AN OFFERING IN THE BLUE CYBER SERIES:

Protection of Common Types of DOD CUI

Version 22 Jul 2021

#6 in the Blue Cyber Education Series

Protected as Controlled Unclassified Information (CUI)

Most information produced for the government are protected as Controlled Unclassified Information (CUI)

- Multiple CUI training presentations are available at www.dodcui.mil
- Also at www.dodcui.mil are several desktop aids on how to mark CUI
- DFARS 204.252-7012 requires the full implementation of NIST SP 800-171 in order to provide adequate security for CUI

CUI Basic vs CUI Specified

CUI Basic and CUI Specified are not different levels of protection.

The difference between the two is on whether the laws, Federal regulations, and Government-wide policies that authorize that category requires safeguards different from the safeguards established for CUI Basic in 32 CFR 2002.14(c),

IF SO, then the information is CUI Specified. More information on this is in 32 CFR 2002 and the CUI Registry. CUI Basic and CUI Specified markings requirements that can be found in the CUI Markings Handbook.

Your Guide to the Different Categories of CUI

https://www.archives.gov/cui/registry/category-list

For each category, this National Archives site will provide

- Definitions
- The safeguarding and/or Dissemination Authority
- Banner marking notes

CUI Category: Controlled Technical Information

Banner Marking: **CUI//SP-CTI**	Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

CUI Category: Export Controlled Research

Banner Marking for Specified Authorities: CUI//SP-EXPT **Banner Marking for Basic Authorities:** CUI	Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information. Related to the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.

Question: ITAR Technical Data has its own protections from DDTC. Is ITAR data always CUI Specific, or only when designated by a government agency? In other words, if we as a contractor are doing an internal R&D effort with ITAR data, would this be CUI//SP?

Answer: *Depending on which legal authority applies to the ITAR information in question, it could be either basic or specified. See the Export control category: https://www.archives.gov/cui/registry/category-detail/export-control.html. Banner markings appear next to each applicable authority, indicating how they should be marked.*

CUI Category: Sensitive Personally Identifiable Information

Banner Format CUI//Category Marking//Limited Dissemination Control	**A subset of PII that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements.** a. Examples of stand-alone PII include Social Security Numbers (SSN), driver's license or state identification number; Alien Registration Numbers; financial account number; and biometric identifiers such as fingerprint, voiceprint, or iris scan. b. Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements: 1. Truncated SSN (such as last four digits) 2. Date of birth (month, day, and year) 3. Citizenship or immigration status 4. Ethnic or religious affiliation 5. Sexual orientation 6. Criminal history 7. Medical information 8. System authentication information such as mother's maiden name, account passwords, or personal identification numbers c. Other PII may be "sensitive" depending on its context, such in as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

CUI Category: Legal Privilege

Banner Marking for Basic Authorities: CUI//PRIVILEGE	Per 15 USC 78x(f)(4): The term "privilege" includes any work-product privilege, attorney-client privilege, governmental privilege, or other privilege recognized under Federal, State, or foreign law. Per 502(g): (1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and (2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial. Note: There are two limited dissemination control markings that can be used with this category; Attorney Work Product (AWP), Attorney Client Privilege (AC). These limited dissemination control markings may be used to help identify the type of privilege in the document and limit the dissemination of that information so as to preserve that privilege. These limited dissemination control markings (AWP, AC) may only be used on information protected under the CUI “Legal Privilege” category.

CUI Category: Health Protected Health Information (PHI, regulated by HIPAA)

Banner Marking for Specified Authorities: CUI//SP-HLTH **Banner Marking for Basic Authorities:** CUI	As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Learn more about protected health information at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

CUI Category:
Small Business Research and Technology

Banner Marking for Basic Authorities: CUI//SBIZ	Relating to certain "Small Business Innovation Research Program" and "Small Business Technology Transfer Program" information in a government database, as referenced in 15 USC 638(k)(2).

CUI Category:
General Proprietary Business Information

Banner Marking for Specified Authorities: CUI//SP-PROPIN **Banner Marking for Basic Authorities:** CUI	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.

Export Controlled Research (regulated by ITAR, EAR)

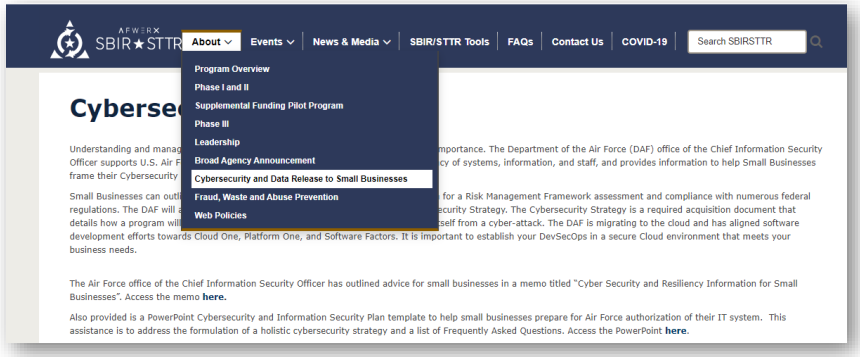
- Export Controlled Research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism, or non-proliferation. The International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) govern this data type. Current law requires that this data be stored in the U.S and that only authorized U.S. persons be allowed access to it.

Federal Information Security Management Act (FISMA) Data

- The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document, and implement security programs for information technology systems and store the data on U.S. soil.

DAF/CO Memo to SBs

https://www.afsbirsttr.af.mil/About/Cybersecurity-and-Data-Release-to-Small-Businesses/



DEPARTMENT OF THE AIR FORCE
1800 AIR FORCE PENTAGON,
WASHINGTON, DC 20330

MEMORANDUM FOR DEPARTMENT OF THE AIR FORCE SMALL BUSINESS INNOVATION RESEARCH AND SMALL BUSINESS TECHNOLOGY TRANSFER PROGRAMS

FROM: Secretary of the Air Force Chief Data Officer (SAF/CO)

SUBJECT: Release of Data to Small Businesses

1. The Department of the Air Force adheres to strict data exchange and security policies to guide in the use and release of data for contractors, civilian employees, and uniformed members of the United States Air Force, United States Space Force, the Air Force Reserve and Air National Guard. Prohibiting improper disclosure of data is vital to national security. This memorandum addresses existing policies and guidance (Enclosure) for Small Businesses to reference in their responsibilities to keep Department of the Air Force data secure. In addition, the following should also be considered:

a. Department of the Air Force data will be visible and accessible to Department of the Air Force entities except where constrained by law, regulation, security classification, guidance, or policy. Even when not constrained by exempted criterion, data exchange is tightly controlled. To keep data safe from improper disclosure or loss, every instance of data sharing with Small Business should be conducted in accordance with the most current Department of the Air Force guidance and at the direction of the local data office and/or the contract technical representative.

b. Data must be protected while at rest, in motion, and in use (e.g., within applications, and through analytics) for release to Department of the Air Force partners, including Small Business. A disciplined approach to data protection, including enterprise attribute-based access control, allows the Department of the Air Force to maximize the use of data while also employing the most stringent security standards to protect the American people.

c. The Department of the Air Force must account for the access, use, and disposition of all its data assets. A good Department of the Air Force-Small Business contractor relationship begins with the proper release of data. Suitability for data release is determined in a security and policy review process managed by the Directorate of Public Affairs (SAF/PA). Subsequently, approval for release is obtained through the appropriate chain of command.

Any Questions?

- This briefing is not a substitute for reading the FARs and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: www.safcn.af.mil/ciso/
  - Select Quick Link: Small Business Cybersecurity Information
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil
  - Daily Office Hours for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!