DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE WASHINGTON, DC

AFGM2020-16-01

23 July 2020

MEMORANDUM FOR DISTRIBUTION: MAJCOMs/FOAs/DRUs

FROM: SAF/AAZ
Air Force Pentagon
Washington, DC 20330-1040

SUBJECT: Air Force Guidance Memorandum for Controlled Unclassified Information (CUI)

ACCESSIBILITY: Publication and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/AAZO

By order of the Secretary of the Air Force, this Air Force Guidance Memorandum (AFGM) is the first instance of a to-be published Air Force publication that provides clarifying guidance concerning Department of Defense Instruction (DoDI) 5200.48, *Controlled Unclassified Information.* The DoDI provides broad and overarching guidance for a phased implementation of CUI. This AFGM implements those requirements in a phased approach. This AFGM will be updated as additional implementation guidance is received from the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). The authorities to waive wing/unit level requirements in this publication are identified with a Tier (T-0, T-1, T-2, T-3), number following the compliance statement. See AFI 33-360, *Publications and Forms Management,* for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. This AFGM does apply to the Air Force Reserve and Air National Guard. Compliance with this memorandum is mandatory.

On March 6, 2020, DoDI 5200.48 was published by OUSD(I&S). Pursuant to the authority in DoD Directive (DoDD) 5143.01 and the December 22, 2010 Deputy Secretary of Defense Memorandum, *DoD Controls Over Information Placed on Publicly Accessible Web Sites Require Better Execution*, DoDI 5200.48 established policy, assigned responsibilities, and prescribed procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556, *Controlled Unclassified Information*; Title 32, Code of Federal Regulations (CFR), Part

2002, *Controlled Unclassified Information*; and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*.

DoDI 5200.48 cancels DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information,* leaving a gap in Department of the Air Force (DAF) implementation guidance that must be addressed by way of an Air Force Guidance Memorandum. This document supplies immediate guidelines aligned with DAF leadership's intent to implement CUI policy established in DoDI 5200.48. This document supersedes sections of Air Force Instruction (AFI) 16-1404, *Air Force Information Security Program*, where the designation For Official Use Only (FOUO) is referenced.

Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program,* and disposed of in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon publishing of a new publication permanently establishing this guidance, whichever is earlier.

ANTHONY REARDON
Administrative Assistant

AFGM2020-16-01
Attachment

1. Purpose. CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information, to include classified national security information and information classified in accordance with Title 42 United States Code Section 2011-2259 (42 USC § 2011-2259). CUI also does not include information possessed and maintained by a non-executive branch entity in its own systems, provided that information does not come from, is not created for, or is not possessed by an executive branch agency or an entity acting for an agency. This AFGM provides guidance for CUI-only material and classified material containing CUI. To the extent its directions are inconsistent with other Air Force publications; the information herein prevails in accordance with AFI 33-360, *Publications and Forms Management.*

2. Responsibilities.

2.1. Secretary of the Air Force, Administrative Assistant (SAF/AA)

2.1.1. In accordance with HAF Mission Directive (MD) 1-6, serves as the Secretary of the Air Force appointed authority responsible for the oversight of Special Programs and Information Protection for the DAF.

2.1.2. On behalf of DAF, submits changes to CUI categories to the CUI Executive Agent (EA) at the National Archives and Records Administration (NARA), in collaboration with USD(I&S).

2.1.3. Provides reports to the CUI EA on the DAF CUI Program status, in accordance with DoDI 5200.48.

2.1.4. Establishes protocol for resolving disputes about implementing or interpreting Executive Order 13556, 32 CFR Part 2002, and DoDI 5200.48, within and between the DAF Components.

2.1.5. Coordinates with the Office of the Deputy Chief Information Officer (SAF/CN) on CUI waiver requests for DAF information systems (IS) and networks.

2.1.6. Coordinates with the USD(I&S) on DAF Component CUI waiver requests.

2.2. Secretary of the Air Force, Director of Security, Special Program Oversight and Information Protection (SAF/AAZ)

2.2.1. Oversees and manages the DAF CUI Program.

2.2.2. Reviews and signs all reports and other correspondence related to the DAF CUI Program.

2.2.3. Recommends changes to DAF CUI policy relating to identifying, safeguarding, disseminating, marking, storing, transmitting, reviewing, transporting, re-using, decontrolling, and destroying CUI, and responding to unauthorized disclosure (UD) of CUI.

2.2.4. Reviews and provide guidance on DAF implementation policy and CUI related matters.

2.2.5. Assists SAF/AA with overseeing the CUI policy and program execution via the Defense Security Enterprise Executive Committee in accordance with DoDD 5200.43, *Management of the Defense Security Enterprise*.

2.3. Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ)

2.3.1. Consistent with DFARS Section 252.204-7012, maintains DAF acquisition contracting processes, policies, and procedures to ensure that covered contractor information systems comply with network security requirements for handling DAF CUI in DAF procurement arrangements, agreements, and contracts, including other transaction authority actions.

2.3.2. Establishes DAF CUI processes, policies, and procedures for grants and cooperative research and development arrangements, agreements, and contracts involving controlled technical information (CTI).

2.3.3. Establishes a standard process to identify CTI; guidelines for sharing, marking, safeguarding, storing, disseminating, decontrolling, and destroying CTI; and CTI records management requirements contained in contracts, as appropriate.

2.3.4. Oversees and ensures DAF CUI guidelines and requirements for sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records management of all research, development, test, and evaluation information are properly executed for all DAF owned records.

2.3.5. Ensures DAF contracts, arrangements, and agreements for research, development, testing, and evaluation identify CUI at the time of award.

2.3.5.1. In collaboration with the Deputy Under Secretary of the Air Force for International Affairs (SAF/IA), ensures DAF international agreements, arrangements, and contracts with foreign partners identify CUI within the documents.

2.3.5.2. In collaboration with SAF/IA, ensures DAF components concluding international agreements, arrangements, and contracts with foreign partners include U.S. Government-approved text on CUI.

2.4. Secretary of the Air Force, Office of the Deputy Chief Information Officer (SAF/CN)

2.4.1. Oversees DAF CUI metadata tagging standards to implement the marking requirements in accordance with Section 6 of this document and ensures consistency of those standards with federal data tagging approaches in accordance with the National Strategy for Information Sharing and Safeguarding.

2.4.2. Integrates CUI metadata tagging standards into DAF information technology content management tools to support discovery, access, auditing, safeguarding, and records management decisions regarding CUI (including monitoring CUI data for visibility, accessibility, trust, interoperability, and comprehension).

2.4.3. Provides policy and standards recommendations to the Secretary of the Air Force, Office of the Secretary (SAF/OS) on updates for the sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records management of DAF CUI residing on both DoD and non-DoD IS in accordance with DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*.

2.4.4. Coordinates with the Director, Defense Counterintelligence and Security Agency (DCSA) to implement uniform security requirements when IS or network security controls for unclassified information are included in DAF classified contracts of the National Industrial Security Program (NISP) contractors falling under DCSA security oversight. For Special Access Programs (SAP), coordinate with the Office of Special Investigations (OSI PJ) when DCSA has been carved out and OSI PJ has been given this responsibility.

2.4.5. Coordinates with SAF/AA to:

2.4.5.1. Implements information security policy standards for markings to display CUI on DAF classified and unclassified systems and networks.

2.4.5.2. Integrates training on safeguarding and handling CUI into updates to initial and annual cybersecurity awareness training.

2.4.5.3. Notifies the CUI EA in coordination with SAF/OS of CUI waivers impacting DAF IS or networks in accordance with 32 CFR Part 2002.

2.5. MAJCOM/DRU/FOA Director, Information Protection

2.5.1. Advises the Security Program Executive (SPE) on CUI security enterprise and information protection issues within the command.

2.5.2. Integrates CUI protection into MAJCOM/DRU/FOA operations.

2.5.3. Provides oversight and direction to security specialists assigned to the MAJCOM/DRU/FOA Information Protection Directorate.

2.5.4. Provides CUI program management, oversight, risk management, policy and guidance to subordinate units within the command.

2.5.5. Ensures damage assessments are completed in accordance with DoD Manual (DoDM) 5200.01 Volume 3, *DoD Information Security Program*: *Protection of Classified Information,* and AFI 16-1404 when required.

2.6. Deputy Under Secretary of the Air Force for International Affairs (SAF/IA)

2.6.1. Authorizes the disclosures of CUI to foreign governments and international organizations in support of DAF international agreements, arrangements, and contracts with foreign partners.

3. Scope. This AFGM provides guidance relating to identification, marking, handling, sharing, decontrolling, destruction, training, and reporting requirements regarding CUI.

4. Identification and Designation.

4.1. CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI is not classified under Executive Order 13526, *Classified National Security Information,* or 42 USC § 2011-2259, as amended.

4.2 All CUI must be controlled until authorized for public release in accordance with DoDIs 5230.09, *Clearance of DoD Information for Public Release,* 5230.29, *Security and Policy Review of DoD Information for Public Release,* DoDM 5400.07, *DoD Freedom of Information Act (FOIA) Program*, and DoDM 5205.07-V1, DoD SAP Security Manual: General Procedures. (**T-0**)

4.3. Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the applicable policies, laws, regulations, and government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI. Information will not be designated CUI for any of the following reasons:

4.3.1. In order to conceal violations of law. (**T-0)**

4.3.2. Inefficiency. (**T-0**)

4.3.3. Administrative Error. (**T-0**)

4.3.4. To prevent embarrassment to a person, organization, or agency. (**T-0**)

4.3.5. To improperly or unlawfully interfere with open competition. (**T-0**)

4.3.6. To control information not requiring protection under a law, regulation, or government-wide policy, unless approved by the CUI EA at NARA, through the USD(I&S). (**T-0**)

4.4. All DAF personnel will apply at least the minimum safeguards identified in this AFGM required to protect CUI. (**T-0**)

5. Marking.

5.1. In accordance with the DoD phased CUI Program implementation described in DoDI 5200.48, all unclassified DAF documents containing CUI must at a minimum carry the "CUI" marking in the banner lines at the top and bottom of each page. Markings are to be applied at the time documents are created to properly protect the information.

5.1.1. All unclassified media/storage devices (CD, DVD, Blue Rays, Portable hard drives, etc.) containing CUI must carry CUI markings. (**T-0**)

5.1.2. Markings will be applied at the time CUI is inputted into the devices to properly protect the information. (**T-0**)

5.2. There is no requirement to add the "U," signifying unclassified, to the banner lines as was previously required with the former FOUO marking (i.e., U//FOUO).

5.3. CUI markings in classified documents will appear in paragraphs or subparagraphs known to contain **only** CUI and must be portion marked with "(CUI)." (**T-0**) "CUI" will **not** appear in the banner lines of classified documents. (**T-0**)

5.4. An acknowledgement must be added to the warning box on the first page of multi-page documents to alert readers to the presence of CUI in a classified DoD document, as shown in the DoDI 5200.48, Section 3.4, Figure 1. (**T-0**)

Figure 1. CUI Warning Box for Classified Material

This content is classified at the [insert highest classification level of the source data] level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to [cite specific reference, where possible, or state "the applicable classification guide(s)"]. This content must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release. [Add a point of contact when needed.]

5.5. In accordance with DoDI 5200.48, all DAF material containing CUI, including a document with comingled classified information, will include a CUI designation indicator containing the information as shown in DoDI 5200.48, Section 3.4, Figure 2. (**T-0**)

Figure 2. CUI Designation Indicator for All Documents and Material

Controlled by: [Name of DoD Component] (Only if not on letterhead) Controlled by: [Name of Office] CUI Category: (List category or categories of CUI) Distribution/Dissemination Control: POC: [Phone or email address]

5.6. The CUI Program does not require the redacting or re-marking of documents bearing legacy markings. However, any new document created with information derived from legacy material must be marked as CUI if the information qualifies as CUI. (**T-0**)

5.6.1. DAF legacy material is unclassified information that has been marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program. This material will not be required to be remarked or redacted while it remains under DoD control or is accessed online and downloaded for use within the DoD.

5.6.2. However, any such document or new derivative document must be marked as CUI if the information qualifies as CUI and the document is being shared outside DoD. (**T-0**)

5.6.3. DAF legacy marked information stored on a DoD access-controlled website or database does not need to be remarked as CUI, even if other agencies and contractors are granted access to such websites or databases.

5.7. Any DAF component or personnel receiving an incorrectly marked CUI document must notify either the disseminating entity or the designating agency and request a properly marked document. (**T-0**)

5.8. Authorized holders who designate CUI must not use alternative markings to identify or mark items as CUI. (**T-0**)

5.9. Within the DAF the application of the control marking "Not Releasable to Foreign Nationals" (NOFORN or NF) will only be applied, when warranted, to unclassified intelligence information properly categorized as CUI and will be reviewed by an intelligence foreign disclosure officer. (**T-0**)

5.10. CUI Basic is the default set of standards authorized holders must apply to all CUI unless there is an annotation making the material CUI Specified. **(T-0)** CUI Specified is the subset of CUI, which utilizes specific handling controls that differ from CUI Basic. During the initial phased implementation of the DAF CUI program, no required distinction must be made between Basic and Specified CUI. (**T-0**) All CUI will be protected in accordance with procedures listed in section seven of this document. Forthcoming guidance will address the distinction between the two levels of CUI. (**T-0**)

5.11. The application of "Releasable to" (REL TO) can only be applied, when warranted and consistent with relevant law, regulation, or government-wide policy or DoD policy, to information properly categorized as CUI with an export control or licensing requirement in coordination with a foreign disclosure officer.

> 5.11.1. CUI transfers to foreign persons must be in accordance with the Arms Export Control Act, International Traffic in Arms Regulations, Export Control Reform Act, Export Administration Regulations, and the DoDI 2040.02, *International Transfers of Technology, Articles, and Services*. (**T-0**)
>
> 5.11.2. In accordance with DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, and 5230.20, *Visits and Assignments of Foreign Nationals*, a positive foreign disclosure decision that has been coordinated through the local servicing Foreign Disclosure office, must be made before CUI is released to a foreign entity. (**T-0**)

6. Handling.

6.1. Authorized holders must keep all CUI under their direct control or protection with at least one physical barrier or coversheet, so as to reasonably ensure that the authorized holder or the physical barrier or cover is protecting the CUI from unauthorized access or observation when outside a controlled environment. **(T-0)**

6.2. When sending CUI only, authorized holders may utilize the U.S. Postal Service or any commercial delivery service to transport or deliver CUI to another entity. In-Transit automated tracking and accountability tools should be used when sending CUI. Interoffice or interagency mail systems may also be utilized to transfer CUI. Packages containing CUI must be marked in accordance with the following requirements: (**T-0**)

> 6.2.1. Address packages that contain CUI for delivery only to a specific recipient. (**T-0**)

6.2.2. Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI. (**T-0**)

6.3. Authorized holders may reproduce (e.g. copy, scan, print, electronically duplicate) CUI in accordance with a lawful government purpose. All, or almost all, printers, copiers, scanners, or fax machines connected to the NIPRNET retain data. Authorized holders must ensure these devices are sanitized when taken out of service in accordance with NIST SP 800-88. **(T-0)**

6.4. Classified material containing CUI will be handled in accordance with DoDM 5200.01, Volume 3 and DoDM 5205.07, Volume 1 for handling instructions. (**T-0**)

7. Safeguarding.

7.1. The DAF will safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders. (**T-0**)

7.2. DAF personnel must utilize controlled environments in order to protect CUI from unauthorized access or disclosure. **(T-0)**

7.3. Personnel must reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI. **(T-0).**

7.4. Personnel will protect the confidentiality of CUI that is processed, stored, or transmitted on DAF or federal information systems in accordance with the applicable security requirements and controls established in DoDM 5200.01, Volume 3, Enclosure 4. **(T-0)**

7.5. When working with classified material containing CUI, personnel will follow guidance in DoDM 5200.01, Volume 3 and DoDM 5205.07, Volume 1 for handling instructions. **(T-0)**

8. Storage.

8.1. DAF personnel will take steps during working hours to mitigate the risk of access by unauthorized personnel, such as not reading, disclosing, or leaving CUI information unattended where unauthorized personnel are present. **(T-0)**

8.2. After working hours, at a minimum, CUI information will be stored in unlocked containers, desks, or cabinets if the government or government-contract building provides security for continuous monitoring of access. (**T-0**) If building security is not provided, the information, at a minimum, will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas in accordance with DoDI 5200.48. (**T-0**)

8.3. The concept of a controlled environment means sufficient internal security measures are in place to prevent or detect unauthorized access to CUI. For DAF, an open storage environment is one example of a setting that meets these requirements as stated in the DoDI 5200.48.

8.4. Classified material containing CUI will be handled using the guidance in DoDM 5200.01, Volume 3 and DoDM 5205.07, Volume 1. (**T-0)**

9. Sharing, Dissemination, and Transmitting.

9.1. DAF personnel must impose dissemination controls by utilizing the dissemination controls listed in Table 2 of DoDI 5200.48, or methods authorized by a specific law, regulation, or government-wide policy. **(T-0)**

9.2. DAF personnel may not impose Limited Dissemination Controls (LDC) that unnecessarily restricts CUI access. (**T-0**)

9.3. In accordance with DoDIs 8500.01, *Cybersecurity*, 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* and AFIs 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* AFI 17-130, *Cybersecurity Program Management*, security controls for systems and networks are set to the level required by the safeguarding requirements for the data or information being processed, as identified in Federal Information Processing Standards 199 and 200. For DoD CUI, the minimum security level will be Moderate Confidentiality in accordance with 32 CFR Part 2002, and NIST SP 800-171. (**T-0**)

9.4. DAF personnel will not use unofficial or personal email accounts (e.g., .net; .com), messaging systems, or other non-DoD information systems, except approved or authorized government contractor systems to conduct official business involving CUI. **(T-0)**

9.5. DoD information systems processing, storing, or transmitting CUI will be categorized at the moderate impact level, and follow the guidance in DoDIs 8500.01 and 8510.01. (**T-0**) Air Force information systems processing, storing, or transmitting CUI will be categorized according to the Risk Management Framework process listed in AFI 17-101 and managed according to the cybersecurity program management framework listed in AFI 17-130. (**T-0**) Non-DoD information systems processing, storing, or transmitting CUI will provide adequate security, and the appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DoD entities in accordance with DoDI 8582.01. The NIST SP 800-171 governs and protects CUI on non-Federal information systems when applied by contract.

9.6. For systems, networks, and programs operating on the various domains, a splash screen warning and notice of consent, as shown in DoDI 5200.48, Section 3.10, Figure 3, must be utilized to alert users of CUI within the program. **(T-0)**

9.7. Authorized holders handling classified material containing CUI will follow guidance in DoDM 5200.01, Volume 3 and DoDM 5205.07, Volume 1 for handling instructions. (**T-0**)

10. Decontrolling.

10.1. All DAF CUI documents and materials will be formally reviewed in accordance with DoDI 5230.09 prior to being decontrolled or released to the public. (**T-0**) CUI associated with SAPs

will be reviewed by the Original Classification Authority (OCA) in accordance with the Security Classification Guide (SCG). (**T-0**)

10.2. DAF may decontrol CUI automatically upon the occurrence of one of the following events, or through an affirmative decision by the designating agency.

10.2.1. When laws, regulations, or government-wide policies no longer require its control as CUI and the authorized holder has the appropriate authority.

10.2.2. When the designating agency decides to release it to the public by making an affirmative, proactive disclosure.

10.2.3. When the agency discloses it in accordance with an applicable information access statute, such as the Freedom of Information Act (FOIA) as addressed in DoDM 5400.07. (**T-0**)

10.3. DAF material with a terminated CUI status will not be publicly released without review and approval in accordance with DoDI 5230.09, DoDI 5230.29, DoDI 5400.04, and DoDM 5205.07, Volume 1.

11. Destruction.

11.1. All DAF authorized holders will destroy records and non-record copies of CUI in accordance with Chapter 33 of Title 44, U.S.C. (**T-0)**

11.2. When destroying record and non-record CUI documents and CUI in electronic form, the DAF must do so in a manner making it unreadable, indecipherable, and irrecoverable. (**T-0**) In accordance with Section 2002.14 of Title 32, CFR and NIST SP 800-88, record and non-record CUI documents must be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and unrecoverable. (**T-0**)

11.3. Classified material containing CUI will follow guidance in DoDM 5200.01, Volume 3 and DoDM 5205.07, Volume 1 for handling instructions. (**T-0**)

12. Training.

12.1. The DCSA and Center for Development of Security Excellence in collaboration with USD(I&S), is in the process of developing CUI training. The expected completion date is September 2020. Once this training becomes available and is disseminated, initial and annual training for CUI will be required, to include maintaining documentation for audit purposes. (**T-0**)

12.1.1. Until the DCSA CUI training becomes available, DAF personnel are not required to complete any CUI training.

12.1.2. Forthcoming guidance will address the timeline for implementing DAF CUI training.

12.2. DAF CUI training will ensure that personnel who have access to CUI receive training on the following: **(T-0)**

12.2.1. Designating CUI. (**T-0**)

12.2.2. Relevant CUI categories and subcategories. (**T-0**)

12.2.3. The CUI Registry. (**T-0**)

12.2.4. Associated Markings. (**T-0**)

12.2.5. Applicable safeguarding, dissemination, and decontrolling policies and procedures. (**T-0**)

12.3. The DoD CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this part.

12.3.1. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

12.3.2. The DoD CUI Registry can be found at the following site. https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx

13. Reporting Requirements.

13.1. Safeguarding requirements and incident response measures for misuse or UD of CUI must be implemented across DAF. (**T-0**)

13.1.1. Senior leaders, contracting officers, commanders, and supervisors at all levels must consider and take appropriate administrative, legal, or other corrective or disciplinary action to address CUI misuse or UD commensurate with the appropriate law, regulation, or government-wide policy. **(T-0)**

13.1.2. Further guidance is forthcoming regarding relevant procedures.

14. Requirements for DAF Contractors.

14.1. When the DAF provides information to contractors, an individual with the appropriate signature and obligation authority must ensure CUI is identified either entirely or partially with assistance from the requirements owners (e.g. program management/acquisition team) via the contracting vehicle, agreement, and/or grant, and will ensure such documents, material, or media are marked in accordance with section six of this document. **(T-0)**

14.2. Whenever the DAF provides CUI to, or CUI is generated by, non-DoD entities, all CUI records must be handled as required by the approved mandatory disposition authority. The contracting officer will ensure protective measures and dissemination controls, including those directed by relevant law, regulation, or government-wide policy, and are expressly written in the contract, grant or other legal agreement, as appropriate. **(T-0)**

14.3. Contracting officers will ensure DAF contracts require contractors to monitor CUI aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. **(T-0)**

14.4. DAF personnel and contractors, pursuant to mandatory DoD contract provisions, will submit unclassified DAF information for review and approval for release in accordance with the Standard DoD Component Processes, DoDI 5230.09, and DoDM 5205.07, Volume 1. **(T-0)**

14.5. All CUI records must follow the approved mandatory disposition authority whenever the DAF provides CUI to, or CUI is generated by, non-DoD entities in accordance with Section 1220-1236 of Title 36, CFR, Section 3301a of Title 44, U.S.C., and the DoDI 5200.48. (**T-0**)

14.6. Certification from the Defense Logistics Agency (DLA) is required before a non-governmental entity (e.g. Contractor, University, Vendor etc.) can handle, have access to or have discussions concerning DOD and/or Canadian Department of National Defense (DND) controlled unclassified information. This includes, controlled unclassified hardware, software and export controlled technical data. During the acquisition process, the Air Force agency that is sponsoring the work has the responsibility to ensure that the non-governmental entity has a valid certification by checking their cage code or name through the certification database: https://public.logisticsinformationservice.dla.mil/jcp/search.aspx."