Department of Defense
INSTRUCTION

NUMBER 8582.01
June 6, 2012

DoD CIO

SUBJECT: Security of Unclassified DoD Information on Non-DoD Information Systems

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Establishes policy for managing the security of unclassified DoD information on non-DoD information systems in accordance with the guidance in DoD Instruction (DoDI) 5025.01 (Reference (a)) and the authority in DoD Directive (DoDD) 5144.1 (Reference (b)).

b. Incorporates and cancels Directive-Type Memorandum 08-027 (Reference (c)).

2. APPLICABILITY. This Instruction:

a. Applies to:

(1) 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 DoD (hereinafter referred to collectively as the "DoD Components").

(2) 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 with the DoD.

b. Does not apply to outsourced information technology (IT)-based processes as described in DoDD 8500.01E (Reference (d)).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that adequate security be provided for all unclassified DoD information on non-DoD information systems. Appropriate requirements shall be incorporated into all contracts, grants, and other legal agreements with non-DoD entities.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE

a. This Instruction is effective June 6, 2012.

b. This Instruction must be reissued, cancelled, or certified current within 5 years of its publication in accordance with Reference (a). If not, this Instruction will expire effective June 6, 2022 and be removed from the DoD Issuances Website.

Teresa M. Takai
DoD Chief Information Officer

Enclosures:
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
(b) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(c) Directive-Type Memorandum 08-027, "Security of Unclassified DoD Information on Non-DoD Information Systems", July 31, 2009 (hereby cancelled)
(d) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(e) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010
(f) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
(g) Defense Federal Acquisition Regulation Supplement, current edition
(h) DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
(i) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(j) DoD Directive 5205.02, "Operations Security (OPSEC) Program," March 6, 2006
(k) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(l) DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007
(m) Executive Order 13526, Classified National Security Information," December 29, 2009
(n) Sections 2153, 2161, 2162, 2163, 2164, and 2165 of title 42, United States Code (also known as the "Atomic Energy Act of 1954, as amended")
(o) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current version
(p) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO, in addition to the responsibilities in section 3 of this enclosure, shall:

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

b. Oversee integration of this guidance into Defense Industrial Base (DIB) cyber security and information assurance activities in accordance with DoDI 5205.13 (Reference (e)).

c. Standardize the implementation of information protection best practices in the DIB.

d. In coordination with the USD(I), ensure that the security of unclassified DoD information on non-DoD information systems that has been identified as controlled unclassified information (CUI) meets the requirements of Executive Order 13556 (Reference (f)) and its implementing directives, consistent with the DoD implementation plan to be provided in accordance with Reference (f) requirements.

2. USD(AT&L). The USD(AT&L), in addition to the responsibilities in section 3 of this enclosure, shall:

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

b. Identify, develop, and implement in the DoD acquisition contracting process policy and procedures for improved protection of unclassified DoD information transiting or residing on non-DoD information systems and networks to include:

(1) Ensuring that the Defense Federal Acquisition Regulation Supplement (DFARS) (Reference (g)) requires DoD contractors and their subcontractors to provide adequate security of DoD information in their possession.

(2) Addressing National Institute of Standards and Technology standards and guidelines, as appropriate.

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

a. Ensure that unclassified DoD information provided to or developed by non-DoD entities in support of DoD activities is minimally protected according to the information safeguards described in Enclosure 3 of this Instruction by including requirements implementing this policy in contracts, grants, and other legal agreements in accordance with guidance issued pursuant to this Instruction.

b. Ensure that any additional protection measures or reporting requirements regarding compromise, loss, or unauthorized disclosure required by DoD Manual 5200.01,Volume 4, DoD 5400.11-R, DoDD 5205.02, DoDI 5200.39, DoD 8580.02-R (References (h), (i), (j), (k), and (l)), and other established DoD information safeguarding policies (e.g., those relating to law enforcement, technical data, or export control) are implemented by the insertion of applicable requirements into contracts, grants, and other legal agreements.

c. Ensure that contracts include appropriate DFARS clauses for safeguarding unclassified DoD information on non-DoD information systems when such clauses are published in Reference (g).

ENCLOSURE 3

PROCEDURES

1. GENERAL. Unclassified DoD information that has not been cleared for public release 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 a contractor (e.g., with a request for proposal).

b. Information developed during the course of a contract, grant, or other legal agreement (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. It is recognized that adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system. However, all unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems shall minimally be safeguarded as follows:

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

b. Protect unclassified DoD information by at least one physical or electronic barrier (e.g., locked container or room, logical authentication or logon procedure) when not under direct individual control of an authorized user.

c. At a minimum, overwrite media that have been used to process unclassified DoD information before external release or disposal.

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

e. Limit transfer of unclassified DoD information to subcontractors or teaming partners with a need to know and obtain a commitment from them to protect the information they receive to at least the same level of protection as that specified in the contract or other written agreement.

f. Transmit e-mail, text messages, and similar communications containing unclassified DoD information 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).

g. Encrypt organizational wireless connections and use encrypted wireless connections where available when traveling. If encrypted wireless is not available, encrypt document files (e.g., spreadsheet and word processing files), using at least application-provided password protected level encryption.

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

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

j. Provide protection against computer network intrusions and data exfiltration, minimally including:

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

(2) Monitoring and control of both inbound and outbound network traffic (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.

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

l. Report loss or unauthorized disclosure of unclassified DoD information in accordance with contract, grant, or other legal agreement requirements and mechanisms.

m. Do not use external IT services (e.g., e-mail, content hosting, database, document processing) unless they provide at least the same level of protection as that specified in the contract or other written agreement.

3. RIGOR. More stringent information safeguards may be imposed at the discretion of the responsible Heads of the OSD and DoD Components.

4. VALIDATION AND COMPLIANCE. Contracts, grants, and other legal agreements shall address how applicable information safeguards will be implemented.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CUI	controlled unclassified information
CPI	critical program information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
IT	information technology
TLS	transport layer security
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Instruction.

adequate security. Protection measures applied are commensurate with the risks of loss, misuse, or unauthorized access to or modification of information.

CUI. Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified pursuant to Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended (References (m) and (n)).

CPI. Defined in Reference (k).

DIB. Defined in Joint Publication 1-02 (Reference (o)).

DoD information. Any information that has not been cleared for public release in accordance with DoDD 5230.09 (Reference (p)) and that is provided by the DoD 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 DoD, 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 with the DoD or another Federal agency.

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

outsourced IT-based process. Defined in Reference (d).

overwrite. To replace data previously stored on storage media with a predetermined set of meaningless data or random patterns.

publically available computer. Any computer available to the general public, usually after certain conditions are met (e.g., payment of a fee, a paying guest in a hotel).