PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Changes Are in Process

Federal government agencies and offices have more than 107 unique markings and over 130 different marking and handling procedures for dealing with information that, by law or regulation, requires some form of protection but is outside the formal system for classifying national security information. For Official Use Only, Law Enforcement Sensitive, Limited Official Use are among the more common labels for such information.

These diverse procedures for handling what is now called Controlled Unclassified Information (CUI) originally worked well within the individual organizations that created them. However, since the September 11, 2001, terrorist attacks the amount of such information being generated to meet national security requirements has soared, and the need to share this information between federal agencies and between federal, state, local, and tribal agencies, has soared. Changed operational needs require a more uniform system of controls.

Presidential Executive Order 13556, "Controlled Unclassified Information," dated November 4, 2010, established a new program for managing all unclassified information in the Executive branch that requires safeguarding or dissemination controls. The National Archives and Records Administration (NARA) serves as the Executive Agent to implement this order and oversee agency actions to ensure compliance The order requires the following:

- Each agency head is required within 180 days of this order (by early May 2011) to submit to the Executive Agent its proposed categories and subcategories of CUI and proposed markings associated with each category.
- The Executive Agent in consultation with the affected agencies will develop and issue directives as necessary to implement this program.
- Within 1 year of the date of this order (by November 4, 2011), the Executive Agent will establish and maintain a public CUI registry that records all authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.
- Within 180 days of the issuance of initial policies and procedures by the Executive Agent, each agency that originates or handles CUI is to provide the Executive Agent with a proposed plan for compliance, including the establishment of interim target dates.

The NARA Controlled Unclassified Information Offce issued its first notice, Initial Implementation Guidance for Executive Order 13556, on June 9, 2011. It directs agencies to establish and manage a CUI program that designates categories of information and how each category will be marked, safeguarded, and disseminated. The CUI Office will maintain a Registry of CUI categories.

Department of Defense Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," dated June 12, 2012, establishes policy for handling controlled but unclassified DoD information in defense industry. This is discussed in a separate file, CUI in

Defense Industry.

Other sections of this module on CUI discuss existing practices as of mid-2011. This entire module will be updated periodically as decisions are made to implement Executive Order 13556..

CUI in Defense Industry

"Department of Defense Instruction 8582.01, "Security of Unclassified Informaton on Non-DoD Information Systems, June 6, 2012, establishes policy for how non-DoD organizations, such as defense industry, are required to manage the security of sensitive DoD information.

Unclassified DoD information that has not been cleared for public release may be disseminated by the contractor, grantor, 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)."

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 incryption 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, antispyware.

(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."

Rigor

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

Validation and Compliance

"Contracts, grants, and other legal agreements shall address how applicable information safeguards will be implemented."

For Official Use Only (FOUO)

For Official Use Only (FOUO) is a document control designation, but not a classification. This designation is used by Department of Defense and a number of other federal agencies to identify information or material that, although unclassified, may not be appropriate for public release.

There is no national policy governing use of the For Official Use Only designation. DoD Directive 5400.7 defines For Official Use Only information as "unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)." The policy is implemented by DoD Regulation 5400.7-R and 5200.1-R.

The For Official Use Only designation is also used by CIA, Homeland Security, and a number of other federal agencies, but each agency is responsible for determining how it shall be used. The categories of protected information may be quite different from one agency to another, although in every case the protected information must be covered by one of the nine categories of information that are exempt from public release under FOIA.

Some agencies use different terminology for the same types of information. For example, Department of Justice uses For Official Use Only but adds the words Law Enforcement Sensitive, abbreviated FOUO-LES. Department of Energy uses Official Use Only (OUO). The National Geospatial-Intelligence Agency uses Limited Distribution. Department of State uses Sensitive But Unclassified (SBU), formerly called Limited Official Use (LOU). The Drug Enforcement Administration uses DEA Sensitive. In all cases the designations refer to unclassified, sensitive information that is or may be exempt from public release under the Freedom of Information Act.

The fact that information is marked FOUO or any comparable designation does not mean it is automatically exempt from public release under FOIA. If a request for the information is received, it must be reviewed to see if it meets the FOIA dual test: (1) It fits into one of the nine FOIA exemption categories, and (2) There is a legitimate government purpose served by withholding the information. On the other hand, the absence of the FOUO or other marking does not automatically mean the information must be released in response to a FOIA request.

Statutory/Regulatory Responsibilities & Obligations

Each government department or agency defines what information shall be protected and how its protected information shall be handled. The procedures for marking, safeguarding, and controlling access to FOUO and comparable categories of information are very similar for all the agencies, but there are some individual differences. The following information pertains only to DoD FOUO information. When dealing with comparable information from another department or agency, check with the originator regarding appropriate handling.

Access to FOUO Information

FOUO information may be disseminated within the DoD components and between officials of the DoD components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other departments and agencies of the executive and judicial branches as needed for a lawful and authorized government purpose.

Special procedures govern the release of FOUO information to Congress and the General Accountability Office (GAO). Special procedures are also required before NGA Limited Distribution information may be provided to any foreign government.

The final responsibility for determining whether an individual has a valid need for access to information designated FOUO rests with the individual who has authorized possession, knowledge, or control of the information and not with the prospective recipient.

Marking FOUO Information

Unclassified documents and material containing FOUO information shall be marked as follows:

- Documents will be marked FOR OFFICIAL USE ONLY at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).
- Pages of the document that contain FOUO information shall be marked FOR OFFICIAL USE ONLY at the bottom.
- Each paragraph containing FOUO information shall be marked with the abbreviation FOUO in parentheses at the beginning of the FOUO portion. Subjects, titles, and each section or part of a document shall be similarly marked.
- Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings which alert the holder or viewer that the material contains FOUO information.
- FOUO documents and material transmitted outside the DoD must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

This document contains information exempt
from mandatory disclosure under the FOIA.
Exemption(s) _ apply.

When FOUO information is contained within a classified document, the same rules apply except that full pages that contain FOUO information but no classified information shall be marked FOR OFFICIAL USE ONLY at both the top and bottom of the page.

Safeguarding FOUO Information

FOUO information should be handled in a manner that provides reasonable assurance

that unauthorized persons do not gain access.

During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO may be stored as a minimum in unlocked containers, desks or cabinets if government or government-contract building security is provided. If government or government-contract building security is not provided, it must be stored at a minimum in a locked desk, file cabinet, bookcase, locked room, or similar place.

FOUO documents and material may be transmitted via first class mail, parcel post, or -- for bulk shipments -- fourth class mail.

Electronic transmission of FOUO information, e.g., voice, data or facsimile, and email, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), whenever practical. FOUO information may be put on an Internet website only if access to the site is limited to a specific target audience and the information is encrypted. See Pre-Publication Review of Website Content.

FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.

Enforcement

Administrative penalties may be imposed for misuse of FOUO information. Criminal penalties may be imposed depending on the actual content of the information (privacy, export control, etc.).

Legal & Regulatory Authorities

5 USC 301 - Departmental Regulations
DoD Regulation 5200.1-R - The Information Security Program
DoD Directive 5400.7 - The Freedom of Information Act (FOIA) Program
DoD Regulation 5400.7-R – The DoD Freedom of Information Act Program
DoD Regulation 5400.11-R – Department of Defense Privacy Program

Personally Identifying Information

The Privacy Act of 1974, as amended, is a Federal law that requires personally identifying information in the custody of the Federal Government about American citizens or approved permanent residents of the United States to be protected from unauthorized disclosure. In passing this law, Congress created a balance between individuals' right to privacy and the government's need to maintain information about individuals.

Privacy information is not just name, date and place of birth, address, and phone number. It includes social security number, payroll number, mother's maiden name, religion, race, information on education, financial and credit data, medical history including results of drug testing, criminal and employment history, work performance ratings, leave balances, types of leave taken, and names of employees who hold government-issued travel cards.

To protect personally identifying information, now often called PII, the Privacy Act requires all executive branch agencies to follow certain procedures when:

- collecting personal information;
- creating databases containing personal identifiers;
- maintaining databases containing personal identifiers;
- disseminating information containing personal data.

Government Contractors

PII in the custody of government contractors is not covered by the Privacy Act unless the contractor is performing on a contract under which the contractor is provided access to or custody of such information by the Federal Government. Under this condition, the law would apply to contractor personnel as it applies to government personnel.

Government contractors in most states are subject to state privacy laws that require companies to protect privacy information as defined by state law.

Statutory/Regulatory Responsibilities & Obligations

System of Records Notice (SORN)

Whenever a federal agency maintains a set of information about individuals from which it can retrieve information by some personal identifier such as a name, social security number, or employee number, this collection of information is what the Privacy Act calls a "system of records."

Before a federal agency can begin to collect personal information for a new system of records, it must go through a complex process that often takes as long as four months. This includes a Privacy Impact Analysis (PIA) and System of Records Notice (SORN) which must be approved and then published in the Federal Register. The SORN is then open for public comment for 40 days.[1]

The SORN must include the lowing information:

- name and location of the system;
- categories of individuals on whom records are maintained in the system;
- ategories of records maintained in the system;
- legal authority for maintaining the system;
- the purposes for which the system will be used. For each type of routine use, the categories of users and their purpose of such use;
- policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
- title, name, and business address of the agency official who is responsible for the system of records;
- agency procedures to notify an individual, at his request, if the system of records contains a record pertaining to him, how to gain access to any record pertaining to him, and how to contest the content of any such record;
- categories of sources of the records in the system.

Safeguarding Privacy Act Information

The law does not specify specific marking or safeguarding requirements. It does require that each government agency that establishes a system of records containing privacy information also establishes "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity…"

Individual agencies establish their own procedures for marking, storing, transporting, and disposing of PII. Agencies typically require:

- that PII be stored in filing cabinets or other containers that prevent unauthorized access;
- that it be clearly marked as Controlled Unclassified Information or with some other approved marking both on paper and on electronic media;
- that email containing PII must be encrypted and must clearly identify the PII material.
- that information transported by hand be shielded by a cover sheet; information sent by ground mail should be addressed to a known person, and the outer envelope should not indicate the presence of sensitive information.
- that information no longer needed be disposed of in a manner that renders the information unrecognizable and beyond reconstruction.

Individual Rights

When a federal agency solicits any PII about an individual for any system of records, it must tell the individual in writing:

- the statute or executive order of the President that authorizes the agency to solicit this

information;

- the principal purposes for which the information is intended to be used;
- the routine uses which may be made of the information as announced in the Federal Register; and
- whether the disclosure of the information is mandatory or voluntary; and the effects, if any, on the individual for not providing the information.

Individuals are usually entitled to access to their own records. The announcement of the system of records in the Federal Register provides the address an individual may use to request access to his or her records, and the government must provide this access either in person or by mail. If an individual believes the information in the record is in error, a formal process is available for requesting correction of the record and for appeal if the manager of the record system refuses to make changes.

Access to Privacy Information

The Privacy Act requires government departments and agencies to develop rules of conduct and training for personnel with access to privacy records. It also requires all departments and agencies to promulgate rules regarding circumstances under which an individual has a right to see his or her own records.

The Privacy Act lists 12 circumstances under which privacy information may be communicated to other persons without the prior written consent of the individual to whom the record pertains. These include any disclosure required to be released under the Freedom of Information Act, information disclosed to another agency for civil or criminal law enforcement purpose, disclosure to either house of Congress, and disclosure mandated by court order. Any other communication of privacy information requires a written request and the prior written consent of the individual to whom the record pertains.

Loss of Information

If you have reason to suspect that PII has been deliberately or accidentally compromised or lost, you must report this immediately to an appropriate authority in your organization. Organizations must take immediate action to notify all individuals whose personal information may have been lost or compromised. The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals or organizations and may lead to identity theft or other fraudulent use of the information. Immediate reporting may enable individuals or organizations to take protective or remedial action to contain the damage.

Unfortunately, there have been a number of recent cases in which thousands, even hundreds of thousands, of PII records have been compromised through a breach of computer security or loss of a laptop computer with such information. Compromise of PII on a single individual may occur through carelessness, ignorance, and accident. Civil and criminal penalties for compromise of PII are described below.

Penalties

The Privacy Act provides for both civil and criminal penalties for violation of this act. The criminal

penalty is a misdemeanor charge and fine of up to $5,000 for knowing and willfully:

- obtaining records under false pretenses;
- willfully disclosing PII data to any person not entitled to access;
- maintaining a system of records without meeting public notice requirements.

Courts may also award civil penalties for:

- unlawfully refusing to amend a record;
- unlawfully refusing to grant access to a record;
- failure to maintain accurate, relevant, timely, and complete information;
- failure to comply with any Privacy Act provision or agency rule when the result is an adverse effect on the subject of the record.

Penalties for these violations include actual damages, payment of reasonable attorney's fees, and removal from employment.

Legal & Regulatory Authorities

Title 5 USC 552a – Records Maintained on Individuals (Privacy Act)
Title 12 USC 3417 -- Civil Penalties
Title 18 USC 1905 – Disclosure of Confidential Information Generally
Title 41 CFR 201-6.1 – Federal Information Resources Management Regulation
E.O. 12564 – Drug Free Federal Workplace
OMB Circular No. A-130 – Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals.
P.L. 100-71 – The Supplemental Appropriations Act of 1987, Section 503.
P.L. 104-13 - Paperwork Reduction Act of 1955.

1. USAID, "Filing a System of Records Notice: Process and Procedures," at http://www.usaid.gov/policy/ads/500/508maa.pdf. Also Department of the Navy, Privacy Office, "Guidelines for Establishing a New Privacy Act System of Records Notice," at http://privacy.navy.mil/tools/guidelines.pdf.

Export-Controlled Information

Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR) or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export-controlled information must be handled as sensitive but unclassified information and marked accordingly. A large, frequently updated database of information on export regulations is available at www.bis.doc.gov.

One objective of the ITAR and EAR is to prevent foreign citizens, industry, or governments, or their representatives, from obtaining information that is contrary to the national security interests of the United States.

Different laws and regulations use different definitions of a U.S. person, U.S. national, and foreign national. This is a source of considerable confusion in implementing international security programs.

The rules are especially confusing when dealing with an immigrant alien who possesses a green card for permanent residence in the United States. For the purpose of export control regulations, such an individual is a "U.S. person" and *can* be allowed access to export-controlled information without an export license. If the export-controlled information is classified, however, the regulations for release of classified information apply. According to the National Industrial Security Program Operating Manual, a permanent resident with a green card is still a foreign national and *not* a "U.S. person." Therefore, such an individual *cannot* have access to classified export-controlled information.

Statutory/Regulatory Responsibilities & Obligations

Export-controlled information may be disseminated only to U.S. citizens or immigrant aliens with a green card. It is important to note that discussion with a foreign national in the United States, or a person "acting on behalf of a foreign person," constitutes an "export" if it reveals technical information regarding export-controlled technology.

Marking Export-Controlled Information

All documents that contain export-controlled technical data must be marked with the following warning:

> **WARNING** - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq.). Violations of these export laws are subject to severe criminal penalties.

Safeguarding Export-Controlled Information

The possessor of export-controlled information must deny the opportunity for access to foreign nationals or any unauthorized person. Records must be maintained for all exports of items on the Department of Commerce Control List for a period of at least two years. Records of the export of items listed on the State Department's ITAR must be maintained for five years.

Export-controlled information may be put on an Internet website only if access to the site is limited to a specific target audience that is authorized to have the information and the information is encrypted. See Pre-Publication Review of website Content.

DoD technical data subject to export controls shall be safeguarded as described in Technical Data.

Enforcement

The penalty for unlawful export of items or information controlled under the ITAR is up to two years imprisonment, or a fine of $100,000, or both. The penalty for unlawful export of items or information controlled under the EAR is a fine of up to $1,000,000 or five times the value of the exports, whichever is greater; or for an individual, imprisonment of up to 10 years or a fine of up to $250,000 or both.

Legal & Regulatory Authorities

Executive Order 12923 Continuation of Export Control Regulations, 30 June 1994.
Title 22 USC 2778 et seq. – Arms Export Control Act.
Title 50 USC 2401 et seq. – Export Administration Act of 1979 (as amended).
Title 50 USC Appendix, Section 10 – Trading With the Enemy Act of 1917.
Title 15 CFR Export Administration Regulations, part 770.
Title 15 CFR part 779 Technical Data.
Title 22 CFR (Dept. of State) Subchapter M, The International Traffic and Arms Regulation (ITAR) Part 121-130.

Proprietary Information & Trade Secrets

The Economic Espionage Act of 1996 (18 USC 1831-39) defines trade secrets as all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

- The owner thereof has taken reasonable measures to keep such information secret, and
- The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through, proper means by the public.

There is no general definition for proprietary information in the U.S. legal code. The Federal Acquisition Regulation (48 CFR 27.402 Policy) does, however, provide a definition:

> "…contractors may have a legitimate proprietary interest (e.g., a property right or other valid economic interest) in data resulting from private investment. Protection of such data from unauthorized use and disclosure is necessary in order to prevent the compromise of such property right or economic interest, avoid jeopardizing the contractor's commercial position, and preclude impairment of the Government's ability to obtain access to or use of such data."

This regulation is intended to protect from disclosure outside the government proprietary information that is provided to the government during a bidding process. Exemption 4 of the Freedom of Information Act exempts from mandatory disclosure information such as trade secrets and commercial or financial information obtained by the government from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness. The law on Disclosure of Confidential Information (18 USC 1905) makes it a crime for a federal employee to disclose such information.

State laws may also apply to unauthorized disclosure of proprietary or trade secret information.

Statutory/Regulatory Responsibilities & Obligations

Safeguarding Proprietary/Trade Secret Information

Effective enforcement of laws governing unauthorized disclosure of proprietary or trade secret information generally requires that the owner of this information must have taken reasonable measures to safeguard it from unauthorized disclosure.

Reasonable measures include building access controls, escorting visitors, marking sensitive documents, non-disclosure agreements, and shredding material when no longer needed.

In the case of defense contractors, the government contract may require a contractor to follow certain safeguarding requirements. The government, in turn, is required to protect proprietary or trade secret information submitted to it during the bidding process (FAR 14.401). Bids must be "kept secure" and remain "in a locked bid box or safe."

Marking Proprietary/Trade Secret Information

Effective enforcement of laws governing unauthorized disclosure of proprietary or trade secret information generally requires that this information be clearly identifiable through appropriate markings. The nature of these markings is left to the discretion of the company. The terms "Company Sensitive" or "Company Proprietary" are sometimes used.

In soliciting bids, the government is required to inform potential contractors how to mark proprietary information (FAR 15.407) to ensure its protection. When a contract is granted, a data rights clause must be included in the contract (FAR (52.227-14) to advise the contractor how to mark proprietary data for protection. The title page and each page containing proprietary information must be marked. The regulations provide no guidance on marking of electronic media while on an electronic system (screen display or file marker).

Enforcement

The Economic Espionage Act contains two separate provisions that make the theft or misappropriation of trade secrets a federal criminal offense. The first provision, under Section 1831, is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, instrumentality, or agent. In contrast, the second provision, under Section 1832, makes the commercial theft of trade secrets a criminal act regardless of who benefits.

A defendant convicted of economic espionage under Section 1831 can be imprisoned for up to 15 years and fined $500,000 or both. Corporations and other organizations can be fined up to $10 million. A defendant convicted for theft of trade secrets under Section 1832 can be imprisoned for up to 10 years and fined $500,000 or both. Corporations and other entities can be fined no more than $5 million.

Three other laws apply to disclosure of specific types of proprietary information, especially disclosure by government personnel:

- For knowing disclosure of non-government information to which a government agency has gained access in connection with a procurement action, Title 41 USC 423 - Procurement Integrity, provides both civil and criminal penalties. The criminal penalty is up to five years imprisonment. The civil penalty is a fine up to $100,000. This applies mainly to government employees who receive non-government information, but also to non-government personnel who receive sensitive

procurement information from government (for example, if government gives industry a bid package containing information from a potential subcontractor). This procurement integrity law applies only prior to the award of a contract. Once a contract has been awarded, other laws with lesser penalties may apply.

- Title 18 USC 1905 applies to disclosure by a government employee of any information provided to the government by a company or other nongovernment organization, if the provider of the information identified it as proprietary or as being provided to the government in confidence. The penalty is mandatory removal from office (termination of employment), and the offender may be fined not more than $1,000 and imprisoned not more than one year.
- For disclosure of nongovernment financial information in the custody of the government, civil remedies are allowed under 12 USC 417 Civil Penalties, which also requires the director of the Office of Personnel Management (OPM) to conduct an investigation and recommend disciplinary action on federal employees found culpable.

Legal & Regulatory Authorities

Title 5 USC 552(b) – Exemption b.(4),- Freedom of Information Act.
Title 12 USC 3417 – Right to Financial Privacy, Civil Penalties.
Title 18 USC 1831–39 - Protection of Trade Secrets [Chapter 90].
Title 18 USC 1905 – Disclosure of Confidential Information.
Title 41 USC 423 – Procurement Integrity.
Executive Order 12600 – Predisclosure Notification Procedures for Confidential Commercial Information.
Title 5 CFR 734 – Employee Responsibilities and Conduct.
Title 36 CFR 1234.10 Paragraph l.
FAR 3.104-1 – Procurement Integrity, General (48 CFR).
FAR 3.104-3 – Statutory Prohibitions and Restrictions (48 CFR).
FAR 14.401 – Receipt and Safeguarding of Bids (48 CFR).
FAR 15.407 - Solicitation Provisions (48 CFR).
FAR 27.4 – Rights in Data and Copyrights (48 CFR).
FAR 52.215-12 – Restriction on Disclosure and Use of Data (48 CFR).
FAR 52.227-14 – Rights in Data (48 CFR).

Marking DoD Technical Data

Appropriate marking and control of certain unclassified technical data dealing with military or space applications are important because foreign corporations and others acting on behalf of foreign governments may otherwise file requests for this information under the Freedom of Information Act. These requests often seek entire defense contract packages. For example, when a major corporation in a friendly country decided to enter the space industry, it made extensive use of FOIA requests as a means of obtaining information from NASA. By some estimates, the corporation filed over 1,500 FOIA requests in a single year.

Federal law (15 USC 140c) allows the Secretary of Defense to withhold from public disclosure any technical data with military or space applications that is in the possession of -- or under control of -- the Department of Defense and that may not be exported lawfully without an approval, authorization or license under the Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR). This does not apply to scientific, education, or other data that qualify for General License GTDA under the EAR. The rationale for this restriction is that public release may constitute an export. DoD Directive 5230.25, "Withholding Unclassified Technical Data from Public Disclosure," implements this law.

Department of Defense Directive 5230.24 establishes a number of procedural requirements intended to identify and control the dissemination of export-controlled technical documents created by DoD-funded research, development, test and evaluation programs. These procedures apply to engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

Statutory/Regulatory Responsibilities & Obligations

Marking and Distribution of Technical Data

One of seven possible distribution statements must be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originator of the document. The originating office may make case-by-case exceptions to the distribution limitations imposed by the statements.

For guidance in assigning and marking distribution controls per DoD Directive 5230.24, see below Distribution Statements on Technical Documents.

Access to Technical Data

It is DoD policy to provide technical data governed by these controls to individuals and

enterprises that are determined to be currently qualified U.S. Government contractors when such data relate to a legitimate business purpose for which the contractor is certified.

Qualified U.S. Government contractors who receive technical data governed by these controls may disseminate such data to others 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 the Export Administration Regulations or the International Traffic in Arms Regulations.
- To another currently qualified U.S. Government contractor, but only within the scope of the certified, legitimate business purpose of such recipient.
- To the Departments of State and Commerce for the purpose of applying for appropriate approvals, authorizations, or licenses under the Export Administration Regulations or the International Traffic in Arms Regulations.

In addition to these need-to-know controls, access is limited to U.S. citizens or a persons admitted lawfully into the United States for permanent residence and who is located in the United States.

Safeguarding Technical Data

The possessor of technical data must take reasonable care to deny access to unauthorized persons. Technical data may be put on an Internet website only if access to the site is limited to a specific target audience and the information is encrypted. See Pre-Publication Review of Website Content.

Enforcement

Agencies have authority to impose administrative sanctions for failure to comply with regulations. Title 22 USC 2778 allows a $1,000,000 fine and 10 years imprisonment for willful violation of arms control laws.

Distribution Statements On Technical Documents

The following are extracts from three elements of the DoD Directive 5230.24 that covers distribution statements on technical documents.

F. Procedures

1. All DoD Components generating or responsible for technical documents shall determine their distribution availability and mark them appropriately before primary distribution. Documents recommended for public release must first be reviewed in accordance with DoD Directive 5230.9 (reference (f)).

2. DoD distribution statement markings shall not be required on technical proposals or similar documents submitted by contractors seeking DoD funds or contracts.

3. Managers of technical programs shall assign appropriate distribution statements to technical documents generated within their programs to control the secondary distribution of those documents.

a. All newly created unclassified DoD technical documents shall be assigned distribution statement A, B, C, D, E, F, or X (see enclosure 3).

b. Classified DoD technical documents shall be assigned distribution statement B, C, D, E, or F. The distribution statement assigned to a classified document shall be retained on the document after its declassification or until changed specifically or removed by the controlling DoD office. Technical documents that are declassified and have no distribution statement assigned shall be handled as distribution statement F documents until changed by the controlling DoD office.

c. Scientific and technical documents that include a contractor-imposed limited rights statement shall be marked and controlled in accordance with subpart 27.4 of the DoD Supplement to the FAR (reference (g)).

d. For each newly generated technical document, managers of technical programs shall determine whether the document contains export-controlled technical data; DoD Directive 5230.25 (reference (c)) provides guidance for making this determination. Additional guidance may be obtained from component legal counsel. All documents that are found to contain export-controlled technical data shall be marked with the export control statement contained in subsection A.8, below, of enclosure 3; any document so marked must also be assigned distribution statement B, C, D, E, F, or X.

e. Technical documents in preliminary or working draft form shall not be disseminated without a proper security classification review and assignment of a distribution statement as required by this Directive.

4. Distribution statements shall remain in effect until changed or removed by the controlling DoD office. Each controlling DoD office shall establish and maintain a procedure to review technical documents for which it is responsible to increase their availability when conditions permit. The controlling DoD office shall obtain public release determinations in accordance with reference (f). If public release clearance is obtained, the controlling DoD office shall assign distribution statement A, cancel any other distribution statement, and notify the proper document handling facilities.

* * *

8. The distribution statement shall be displayed conspicuously on technical documents so as to be recognized readily by recipients.

a. For standard written or printed material, the following applies:

(1) The distribution statement shall appear on each front cover, title page, and DD Form 1473, "Report Documentation Page."

(2) When possible, parts that contain information creating the

requirement for a distribution statement shall be prepared as an appendix to permit broader distribution of the basic document.

(3) When practical, the abstract of the document, the DD Form 1473 and bibliographic citations shall be written in such a way that the information will not be subject to distribution statement B, C, D, E, F, or X.

b. If the technical information is not prepared in the form of an ordinary document (such as this Directive) and does not have a cover or title page (such as forms and charts), the applicable distribution statement shall be stamped, printed, written, or affixed by other means in a conspicuous position.

Extracts from DoD Directive 5230.24 (Enclosure 3)

A. The following distribution statements and notices are authorized for use on DoD technical documents:

1. **DISTRIBUTION STATEMENT A**. Approved for public release; distribution is unlimited.

a. This statement may be used only on unclassified technical documents that have been cleared for public release by competent authority in accordance with DoD Directive 5230.9. Technical documents resulting from contracted fundamental research efforts will normally be assigned Distribution Statement A, except for those rare and exceptional circumstances where there is a high likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to defense, and agreement on this situation has been recorded in the contract or grant.

b. Technical documents with this statement may be made available or sold to the public and foreign nationals, companies, and governments, including adversary governments, and may be exported.

c. This statement may not be used on technical documents that formerly were classified unless such documents are cleared for public release in accordance with reference (f).

d. This statement shall not be used on classified technical documents or documents containing export-controlled technical data as provided in DoD Directive 5230.25 (reference (c)).

2. **DISTRIBUTION STATEMENT B.** Distribution authorized to U.S. Government agencies only (fill in reason) (date of determination]. Other requests for this document shall be referred to (insert controlling DoD office).

a. This statement may be used on unclassified and classified technical documents.

b. Reasons for assigning distribution statement B include:

- **Foreign Government Information**: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DoD 5200.1-R.

- **Proprietary Information**: To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside the U.S. Government.
- **Critical Technology**: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25 (reference (c)).
- **Test and Evaluation**: To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.
- **Contractor Performance Evaluation**: To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.
- **Premature Dissemination**: To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.
- **Administrative or Operational Use**: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.
- **Software Documentation**: Releasable only in accordance with DoD Instruction 7930.2 (reference (i)).
- **Specific Authority**: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DoD or DoD Component regulatory documents. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

3. **DISTRIBUTION STATEMENT C.** Distribution authorized to U.S. Government agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).

a. Distribution statement C may be used on unclassified and classified technical documents.

b. Reasons for assigning distribution statement C include:

- Foreign Government Information: Same as distribution statement B.
- Critical Technology: Same as distribution statement B.
- Software Documentation: Same as distribution statement B.
- Administrative or Operational Use: Same as distribution statement B.
- Specific Authority: Same as distribution statement B.

4. **DISTRIBUTION STATEMENT D.** Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

a. Distribution statement D may be used on unclassified and classified technical documents.

b. Reasons for assigning distribution statement D include:

- Foreign Government Information: Same as distribution statement B.
- Administrative or Operational Use: Same as distribution statement B.
- Software Documentation: Same as distribution statement B.
- Critical Technology: Same as distribution statement B.
- Specific Authority: Same as distribution statement B.

5. **DISTRIBUTION STATEMENT E.** Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

a. Distribution statement E may be used on unclassified and classified technical documents.

b. Reasons for assigning distribution statement E include:

- Direct Military Support: The document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States. Designation of such data is made by competent authority in accordance with DoD Directive 5230.25 (reference (c)).
- Foreign Government Information: Same as distribution statement B.
- Proprietary Information: Same as distribution statement B.
- Premature Dissemination: Same as distribution statement B.
- Test and Evaluation: Same as distribution statement B.
- Software Documentation: Same as distribution statement B.
- Contractor Performance Evaluation: Same as distribution statement B.
- Critical Technology: Same as distribution statement B.
- Administrative/Operational Use: Same as distribution statement B.
- Specific Authority: Same as distribution statement B.

6. **DISTRIBUTION STATEMENT F.** Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority.

a. Distribution statement F is normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists (e.g., designation as direct military support as in statement E).

b. Distribution statement F is also used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505,

DoD 5200.1-R (reference (h)).

7. **DISTRIBUTION STATEMENT X.** Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with reference (c) (date of determination). Controlling DoD office is (insert).

a. Distribution statement X shall be used on unclassified documents when distribution statements B, C, D, E, or F do not apply, but the document does contain technical data as explained in reference (c).

b. This statement shall not be used on classified technical documents; however, it may be assigned to technical documents that formerly were classified.

8. **Export Control Warning**: All technical documents that are determined to contain export-controlled technical data shall be marked "WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et q.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25." When it is technically infeasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export Controlled Data" required by DoD Directive 5230.25 (reference (c)).

9. **Handling and Destroying Unclassified/Limited Distribution Documents**: Unclassified/Limited Distribution documents shall be handled using the same standard as "For Official Use Only (FOUO)" material, and will be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicate that this destruction method is not sufficiently protective of unclassified limited information, local authorities may prescribe other methods but must give due consideration to the additional expense balanced against the degree of sensitivity.

Extracts from DoD Directive 5230.24 (Enclosure 4)

Contractor-Imposed Distribution Statements

1. Part 27, Subpart 27.4 to the DoD Supplement to the Federal Acquisition Regulation (FAR) (reference (g)) stipulates control procedures for contractor-controlled technical data to which the Government has limited rights. In this case, an approved statement from the DoD Supplement to the FAR shall appear on all copies of each document. Unmarked or improperly marked technical documents supplied by a contractor shall be handled in accordance with the DoD Supplement to the FAR. Limited rights information shall be assigned distribution statements B, E, or F.

2. The limited rights statement shall remain in effect until changed or canceled under contract terms or with the permission of the contractor, and until the controlling DoD Component notifies recipients of the document that the statement may be changed or canceled. Upon cancellation of the statement, the distribution, disclosure, or release of the technical document shall then be controlled by its security classification or, if unclassified,

by the appropriate statement selected from this Directive.

3. Reference (g) defines limited rights as the right to use, duplicate, or disclose technical data in whole or in part, by or for the U.S. Government with the expressed limitation that such technical data, without the written permission of the party furnishing such technical data, may not be:

a. Released or disclosed in whole or in part outside the Government.

b. Used in whole or in part by the Government for manufacture, or in the case of computer software documentation, for reproduction of the computer software.

c. Used by a party other than the Government, except for:

(1) Emergency repair or overhaul work only by or for the Government, when the item or process concerned is not otherwise reasonably available to enable timely performance of the work, provided that the release or disclosure outside the Government shall be made subject to a prohibition against further use, release, or disclosure.

(2) Release to a foreign government, as the interest of the United States may require, only for information or evaluation within such government or for emergency repair or overhaul work by or for such government under the conditions of subparagraph 3.c. (1), above.

Source Selection Data

Source Selection Data is information related to the decisionmaking process (including the decision itself) for an award of a contract to industry. Information in this category is generally only sensitive until after formal award of the contract.

Such information must be protected from disclosure outside the Government and limited within the Government to individuals with a need to know that information.

Statutory/Regulatory Responsibilities & Obligations

Federal Acquisition Regulations (FAR) specify procedures to be followed to protect source selection data.

Access to Source Selection Data

Bids may not be disclosed except on a need-to-know basis and only to Government employees (FAR Part 14.401 -- Receipt and safeguarding of bids (48 CFR)).

Proprietary and source selection information may only be disclosed to individuals authorized by the head of an agency (FAR Part 3.104.5 Disclosure, Protection, and Marking of Proprietary and Source Selection Information). For contracts over $100,000, the names of individuals having access to the file shall be listed with the contract file.

Marking Source Selection Data

Source selection information shall be marked on the cover page and each page that contains source selection information with the legend SOURCE SELECTION INFORMATION.

Safeguarding Source Selection Data

Bids shall be "kept secure" in a "locked bid box or safe."

Penalties

For knowing disclosure of non-government information to which a government agency has gained access in connection with a procurement action, Title 41 USC 423 - Procurement Integrity, provides both civil and criminal penalties. The criminal penalty is up to five years imprisonment. The civil penalty is a fine up to $100,000.

This applies mainly to government employees who receive non-government information, but also to non-government personnel who receive sensitive procurement information from government (for example, if government gives industry a bid package containing information from a potential subcontractor). This procurement integrity law applies only prior to the award of a contract. Once a contract has been awarded, other laws with lesser penalties may apply.

Title 18 USC 1905 applies to disclosure by a government employee of any information

provided to the government by a company or other nongovernment organization, if the provider of the information identified it as proprietary or as being provided to the government in confidence. The penalty is mandatory removal from office (termination of employment), and the offender may be fined not more than $1,000 and imprisoned not more than one year.

Legal & Regulatory Authorities

Title 41 USC 421 -- Federal Acquisition Regulatory Council
Title 41 USC 423 -- Procurement Integrity
FAR Part 3.104-1 -- Procurement Integrity, General (48 CFR)
FAR Part 3.104.3 -- Statutory Prohibitions and Restrictions (48 CFR)
FAR Part 3.104-5 -- Disclosure, Protection, and Marking of Proprietary and Source Selection Information.
FAR Part 14.401 -- Receipt and Safeguarding of Bids (48 CFR)
FAR Part 15.407 -- Solicitation Provisions (48 CFR)
FAR Part 27.4 -- Rights in Data and Copyrights
FAR Part 52.215-12 -- Restriction on Disclosure and Use of Data (48 CFR)

Unclassified Controlled Nuclear Information (UCNI)

Unclassified Controlled Nuclear Information (UCNI) under jurisdiction of the Department of Energy includes unclassified facility design information, operational information concerning the production, processing or utilization of nuclear material for atomic energy defense programs, safeguards and security information, nuclear material, and declassified controlled nuclear weapon information once classified as Restricted Data (RD).

Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI) is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material, equipment, or facilities.

Information is designated UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of Special Nuclear Material, equipment, or facilities.

Statutory/Regulatory Responsibilities & Obligations

Access to UCNI Information

An individual must have an official need to know the information and be a federal employee, member of the U.S. Armed Services, contractor, consultant, law enforcement official, local government official, Indian tribal government official, or a foreign official who is part of an approved intergovernmental activity. A person with access to UCNI may disseminate that information only to other authorized individuals.

Marking UCNI Information

Different marking procedures apply for UCNI and DoD UCNI.

UCNI: If a document or material ***may*** contain UCNI, it should be marked in a conspicuous manner with the following notice:

> Not for Public Dissemination
> May contain Unclassified Controlled Nuclear Information subject to section 148 of the Atomic energy Act of 1954, as amended (42 U.S.C. 2168). Approval by the Department of Energy prior to release is required.

If information or material is definitely known to contain UCNI, it should be marked in a conspicuous manner with one of the following notices:

> Unclassified Controlled Nuclear Information
> Not for Public Dissemination

Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168)

or

Not for Public Dissemination
Unauthorized dissemination subject to civil and criminal sanctions under 42 U.S.C. 2168.

DoD UCNI: Unclassified documents and material containing DoD UCNI information shall be marked as follows:

- The face of the document and the outside of the back cover (if there is one) shall be marked DoD Unclassified Controlled Nuclear Information. Portions of a document that contain such information shall be marked with DoD UCNI at the beginning of the portion.
- Pages of a classified document that contain no classified information but do contain DoD UCNI information shall be marked at the top and bottom of the page DoD Unclassified Controlled Nuclear Information.
- Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings which alert the holder or viewer that the material contains DoD UCNI information.
- DoD UCNI documents and material transmitted outside the originating agency must bear an expanded marking on the face of the document so that recipients understand the status of the information. A statement similar to the following should be used:

DEPARTMENT OF DEFENSE
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
EXEMPT FROM MANDATORY DISCLOSURE
(5 USC 552(b)(3), as authorized by .10 USC 128)

Safeguarding UCNI Information

Different safeguarding procedures apply for UCNI and DoD UCNI.

UCNI: When UCNI information is in use, physical control must be maintained to prevent unauthorized access. When not in use, it must be stored in a secure container (e.g., locked desk or file cabinet) or in a location where access is limited (e.g., locked or guarded office, controlled access facility).

UCNI documents or material may be disposed of by any method that assures sufficiently complete destruction to prevent its retrieval.

A document or material containing UCNI material may be transmitted by U.S. first class, express, certified, or registered mail. It must be packaged to prevent disclosure of the presence of UCNI to unauthorized persons.

UCNI may be discussed or transmitted over an unprotected telephone or

telecommunications circuit when required by operational considerations. More secure means of communication should be utilized whenever possible.

UCNI information may be put on an Internet website only if access to the site is limited to a specific target audience and the information is encrypted. See Security Criteria fpr Website Content.

DoD UCNI: During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, DoD UCNI information shall be stored as a minimum in unlocked containers, desks or cabinets if government or government-contract building security is provided. If government or government-contract building security is not provided, it must be stored at a minimum in a locked desk, file cabinet, bookcase, locked room, or similar place.

DoD UCNI documents and material may be transmitted via first class mail, parcel post, or -- for bulk shipments -- fourth class mail. Electronic transmission of UCNI and DoD UCNI information (voice, data or facsimile) should be by approved secure communications systems whenever practical.

DoD UCNI documents may be destroyed by shredding or tearing into pieces and discarding the pieces in a regular trash container unless circumstances suggest a need for more careful protection.

Enforcement

Violation of Section 148 of the Atomic Energy Act carries a civil fine not to exceed $110,000. In addition, the individual may be subject to a criminal penalty under Section 223 of the Act.

Legal Authorities

42 USC 2168 – Atomic Energy Act of 1954.
10 CFR Part 1017 – Identification and Protection of Unclassified Controlled Nuclear Information.
DoD Regulation 5200.1-R, Information Security Program.

Sensitive Security Information

Sensitive Security Information (SSI) is a control designation used by the Department of Homeland Security, and particularly the Transportation Security Administration. It is applied to information about security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation. The applicable information is spelled out in greater detail in 49 CFR 1520.7.

The SSI applies to information that the government obtains from the private sector or develops on its own while carrying out certain security or research and development activities relating to any mode of transportation. It protects information that, if disclosed, would be an unwarranted invasion of personal privacy, reveal a trade secret or privileged or confidential commercial or financial information, or make it easier for hostile elements to avoid security controls.

Statutory/Regulatory Responsibilities & Obligations

The Transportation Security Administration (TSA) has oversight responsibility for protecting Sensitive Security Information.

Access to SSI

Access to SSI is based on need to know. A Federal employee has a need to know SSI when access to the information is necessary for the employee to accomplish official duties. A contractor employee has a need to know SSI when access to the information is necessary for the employee to carry out a requirement of a Federal contract relating to transportation security.

Marking SSI

Any person who creates a document containing SSI must include a protective marking and limited distribution statement that clearly identifies the information as SSI and specifies the distribution limitation required. A person who receives a record containing SSI that is not marked accordingly must add such marking and inform the sender of its omission.

The protective marking, "SENSITIVE SECURITY INFORMATION," must be written or stamped in plain style bold type, such as Times New Roman font size 16 or an equivalent style and font size. For documents, it must be applied at the top of the outside of any front cover (including a binder or folder), on the top of any title page, on the top of the first page and each subsequent page, and on the top of the outside of any back cover (including a binder or folder). This marking should be placed in a comparable location on charts, maps, or drawings and on film, video, or electronic media.

A distribution limitation statement must be applied at the bottom of the outside cover of any front cover (including a binder or folder), on the bottom of any title page, on the bottom of

the first page and each subsequent page, and on the bottom of the outside of any back cover (including a binder or folder). It should be placed in a comparable location on other forms of media. The distribution limitation statement should be written or stamped in plain style bold type using Times New Roman and a font size of 8 or an equivalent style and font size. This statement must read as follows:

> " WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the TSA Administrator, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 522."

Documents that transmit SSI but do not themselves contain SSI must be marked with the distribution limitation statement. In addition, the following statement must be affixed to the front page of the transmittal document.

> "The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed."

Safeguarding SSI

All personnel possessing SSI are responsible for ensuring that such information is safeguarded at all times from disclosure to unauthorized personnel. When the information is not under the individual's direct physical control, the individual is responsible for ensuring that it is safeguarded and protected so that it is not physically or visually accessible to persons who do not have a need to know. When unattended, SSI must be secured in a locked container, office, or other restricted access area with access to the keys or combination limited to those with a need to know.

Control and Release of SSI

SSI may be released to federal, state and municipal government officials/employees, local law enforcement officials, and regulated parties who have a need to know as established by regulation or authorized by the TSA Administrator.

SSI requested under the Freedom of Information Act is exempt from disclosure under the FOIA based on Exemption 3, 5 USC 552(b)(3). Any decision to release SSI under the FOIA must have the concurrence of the TSA Administrator.

Requests for information that are addressed to regulated parties, such as requests under state and local freedom of information or open records acts, should be referred to the TSA Administrator. TSA works with operators, carriers, and other affected entities to determine what records or portions of records should remain undisclosed and what may be released.

If a record contains SSI but also contains non-SSI that may be disclosed, the latter will be provided in response to a FOIA request, provided the record is not otherwise exempt from disclosure under FOIA, if it is practical to redact the requested information from the record.

When a contractor needs to make copies of SSI, the contractor must make prior notification in writing, through the Contracting Office, to the originator of the SSI.

Packaging and Transmitting SSI

SSI may be transmitted by U.S. Postal Service first class mail or regular parcel post, or by other delivery services such as Federal Express or UPS. It must be enclosed in an opaque envelop or other opaque wrapping. Addressing the package with an attention line containing the name and office of the recipient helps to ensure that the SSI material is received and opened only by authorized personnel. When hand-carried within or between buildings, SSI must be protected by a cover sheet, protective folder, distribution pouch, or other method to prevent visual disclosure.

When transmitted by email, SSI must be in a password-protected attachment. The passwords and procedures must comply with standards set by the TSA Office of Information Security.

When sending SSI by fax, the sender must assure that the receiving fax machine is in a secure area or that an authorized recipient is at the receiving fax machine to promptly retrieve the information.

When communicating SSI by telephone, the caller must ensure that the person receiving the SSI is an authorized recipient. Mobile and cordless telephones should be avoided if at all possible, because such conversations are easier to intercept and monitor.

Posting of SSI on Internet or intranet sites is permitted only on sites approved by the TSA Office of Information Security. Such sites must meet prescribed security standards.

Destruction of SSI

SSI should be destroyed in a manner that ensures recovery of the sensitive information is difficult, if not impossible. Any means approved for the destruction of national security classified material may also be used for SSI. If no such means are available, SSI may be destroyed by tearing it into small pieces and assimilating it with other waste material. When destroying SSI by hand, it must be cut or torn into pieces measuring not more than 1/2 inch on a side and then mixed with other wastepaper.

When a contractor proposes to destroy records containing SSI, the contractor must first provide notification in writing, through the Contracting Office, to the information originator. This notification must include the following minimum information: identification of information to be destroyed, quantities of copies, date and place of destruction, method of destruction, and residual SSI remaining in custody of the contractor.

Relationship to Other Document Designations

SSI is one of a number of categories of information that are commonly referred to as "sensitive but unclassified" information. Some of these categories, such as SSI, Protected Critical Infrastructure Information (Protected CII), and Privacy Act Information are defined by legislation. One prominent category -- For Official Use Only (FOUO) -- is not defined by legislation; its usage varies from one agency to another. Because SSI is defined by legislation, rules for marking and handling SSI take precedence over agency procedures for handling FOUO. No document should ever be marked both SSI and FOUO.

It is possible, however, for the same document to be marked both SSI and Protected CII. This will happen when the SSI document also meets the requirement for Protected CCI, that is, it is provided to the government voluntarily rather than in response to a government requirement. As a general rule, SSI is either created by TSA or required to be submitted to TSA or another part of the Federal government. If a document carries both markings, it must be handled according to the more stringent Protected CII rules.

Enforcement

Violation is a civil offense as compared with PCII which is a criminal offense.

Legal & Regulatory Authorities

Title 49 CFR 1520 -- Protection of Sensitive Security Information

Protected Critical Infrastructure Information

The Department of Homeland Security's Protected Critical Infrastructure Information (PCII) Program enables private sector organizations to share sensitive information about critical infrastructure with government entities. The PCII information is used by the Department of Homeland Security and other federal, state and local analysts to:

- Evaluate physical security risks associated with critical infrastructure and other protected systems;
- Create reports regarding improvements to our country's emergency preparedness;
- Enhance disaster recovery preparedness measures.

The PCII program is governed by the Critical Infrastructure Information Act of 2002. If information meets the requirements of this act, the government is protected from any requirement to release this information to the public under the Freedom of Information Act (FOIA), state or local disclosure laws, or any civil litigation.

Government entities must meet basic requirements for safeguarding PCII and be formally accredited by the PCII Program Office. The Program Office monitors ongoing compliance with these requirements to ensure PCII is not mishandled or misused. Program success depends on ensuring that information shared by the private sector remains protected.

Further information about this program is available at www.dhs.gov/pcii. If your office needs critical infrastructure information, contact the PCII Program Office at 202-360-3023 or via email at pcii-info@dhs.gov.

Operations Security (OPSEC)

OPSEC is the shorthand term for operations security. OPSEC is not a specific category of information. Rather, it is a process for identifying, controlling, and protecting generally unclassified information which, if it becomes known to a competitor or adversary, could be used to our disadvantage.

OPSEC focuses on identifying and protecting information that might provide a competitor or adversary with clues to our plans or capabilities, and thereby enable the competitor or adversary to thwart a planned operation or activity.

The OPSEC process is applied to a wide variety of situations in a competitive or adversary environment. If you have ever given a surprise party or attempted to make your house look lived-in while you were away, by arranging for someone to pick up your newspapers or installing a light timer, you have practiced OPSEC.

The following are just a few examples of indicators that, under certain circumstances, might provide clues that tip off a competitor or adversary to your plans or capabilities: supply and equipment orders, transportation plans, mission-specific training, changes in communication patterns, leaders' travel, changes in work hours (working nights and weekends). Any change in an established pattern might prompt an adversary observer to ask why this action is occurring and what it might mean regarding one's intentions.

OPSEC is used by government agencies and contractors in the development and acquisition of new equipment, in intelligence collection, by warfighters at all levels, by crimefighters in many roles, as well as by private enterprise -- all to supplement traditional security measures for protecting potentially exploitable information.

The OPSEC process is a risk-management instrument that enables the manager or commander to view an operation or activity from the perspective of an adversary. The key feature of this approach is to look at our own methods and activities from the adversary's viewpoint by putting ourselves in an adversary's shoes and asking the question: "What information do I need to know to thwart the other side's intentions and actions, and what are the paths to the information I need?"

The OPSEC process traditionally involves five interdependent phases.

The first **identifies critical information**. That is, what are we trying to protect? Is it a single set of data relating to the timing (or other details) of a military operation? Or might it be a whole process embedded within an acquisition program? Or perhaps the patterns or profile of an undercover police officer? In each of these examples, there are data that need to be kept from someone (an opposing force, a foreign government, a foreign competitor, or a criminal).

This leads to the second element -- an **analysis of the threat**. Who wants or needs our critical information? Who is our adversary (not necessarily an enemy)? An integral part of

this phase is the identification of how our adversary might collect our information. Would he be likely to review open source literature, send corporate or state-sponsored spies to infiltrate or seek out the data, or use technical means such as eavesdropping, photographing, etc.? OPSEC considers a variety of potential adversaries -- ranging from the **active** (target or enemy or main competitor) to the **passive** (sympathizer or someone who supplies data to the active adversary) to the **inadvertent** (someone who accidentally gives away information) -- all of whom warrant recognition, assessment, and resolution of the particular level and type of threat they pose.

The third phase looks at **vulnerabilities**, direct and indirect, surrounding our operation. We look at how the activity *actually* works, rather than how people *think* it works. We study the chronology and timing of events, along with the flow of information, to ascertain which adversary would be interested in what data, and how he would be able to obtain them. Are there things that we do to give away our data directly, or are there certain signs that would lead a prudent adversary to deduce our data (indicators or clues)? We consider the *magnitude* of the vulnerabilities, as well as the *impact* of the loss of our data. In other words, how big is the problem, and how bad is it?

At this stage, the manager evaluates the **risk** to his or her operation or activity, asking: "Does the possible loss of information about my operation or activity warrant taking steps to reduce or (hopefully) negate the adversary's potential efforts to thwart my operation or activity?" The costs associated with fixing the vulnerability are weighed against the cost of the loss of the data, keeping in mind the likelihood of our data being lost as well as the impact such loss would entail. One method to reach a reasonable conclusion of the practicality of solution(s) might be to multiply the estimated loss in dollars*,* by the impact of risk, by the likelihood of risk. The solution, in dollars, must then be less expensive for the solution to be feasible.

Countermeasures, finally, are the *solutions* that a manager employs to reduce risks to an acceptable level, whether by eliminating indicators or vulnerabilities, disrupting the effective collection of information, or by preventing the adversary from accurately interpreting the data. Countermeasures are dictated by cost, timing, feasibility, and the imagination of the personnel involved. The most effective tend to be simple, straightforward, and inexpensive procedural adjustments that fit the solution to the need. Countermeasures are instituted in rank order to protect the vulnerabilities having the most impact (in dollars, lives, mission failure, etc.). Multiple countermeasures, enacted together, often provide a synergistic effect that compounds the benefits without unduly raising the cost level.

While OPSEC is not a cure-all, it *is* a vital, easy-to-use tool that ideally is instituted at the very onset of an activity. If the personnel involved develop an "OPSEC mindset," effectiveness is enhanced and mission success is more likely. OPSEC is neither difficult nor time-consuming; instead, it can easily become a "matter-of-course" process.

Related Topic: Pre-Publication Review of Website Content.

Reference

This information was provided to PERSEREC by the Interagency OPSEC Support Staff.

Freedom of Information Act

The public has a right to information concerning the activities of its government. The Freedom of Information Act (FOIA) requires all Federal agencies to conduct their activities in an open manner and to have a system for providing the public with the maximum amount of accurate and timely information allowed by law. Agencies commonly have a FOIA office for processing public requests for information.

The FOIA allows nine exemptions from this mandatory release policy. The purpose of the exemptions is to preclude the unauthorized disclosure of information that requires protection. These exemption categories reflect laws, executive orders, regulations, or court decisions that either require or permit protection of certain classes of information. The exemption categories, in turn, also help define information that may be protected. For example, Department of Defense Regulation 5200.1-R defines For Official Use Only information as "unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)."

DoD Regulation 5200.1-R, Appendix C, describes the nine FOIA exemptions as written below. The wording reflects the history of court decisions interpreting the Freedom of Information Act and, therefore, differs from the language of the act itself. To be exempt from mandatory release, information must fit into one of the following categories ***and*** there must be a legitimate government purpose served by withholding it.

1. Information which is currently and properly classified.

2. Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)

3. Information specifically exempted by statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future or to protect the government's interest in compliance with program effectiveness.

5. Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.

6. Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

7. Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to

a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others; (d) disclose the identify of a confidential source; (e) disclose investigative techniques or procedures; or (f) could reasonably be expected to endanger the life or physical safety of any individual

8. Certain records of agencies responsible for supervision of financial institutions.

9. Geological and geophysical information concerning wells.

Statutory/Regulatory Responsibilities & Obligations

FOIA requires agencies to promulgate policies to implement the requirements of the act and to publish these policies in the Federal Register. Each agency is responsible for establishing an appropriate administrative system to manage the FOIA.

The act has no requirements for protection of information. It only permits withholding information from disclosure, when appropriate.

When a FOIA request seeks public release of information held under exemption 4 (commercial information provided to the government on a confidential basis), the responsible government agency must determine whether the public's right to know outweighs the company's right to protection of proprietary information. If the agency determines that the information should be released under FOIA, Executive Order 12600 requires that the company be advised and be given an opportunity to present its arguments for continued protection before the information is released.

Any person who believes the federal government is withholding information from the public improperly may bring legal action against the responsible agency. District Courts of the United States have jurisdiction to enforce the requirements of this law by declaratory judgment, injunctive relief, or other relief as may be appropriate.

Legal & Regulatory Authorities

Title 5 USC 552 – Public Information; Agency Rules, Opinions, Orders, Records, Land Proceedings. Executive Order 12600 – Predisclosure Notification Procedures for Confidential Commercial Information. Presidential Memorandum on Administration of Freedom of Information Act, Oct. 4, 1993. Attorney General memorandum for heads of Department and Agencies, Freedom of Information Act, Oct 4, 1993.

Security Criteria
For Website Content

With all its many benefits, the Internet can also do a great deal of harm if not used properly. Information on the Internet that may be intended for a limited audience is actually available to a worldwide audience. The World Wide Web was not designed with security in mind, and unencrypted information is at high-risk of compromise to any interested adversary or competitor. It is very easy to search the web and put together related pieces of information from different sites.

Guidance for what goes on a website takes into account what security access controls, if any, are in effect for the site, the sensitivity of the information, and the target audience for which the information is intended. Briefly, none of the various types of sensitive but unclassified information discussed in this module may go on a website unless that site is protected by encryption. Decisions on the handling of proprietary or trade secret information in the private sector are made by the owners of that information.

Department of Defense (DoD) has rules for what should and should not go on a website and how information should be reviewed before it is posted on a website. The DoD policy is cited under Reference below. This policy applies to all unclassified DoD websites and to review and approval of requests received from DoD contractors and subcontractors or other U.S. Government agencies to post DoD information on their websites.

The following table from the DoD guidance on reviewing websites[1] has been modified to fit into a smaller space. The table is a guide to determining an acceptable level of risk, but the listed types of access controls are not necessarily the only options available for protecting information.

If access control is:	the vulnerability is:	and information can be:
Open -- no access limitations, plain text, unencrypted.	Extremely high. Subject to worldwide dissemination and access by everyone on the Internet.	Non-sensitive, of general interest to the public, cleared and authorized for public release. Worldwide dissemination must pose limited risk even if information is combined with other information reasonably expected to be in the public domain.
Limited by Internet domain (e.g., mil, gov) or IP address. Plain text, unencrypted.	Very high. This limitation is not difficult to circumvent.	Non-sensitive, not of general interest to the public although approved and authorized for public release. Intended for DoD or other specifically targeted audience.
Limited by requirement for User ID and password. Plain text, unencrypted.	High. Still vulnerable to hackers, as User IDs and passwords can be compromised if encryption is not used.	Non-sensitive information that is appropriate only for a specific targeted audience.
User certificate based (software). Requires PKI. encryption through use of secure sockets layer.	Moderate. This provides a moderate level of secure access control.	Sensitive unclassified information, and information that is "sensitive by aggregation."

User certificate based (hardware). Requires PKI encryption.	Very low vulnerability.	Sensitive unclassified information, and information that is "sensitive by aggregation" where extra security is required.

DoD guidelines also require that judgments about the sensitivity of information take into account the potential consequences of "aggregation." The term "sensitive by aggregation" refers to the fact that information on one site may seem unimportant, but when combined with information from other websites, it may form a larger and more complete picture that was neither intended nor desired. In other words, the combination of information from multiple websites may amount to more than the sum of its parts. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that the site will be accessed by those seeking information that can be used against us.

Before putting any information on a website, you must consider how an adversary or competitor might use that information to target your organization's personnel or activities. This requires applying risk management concepts to balance the benefits gained from using the Internet against the potential security and privacy risks created by having that information available to a worldwide audience.

There are several common mistakes that people make when deciding what to put on a website. One is to ignore the danger associated with personal data on the Internet. Another is to assume that information is not sensitive just because it is not marked with any sensitivity indicator. A third is that people underestimate the ease and potential significance of "point-and-click aggregation" of information.

Inclusion of information about home addresses or family members in biographic summaries is one of the most common errors. Personal information that could facilitate criminal, harassment, or terrorist activity against military personnel or government or defense contractor employees should not be on the Internet. This includes home address, telephone numbers other than those readily available to the public, social security number, date of birth, and any identifying information at all about family members.

For Official Use Only information and other sensitive but unclassified information is normally given a control marking at the time it is created. However, the absence of any control marking is not a valid basis for assuming that information is non-sensitive. Before putting unmarked information on a website, it must be examined for the presence of information that requires protection and qualifies as exempt from public release.

People who have not themselves developed strong skills at searching the Internet generally underestimate the amount and nature of the information that can be found there and the ease with which it can be located. The vast quantity of information on the Internet, combined with powerful computer search engines, has spawned sophisticated "data mining" techniques for the rapid collection and combination of information from many different websites. Very little know-how is needed, as the tools of the Internet have been designed to do this. A single user sitting at a computer in a foreign country can now

identify, aggregate, and interpret information available on the Internet in ways that sometimes provide insights into classified or sensitive unclassified programs or activities.

Information relevant to Operations Security (OPSEC) is a particular concern. Commanders and program managers responsible for OPSEC need to identify what needs to be protected and then take a "red team" approach to how outsiders might obtain unauthorized knowledge. As a double check, military reserve units have been tasked to conduct ongoing operations security and threat assessments of DoD websites.

One useful tool is to do your own keyword search on the Internet to learn what related information is already out there that others might use to deduce information about your sensitive activity. As you visit these other sites or read newsgroup messages, see if they have information that could be used in conjunction with your information, or with information from some other site, to deduce your sensitive information.

For example, seemingly non-sensitive technical data, when associated with a specific research or development program, might provide clues to a new weapon's capabilities, vulnerabilities, or intended uses. Similarly, unclassified and seemingly innocent information on things such as personnel travel, commercial support contracts, changes in unit deployment or training, changes in communications patterns, messages between soldiers and family members, supply and equipment orders or deliveries, etc., might, when combined with other information, provide a tip-off to sensitive plans and intentions.

Related Topics: Computer Vulnerabilities, Operations Security (OPSEC), DoD Technical Data, For Official Use Only.

Reference

1. "Website Administration Policies and Procedures, November 25, 1998, Office of the Assistant Secretary of Defense (C3I). Approved by the Deputy Secretary of Defense December 7, 1998. The full document is available on the Internet at http://www.defense.gov/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.aspx