ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NETWORKS AND INFORMATION INTEGRATION

July 31, 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-027 – Security of Unclassified DoD Information on Non-DoD Information Systems

References: See Attachment 1

Purpose. In accordance with the authority in DoD Directive 5144.1 (Reference (a)), this DTM establishes policy for managing the security of unclassified DoD information on non-DoD information systems. Subchapter III of chapter 35 of title 44, United States Code (Reference (b)) mandates that DoD information and DoD information systems be appropriately protected. DoD Instruction 8510.01 (Reference (c)) addresses the protection of classified and unclassified DoD information on information systems owned by the Department of Defense or operated on behalf of the Department by non-DoD entities. DoD Manual 5220.22-M (Reference (d)) addresses the protection of classified information released or disclosed to industry, including what is processed on their information systems. This DTM is effective immediately; it shall be incorporated into the appropriate DoD 8500 series issuances within 180 days.

Applicability. This DTM applies to:

- OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

- All unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems, to the extent provided by the applicable contract, grant, or other legal agreement or understanding with the Department of Defense. It does not apply to outsourced IT-based processes as described in Reference (c).

Definitions. These terms and their definitions are for the purpose of this DTM.

- adequate security. Protection measures applied are commensurate with the risks (i.e., consequences and their probability) of loss, misuse, or unauthorized access to or modification of information.

- DoD information. Any information that has not been cleared for public release in accordance with DoD Directive 5230.09 (Reference (e)) AND that is provided by the Department of Defense to a non-DoD entity, or that is collected, developed, received, transmitted, used, or stored by a non-DoD entity in support of an official DoD activity.

- non-DoD entity. Any person who is not a civilian employee or military member of the Department of Defense, or any entity or organization that is not a DoD Component. This includes any non-DoD Federal agency and its personnel, and any contractor, grantee, awardee, partner, or party to any form of legal agreement or understanding with the Department of Defense or another Federal agency.

- non-DoD information system. Any information system that is not owned, used, or operated by the Department of Defense AND that is not used or operated by a contractor or other non-DoD entity on behalf of the Department of Defense.

Policy. It is DoD policy to provide adequate security for all unclassified DoD information on non-DoD information systems. Appropriate requirements shall be incorporated into all contracts, grants, and other legal agreements or understandings with

non-DoD entities. Attachment 2 provides basic guidelines that can be tailored or enhanced to provide solutions for protection of such information.

Responsibilities. See Attachment 3.

Releasability. UNLIMITED. This DTM is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

Cheryl J. Roby
Acting Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Attachments:
As stated

ATTACHMENT 1

REFERENCES

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(b) Subchapter III of Chapter 35 of title 44, United States Code
(c) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(d) DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006
(e) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(f) Presidential Memorandum, "Designation and Sharing of Controlled Unclassified Information (CUI)," May 9, 2008
(g) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

ATTACHMENT 2

BASIC INFORMATION SECURITY GUIDELINES FOR PROTECTION OF UNCLASSIFIED DoD INFORMATION ON NON-DoD SYSTEMS

1. GENERAL. This attachment applies to unclassified DoD information. Such information may be disseminated by the contractor, grantee, or awardee to the extent required to further the contract, grant, or agreement objectives, provided that the information is disseminated within the scope of assigned duties and with a clear expectation that confidentiality will be preserved. Examples include:

a. Non-public information provided to the contractor (e.g., with the request for proposal).

b. Information developed during the course of the contract, grant, or other legal agreement or understanding (e.g., draft documents, reports, or briefings and deliverables).

c. Privileged information contained in transactions (e.g., privileged contract information, program schedules, contract-related event tracking).

2. INFORMATION SAFEGUARDS

a. Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

b. Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

c. Sanitize media (e.g., overwrite) before external release or disposal.

d. Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best available encryption technology.

e. Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

f. Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and

environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.

g. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

h. Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

i. Provide protection against computer network intrusions and data exfiltration, minimally including the following:

(1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

(2) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(3) Prompt application of security-relevant software patches, service packs, and hot fixes.

j. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled) as specified in contracts, grants, and other agreements.

k. Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

3. VALIDATION AND COMPLIANCE. Contracts and agreements should address how applicable information safeguards will be implemented.

ATTACHMENT 3

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall:

a. Oversee implementation of this guidance in coordination with the Under Secretary of Defense for Intelligence and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L), as appropriate.

b. Standardize the implementation of information protection best practices in the Defense Industrial Base (DIB).

c. Coordinate DoD convergence with emerging efforts in the broader government community to manage CUI, as defined in the Presidential Memorandum (Reference (f)), more effectively.

2. USD(AT&L). The USD(AT&L) shall:

a. Engage with the DIB to identify and validate approaches to improve protection of DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

b. Revise the Defense Federal Acquisition Regulation Supplement to implement this policy to require DoD contractors and their subcontractors to provide adequate security of DoD information in the contractor's and/or subcontractor's possession, including addressing National Institute of Standards and Technology standards and guidelines, as appropriate.

3. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Ensure that unclassified DoD information provided to or developed by non-DoD entities in support of DoD activities is protected according to the information safeguards described in Attachment 2 of this DTM by including requirements implementing this policy in contracts, grants, and other legal agreements or understandings in accordance with guidance issued pursuant to this DTM.

b. Ensure that any additional protection measures and reports regarding loss or unauthorized disclosure required by DoD 5400.11-R (Reference (g)) and other established

DoD information safeguarding policies (e.g., those relating to medical information, CPI, export control) are implemented by the insertion of applicable requirements into contracts, grants, and other legal agreements or understandings.