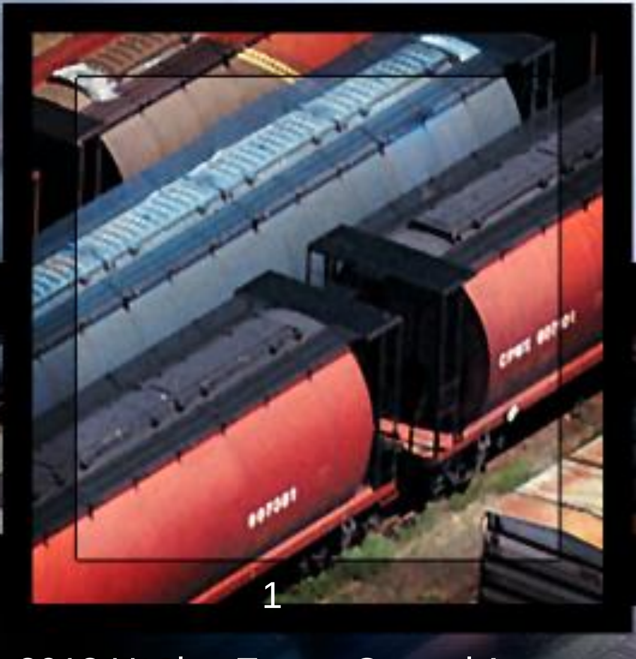
SAFEGUARDING UNCLASSIFIED INFORMATION PROTECTED FOR RELEASE BY THE ARMS EXPORT CONTROL ACT



Arms Export Control Act; Executive Order 12470 and
DoD Directive 5230.25

Scope of Briefing

- This briefing addresses safeguarding issues related to unclassified information protected for release by the Arms Export Control Act.
- It provides an overview of the process and procedures to be followed by a contractor to obtain such information in support of a government requirement.
- It recommends certain security precautions.
- It identifies future safeguards which are being currently evaluated by the Department of defense.

Information Safeguarding Regs and Directives

- DoD 5200.1-R, *Information Security Program Regulation*
- DoD 5220.22-M, *National Industrial Security Program Operating Manual*
- DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*
- DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*
- Title 10, United States Code 130, *Authority to Withhold from Public Disclosure Certain Technical Data*
- Title 22, United States Code 2571 et seq., *Arms Export Control Act*

Three primary rules to follow

- First – the government client is the owner of the “protected information.”
- Second – In the event of a conflict, Security Guidance provided by the government customer takes precedence over information provided in this briefing.
- Third: The information obtained from the government was obtained for one purpose only – performance of a government contract requirement –

DO NOT USE PROTECTED INFORMATION FOR ANY OTHER PURPOSE.

Unclassified Technical Data With Military or Space Applications.

- Certain unclassified information may not be released to the public or a foreign entity unless first approved or licensed under the Arms Export Control Act or E.O. 12470.
- Because public disclosure of any technical data with military or space application is tantamount to providing uncontrolled foreign access, withholding such data from public disclosure, unless approved, authorized, or licensed in accordance with export control law is necessary and in the national interest. (DOD Directive 5230.25)

Types of Information Protected

- Technical reports, engineering drawings, operation and maintenance manuals, training manuals, military specifications and standards related to particular types of equipment.
- Most test reports meet this standard. They meet the standards if they show what individual components can be used within a larger weapons system; what weapons can be used for particular purposes; or show how to use, maintain, or train people to use particular weapons.
- *They do not meet this standard if they simply show the operating characteristics of a weapon, and this information would not affect the decision to use the weapon. In the latter case, the information might qualify for security classification, but would not meet export-control standards.*

Protective Markings

Information protected under DOD Directive 5230.25 will be marked:

WARNING--This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. 2751 et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401, et seq. Violation of these export-control laws is subject to severe criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25.

How to safeguard

- Ensure the protected information is used only for the purposes for which it was obtained – government contract performance.
- Treat as if the information was Personally Identifiable Information (PII).
  - *Would you allow anyone access to a document that contained your Name, SSN and address?*
- When not in use, secure the information in a desk or cabinet to prevent unauthorized access.
- Do not release to, or allow access by, unauthorized personnel.
- Documents / data maintained in information systems should be password protected.
- Ensure printed documents are secured properly until such time as they can be disposed of when no longer needed.
- Ensure documents, compact discs and other materials are marked appropriately

IT / Communication Systems…

- Laptop computers and PDAs / Smart-phones are integral to business operations.
- Caution must be exercised when any of these systems contain information protected for release under the Arms Export Control Act.
- The use of a dedicated web accessed system – utilizing user ID and password control – is a recommended method for storing related data.
- Password protect or encrypt all data residing on company laptops / PDA / Smart-phones.
- Do not store or process any controlled information on *personal* computers / PDA / Smart-phones.
- Do not process DOD information on public computers (*e.g.,* those available for use by the general public in kiosks, hotel business centers)

Dissemination

Qualified U.S. contractors who receive technical data may disseminate such data for purposes consistent with their certification without the prior permission of the controlling DoD office or when such dissemination is:

- To any foreign recipient for which the data are approved, authorized, or licensed under E.O. 12470 or the Arms Export Control Act
- To another currently qualified U.S. contractor but only within the scope of the certified legitimate business purpose of such recipient.
- To the Departments of State and Commerce, for purposes of applying for appropriate approvals, authorizations, or licenses for export under the Arms Export Control Act or E.O. 12470 .
- To Congress or any Federal, State, or local governmental agency for regulatory purposes, or otherwise as may be required by law or court order.

Disposal / Destruction

- The preferred method of disposal of unclassified, limited distribution documents is by shredding, although the shredder need not be approved for classified documents. Alternatively:
- Place different parts in different recycling or waste bins, or
- Tear them into three or more pieces placing them in a single bin, or
- Burn them.
- Destruction of Digital Media. Media containing unclassified, limited distribution data must be “cleared” before recycling: floppy disks and hard drives must be reformatted and magnetic tapes must be erased. For guidance on destruction of compact disks, refer to MIL-HDBK-9660, *DOD Produced CD-ROM Products.*

Certification Requirements

- Recipients of the export-controlled technical data must be a U.S. citizen or a person admitted lawfully into the United States for permanent residence and is located in the United States.

- The data are needed to bid or perform on a contract with the Department of Defense, or other U.S. Government Agency, or for other legitimate business purposes in which the U.S. contractor is engaged, or plans to engage.

- The U.S. contractor acknowledges its responsibilities under U.S. export control laws and regulations and agrees that it will not disseminate any export-controlled technical data in a manner that would violate applicable export control laws and regulations.

Certification requirements (Cont’d)

- The U.S. contractor also agrees that, it will not provide access to export-controlled technical data subject to this Directive to persons other than its employees or persons acting on its behalf, without the permission of the DoD Component that provided the technical data.

- To the best of its knowledge and belief, the U.S. contractor knows of no person employed by it, or acting on its behalf, who will have access to such data, who is debarred, suspended, or otherwise ineligible from performing on U.S. Government contracts; or has violated U.S. export control laws or a certification previously made to the Department of Defense under the provisions of this Directive.

- The U.S. contractor itself is not debarred, suspended, or otherwise determined ineligible by any Agency of the U.S. Government to perform on U.S. Government contracts, has not been convicted of export control law violations, or otherwise not been disqualified.

In the works at DOD …

Currently DOD is evaluating security requirements for the protection of unclassified – but sensitive – information. It proposes a two level approach – basic and enhanced.

BASIC PROTECTIONS	
Protecting DOD information on public computers or Web sites	Do not process DOD information on public computers (*e.g.,* those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. DOD information shall not be posted on Web sites that are publicly available or have access limited only by domain/IP restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies.
Transmitting electronic information	Transmit e-mail, text messages, blogs, and similar communications using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment.
Transmitting voice and fax information	Transmit voice and fax information only when the sender has a reasonable assurance that access is limited to authorized recipients.
Physical or electronic barriers	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
Sanitization	Sanitize media in accordance with National Institute of Standards and Technology (NIST) 800–88, Guidelines for Media Sanitization, at *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf,* before external release or disposal
Intrusion protection	Provide protection against computer intrusions and data exfiltration, minimally including the following: (i) Current and regularly updated malware protection services, *e.g.,* anti-virus, antispyware. (ii) Prompt application of security-relevant software upgrades, *e.g.,* patches, servicepacks, and hot fixes
Limitations	Transfer DOD information only to those subcontractors that both have a need to know and provide at least the same level of security as specified in this clause

In the works (Continued)

ENHANCED PROTECTIONS “All of the ABOVE – PLUS:”	
Encryption/Storage	Encrypt using the Security Controls for Federal Information Systems and Organizations at (*http://csrc.nist.gov/publications/PubsSPs.html*) for both organizational wireless connections, and when traveling use encrypted wireless connections where available. 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. Encrypt all information identified in paragraph (b)(2) of this clause 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 level of encryption technology available, given facilities, conditions, and environment.
Network intrusion protection	Provide adequate protection against computer network intrusions and data exfiltration, as follows: (A) Current and regularly updated malware protection services, *e.g.,* anti-virus, antispyware. (B) Monitoring and control of both inbound and outbound network traffic as appropriate (*e.g.,* at the external boundary, sub-networks, individual hosts) to include blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, or host-based security services. (C) Prompt application of security-relevant software patches, service-packs, and hot fixes.
Information Security Controls	The Contractor shall implement information security controls in its project, enterprise, or company-wide unclassified information security program. The information security program shall address the security controls described in the NIST Special Publication 800–53 (Current Version), Recommended Security Controls for Federal Information Systems and Organizations

In the works (Continued)

Cyber Intrusion reporting (For Enhanced Protections only)	(1) *Reporting requirement.* The Contractor shall report to the Defense Cyber Crime Center's (DC3) DoD–DIB Collaborative Information Sharing Environment (DCISE) (URL to be determined) within 72 hours of discovery of any cyber intrusion events that affect DoD information resident on or transiting the contractor's unclassified information systems. (2) *Reportable events.* Reportable cyber intrusion events include the following: (i) A cyber intrusion event appearing to be an advanced persistent threat. (ii) A cyber intrusion event involving data exfiltration or manipulation or other loss of any DoD information resident on or transiting its, or its subcontractors', unclassified information systems. (iii) Intrusion activities not included in paragraph (c)(2)(i) or (ii) of this clause that allow illegitimate access to an unclassified information system on which DoD information is resident or transiting.