmission.
- *Transmission via a Website:* Do not post DPI to Web pages that are publicly available or have access limited only by domain/IP restriction. As permitted by other contract provisions, DPI may be posted to Web pages that control access by user ID/password, user certificates, or other technical means, and which provide protection via use of secure sockets or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).
- Contract requirements for information security must ensure that cyber security standards and reporting are applied to subcontractors or teaming partners as appropriate.

III. DoD Resources

1. The PM should leverage shared DoD resources to manage the ongoing network threats. All intrusions or incidents involving the potential compromise, exfiltration, or other loss of any DPI on a DIB information system shall be reported to the Office of DoD-DIB Collaborative Information Sharing Environment (ODCISE), located in the DoD Cyber Crime Center (DC3), whose contact information may be found at <http://www.dc3.mil/dc3/dc3Contact.php>. Given that reporting timeliness may enhance the value of certain information shared with other ODCISE subscribers, such initial reports must be made as expeditiously as possible—in all cases within 72 hours of discovery. Initial report content should include the following information, as available:

- Applicable dates, including date of compromise and date of discovery;
- Threat methodology, including all known “resources” used (e.g., IP addresses, domain names, software tools);
- An account of what actions the threat(s) may have taken on the victim system/network, and

- What information may have been compromised, exfiltrated, or lost and its potential impact on government programs.
2. Existing NISPOM reporting requirements to Defense Security Service (DSS) remain applicable in accordance with contract requirements, and are consistent with the intent of this guidance.
 3. In some cases, additional forensic assessments may be necessary to ascertain intruder methodology and identify systems compromised as a result of the intrusion.
 4. The DoD focal point for conducting damage assessment, OUSD(AT&L) Damage Assessment Management Office, will provide detailed guidelines and processes as needed and appropriate. Once ODCISE determines there was a likely data compromise, exfiltration, or loss from a DIB information system, they will contact the DAMO to begin an initial triage of the suspected compromised data. Depending on the severity of damage or loss, the DAMO may organize an Integrated Product Team (IPT) consisting of DoD Service / Agency and /or DIB subject matter experts to further analyze the data.



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu