**Department of Veterans Affairs**
**Washington, DC 20420**

**VA DIRECTIVE 6332**
**Transmittal Sheet**
**June 4, 2024**

# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

1. **REASON FOR ISSUE**: To establish the Department of Veteran Affairs (VA) policy for Controlled Unclassified Information (CUI) in accordance with Executive Order (EO) 13556 and Title 32 Code of Federal Regulations (CFR) Part 2002.

2. **SUMMARY OF CONTENT/MAJOR CHANGES**: This is a new directive. This directive sets forth the following:

   a. Policy for the VA CUI Program which requires VA-wide compliance with EO 13556, 32 CFR Part 2002 and the CUI Registry;

   b. Responsibilities for implementing, managing and monitoring the VA CUI Program; and

   c. References related to the VA CUI Program.

3. **RESPONSIBLE OFFICE**: Office of Information and Technology (OIT) (005).

4. **RELATED HANDBOOK**: Not applicable.

5. **RESCISSION**: Not applicable.

**CERTIFIED BY:**

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:**

/s/
Kurt DelBene
Assistant Secretary for
Information and Technology and
Chief Information Officer

**DISTRIBUTION**: Electronic only

# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

## TABLE OF CONTENTS

# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

## 1. PURPOSE AND SCOPE.

a. On November 4, 2010, the President signed EO 13556, establishing the CUI Program and designating the National Archives and Records Administration (NARA) as the CUI Executive Agent (CUI EA) to oversee agency actions and ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

b. The CUI Program is an information management framework designed to standardize the way the executive branch handles information it creates or possesses, or that an entity creates or possesses for or on its behalf, that requires safeguarding or dissemination controls in accordance with law and government-wide policies, excluding information that is classified under EO 13526, Classified National Security Information, 75 Federal Register (FR) 707 (Jan. 5, 2010), or the Atomic Energy Act of 1954 (42 United States Code (U.S.C.) § 2011, et seq.).

c. On November 14, 2016, 32 CFR Part 2002 established requirements for agencies on designating, safeguarding, disseminating, marking, decontrolling and disposing of CUI, self-inspection and oversight requirements and other requirements of the CUI Program. 32 CFR Part 2002 affects federal executive branch agencies that create or possess CUI as well as other entities that create or possess CUI on behalf of the federal government.

d. The VA CUI program standardizes and simplifies the way in which VA will mark and safeguard sensitive documents. The new category of “CUI” is meant to replace previous forms of marking sensitive information. The VA CUI Program will be implemented in phases.

e. This directive establishes a high-level policy for all VA personnel on the requirements of the CUI Program in accordance with EO 13556, 32 CFR Part 2002 and the CUI Registry. VA personnel includes VA contractors, business associates and other entities that handle VA information under contract, agreement, or other legally binding document. Further requirements and training regarding processes, roles and responsibilities will be provided prior to the full transition to the CUI Program.

2. **LIMITATIONS ON APPLICABILITY OF THIS DIRECTIVE.** CUI requirements contained within this directive do not apply to non-VA entities other than contractors, business associates, or other entities described above unless a law, regulation, or government-wide policy (LRGWP) permits or requires VA to impose such requirements. Nothing in this policy may be construed or used as the basis for withholding any information from VA, including the VA Office of Inspector General (OIG) except pursuant to any provision of law enacted by Congress that (1) expressly refers to the Inspector General and (2) limits the right of access of the Inspector General. Any information withheld from OIG must be properly marked with the correct CUI marking that identifies the applicable law authorizing withholding under § 6(a)(1)(B) of the Inspector General Act of 1978 [5 U.S.C. App. 3] or identifies Grand Jury material withheld under § 6(a)(1)(C) of the Act.

3. **POLICY.** The following sections define the requirements of the CUI Program and their applicability within the Department. Additionally, the roles and responsibilities of personnel within the Department are defined in section 4, entitled *Responsibilities*, as they relate to the CUI Program.

   a. **CUI Registry**. The CUI Registry, which was developed by NARA, is an online, publicly available repository of all CUI guidance, requirements and categories of CUI to include 32 CFR Part 2002 and EO 13556. The CUI Registry is the sole authoritative repository for requirements of the CUI Program and is the primary source for determining which unclassified information requires or permits agencies to handle that information by means of safeguarding or dissemination controls. VA may not implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by the CUI Registry, unless otherwise permitted by NARA following a formal request process. The CUI Registry can be found at https://www.archives.gov/cui. Prior to the full transition to CUI operations, VA will issue tailored guidance that will supplement the CUI Registry and serve as VA's primary source for Category, marking and authority references and guidance.

   b. **CUI Categories**. The CUI Registry provides a repository of all LRGWP that identify unclassified information as CUI. This list of LRGWP is organized by Category Groupings which are further broken down into Categories. Categories of CUI organize the Registry by similar LRGWP to streamline markings and to reduce confusion for agencies and their workforce. Per CUI Program requirements, VA will follow NARA's list of CUI Categories and associated LRGWP as defined in the CUI Registry to identify, mark, safeguard, disseminate, decontrol and destroy CUI.

   c. **Types of CUI**. There are two primary types of CUI; CUI Basic and CUI Specified. These types of CUI differ based on the controls defined within the associated LRGWP of each Category. The term "controls" refers to the safeguarding or dissemination requirements that the LRGWP requires or permits agencies to use when handling CUI. The definition of the two types of CUI, as defined in 32 CFR Part 2002, can be found below:

(1) ***CUI Basic*** is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in [32 CFR Part 2002] and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified) and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

(2) ***CUI Specified*** is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations and Government-wide policies do not provide specific guidance.

d. **Authorized Holders of CUI**. An authorized holder is an individual, organization, or group of users that is permitted to designate or handle CUI, consistent with the guidelines in this directive, 32 CFR Part 2002 and the CUI Registry. At VA, authorized holders are considered any personnel who has completed the mandatory VA CUI Basic training as assigned in the VA Talent Management System (TMS). However, authorized holders may only handle CUI when furthering a lawful government purpose.

e. **Lawful Government Purpose.** Lawful government purpose, as defined by the CUI Registry, is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement). At VA, an authorized holder's lawful government purpose is defined by VA policy, position descriptions, or contractual requirements.

f. **CUI Training**. All levels of VA staff, contractors, volunteers, interns and trainees may complete CUI Basic training assigned through the VA Talent Management System (TMS). If updates are made to the training course, or if VA identifies a need to increase the frequency of training, VA may change the training frequency or requirements for training completion at any time. Additional, role-based, or similar, training may also be assigned through the VA TMS for VA personnel who have specialize job requirements or handle CUI Specified on a regular basis, as deemed necessary.

g. **Identifying and Marking CUI**. VA authorized holders must be able to identify information that qualifies as CUI and mark that information as CUI in accordance

with 32 CFR Part 2002, the CUI Registry that established the CUI Categories, the applicable LRGWPs, this Directive and additional VA CUI implementation guidance as it becomes available.

h. **Accessing and Disseminating CUI**. VA authorized holders may only disseminate and permit access to CUI to authorized holders in accordance with a lawful government purpose. Authorized holders may not restrict access to CUI unless a LRGWP in the CUI Registry requires them to do so. Authorized holders must have a reasonable expectation that the recipient of CUI is aware of and understands the safeguarding requirements defined in 32 CFR Part 2002 and the CUI Registry.

i. **Physical Safeguarding of CUI**. In accordance with 32 CFR Part 2002, VA authorized holders must safeguard CUI in a manner that minimizes the risk of unauthorized disclosure while allowing for timely access by authorized holders. Authorized holders will have access to controlled environments in which to protect physical CUI from unauthorized access or observation. When outside a controlled environment, the authorized holder must keep the physical CUI under their direct control or protect it with at least one physical barrier. The authorized holder or the physical barrier must protect the CUI from unauthorized access or observation. When an authorized holder discusses CUI, they must reasonably ensure that unauthorized individuals cannot overhear the conversation and that unauthorized users cannot access or observe CUI. For example, authorized holders should discuss CUI only when furthering a lawful government purpose and only within the confines of a closed conference room or closed office. VA physical security requirements for specialized organizations such as those defined in *VA Directive* and *Handbook 0730* are also sufficient for the safeguarding of CUI if the physical security requirements meet the minimum standard of one physical barrier for CUI Basic or any additional requirements for CUI Specified as defined by the coinciding Category LRGWP. VA authorized holders must comply with VA's CUI physical safeguarding standards when these directives and handbooks do not apply. The physical input and output products of VA information systems that contain CUI, such as disks, paper, flash drives or any other data storage device, shall be marked as containing CUI and they should be protected against misuse and unauthorized access, unauthorized disruption, unauthorized disclosure, or unauthorized modification or destruction. Safeguarding measures that are authorized or accredited for classified information are also adequate for safeguarding CUI.

j. **Safeguarding Electronic CUI**. VA information systems that process, store, or transmit CUI must be configured, at a minimum, to meet the Moderate Confidentiality Impact Value in accordance with 32 CFR Part 2002 and National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems, as incorporated by reference, but can also be configured to meet the High Confidentiality Impact Value internally or by means of agreement. VA must also apply the appropriate security

requirements and controls defined in FIPS PUB 200, Minimum Security requirements for Federal Information and Information Systems and Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, to CUI as incorporated by reference in 32 CFR Part 2002. Non-Federal information systems that contain Federal Information that VA determines is CUI must follow the requirements defined in NIST SP 800-171 and must also follow the requirements in NIST SP 800-172 as determined appropriate by VA. These requirements are applicable unless the LRGWP for the CUI Category of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality. For more information regarding the establishment or management of a VA system, please see *VA Handbook 6500*.

k. **Decontrolling CUI**. Decontrolling CUI relieves authorized holders from requirements to handle the information under the CUI Program but does not constitute authorization for release.

(1) VA employees designated as authorized holders shall be authorized to decontrol CUI, consistent with VA guidance and the corresponding LRGWP. VA contractors and all other non-employees are not authorized to decontrol CUI unless explicitly authorized by the VA CUI SAO, VA CUI PM, or designee to allow CUI decontrol authority to be included in a contract, inter-agency agreement, or other legal instrument with an external party.

(2) VA must decontrol any CUI designated by VA that no longer requires safeguarding or dissemination controls as soon as is practicable, unless doing so conflicts with the governing law, regulation, or Government-wide policy.

l. **CUI and Records Management**. The indication of CUI does not affect the NARA approved records retention and disposition requirements for VA records. Records must still be maintained per applicable Record Control Schedules or General Records Schedules. However, if the record does contain CUI, then CUI approved destruction practices must be followed for any record requiring destruction. Once agencies implement the CUI Program, legacy markings such as FOUO or SBU will no longer be used. As the CUI Program is implemented, U//FOUO will cease to be an authorized marking, but you may still see it on legacy documents as we transition to CUI.

m. **Transferring Records with CUI**. When feasible, VA should decontrol records containing CUI prior to transferring to NARA. When VA cannot decontrol records before transferring them to NARA, VA must indicate on a Transfer Request in NARA's Electronic Records Archives or on a Standard Form 258 paper transfer form, that the records should continue to be controlled as CUI.

n. **Waivers of CUI Marking Requirements.** Marking waivers may be issued for CUI when it is determined that marking the CUI is excessively burdensome and does not affect the safeguarding of the information. VA authorized holders may submit a waiver request to the VA CUI Senior Agency Official (SAO) and CUI Program Manager (PM) for all or some of the CUI marking requirements while the CUI remains within VA. The VA CUI SAO and CUI PM may also determine that a waiver is appropriate if removing legacy markings or if re-marking legacy information as CUI would be excessively burdensome. To submit a waiver request, VA authorized holders can send an email to CUI@va.gov describing the circumstances requiring a waiver and the VA CUI SAO and CUI PM will review and respond to the request accordingly.

o. **CUI and Disclosure Statutes.** The fact that information is designated as CUI does not prohibit its disclosure if it is made according to criteria set out in a governing law such as FOIA or the Whistleblower Protection Act of 1989.

p. **CUI Incident Identification and Reporting.** VA personnel are required to report the misuse of CUI when CUI is used in a manner not in accordance with EO 13556, 32 CFR Part 2002, the CUI Registry, this directive, or the applicable LRGWP that governs 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. If the misuse of CUI, intentional or unintentional, is suspected, VA employees, contractors and other personnel must report all CUI complaints or actual or suspected misuse or breaches involving CUI. All such incidents with CUI implications must be responded to in a timely fashion in accordance with 32 CFR Part 2002, VA incident and data breach management policies such as VA Handbook 6500.2 and as defined by sanctions associated with LRGWP in the CUI Registry.

q. **Challenges to the Designation of CUI**. VA-authorized holders who believe that information has been incorrectly designated as CUI should contact the VA CUI PM at CUI@va.gov for assistance.

## 4. RESPONSIBILITIES.

a. **VA CUI Senior Agency Official (SAO)** shall:

(1) Direct and oversee VA's CUI Program;

(2) Designate a VA CUI Program Manager (PM);

(3) Ensure VA has CUI implementing policies and plans, as needed;

(4) Approve VA policies, as required, to implement the CUI Program; and

(5) Establish and maintain a self-inspection program to ensure VA complies with the principles and requirements of EO 13556, 32 CFR Part 2002 and the CUI Registry.

(6) Implement an education and training program pursuant to 32 CFR 2002.30;

(7) Upon request of the CUI EA under section 5(c) of EO 13556, provide an update of CUI implementation efforts for subsequent reporting;

(8) Submit to the CUI EA any law, regulation, or Government-wide policy not already incorporated into the CUI Registry that VA proposes to use to designate unclassified information for safeguarding or dissemination controls;

(9) Coordinate with the CUI EA, as appropriate, any proposed law, regulation, or Government-wide policy that would establish, eliminate, or modify a category of CUI, or change information controls applicable to CUI;

(10) Establish processes for handling CUI decontrol requests submitted by authorized holders;

(11) Establish basic physical safeguarding standards where VA Directive 0730 and Handbook 0730 do not apply and align such standards with other existing VA policies;

(12) Establish a mechanism by which authorized holders (both inside and outside VA) can contact a designated VA representative for instructions when they receive unmarked or improperly marked information a VA authorized holder designated as CUI;

(13) Establish a process to accept and manage challenges to CUI status (which may include improper or absent marking);

(14) Establish processes and criteria for reporting and investigating misuse of CUI; and

(15) Follow the requirements for the CUI SAO listed in 32 CFR 2002.38(e), regarding waivers for CUI.

b. **VA CUI Program Manager (PM)** shall:

(1) Serve as the manager in charge of implementing the CUI Program at VA;

(2) Define CUI Program implementation strategies and plans and execute strategies and plans to meet the requirements of the CUI Program;

(3) Develop and implement policies to issue CUI Program compliance requirements at VA;

(4) Develop and implement training and educational materials to inform VA authorized holders on their roles and responsibilities as they relate to CUI;

(5) Support the establishment and implementation of a self-inspection program to ensure VA complies with the requirements of EO 13556, 32 CFR Part 2002 and the CUI Registry;

(6) Oversee and manage the process for handling CUI decontrol requests submitted by authorized holders;

(7) Oversee and manage the incident management process for reporting and investigating misuse of CUI;

(8) Oversee and manage the process for addressing disputes and challenges to CUI status (which may include improper or absent marking);

(9) Oversee and manage the mechanism in which authorized holders (both inside and outside the agency) can contact a designated VA representative for instructions when they receive unmarked or improperly marked information VA designated as CUI;

(10) Attend meetings conducted by the CUI EA (e.g., the CUI Advisory Council) and communicate critical program updates to the CUI SAO as necessary; and

(11) Upon request of the CUI EA under section 5(c) of EO 13556, provide an update of CUI implementation efforts on an annual basis following the NARA ISOO developed reporting template for subsequent reporting.

c. **VA Chief Information Security Officer** shall Ensure VA IT system security directives and handbooks reflect CUI security requirements for VA IT systems, as well as non-federal IT systems that are storing information on behalf of the VA.

d. **VA Senior Agency Official for Privacy must do the following** shall Ensure VA privacy directives and handbooks reflect privacy-related CUI requirements.

e. **VA Contracting Officers (COs) and Contracting Officer Representatives (CORs)** shall follow the responsibilities as outlined in VAAR 839.101 as it pertains to protecting VA information, information systems and information technology when acquiring information technology, including information technology-related contracts which may involve services (including support services) and related sources.

f. **VA Supervisory Personnel** shall

(1) Ensure staff complete all mandatory CUI training assigned in TMS and understand this directive, their role and responsibilities as they relate to the CUI Program and VA CUI marking and handling requirements;

(2) Ensure that all complaints and actual or suspected incidents or breaches of CUI are recorded following the requirements in this directive and in VA Handbook 6500.2 for incidents or breaches of VA Sensitive Information;

(3) If necessary, escalate issues regarding CUI to the CUI PM and respond to requests for CUI related reports in a timely manner; and

(4) Assist VA PMs in resolving CUI incidents in a timely fashion and in accordance with applicable LRGWP, when related to their office, job function, or staff.

g. **VA Personnel** shall:

(1) Only handle or access CUI in accordance with Handbook. 6500 and the Rules of Behavior (ROB), for a lawful government purpose.

(2) Submit requests, as necessary, to decontrol CUI or to waive CUI marking requirements following VA's decontrol and waiver request processes.

(3) Notify the designating agency of any information suspected to be incorrectly designated as CUI.

(4) Report all complaints and actual or suspected incidents (including information incorrectly designated as CUI) or breaches involving CUI following the requirements in this directive.

(5) Utilize controlled environments in accordance with Handbook. 6500 and the ROB to protect CUI from unauthorized access or observation when observing or discussing CUI in accordance with this directive.

(6) Comply with Handbook. 6500 and the ROB to protect CUI from unauthorized access or observation using a physical or electronic barrier especially when outside a controlled environment.

## 5. REFERENCES.

a. Statutes and Regulations:

(1) Controlled Unclassified Information (CUI) 32 CFR Part 2002

(2) Freedom of Information Act (FOIA), 5 U.S.C. § 552

(3) Privacy Act of 1974, 5 U.S.C. § 552a

(4) Confidential Nature of Claims, 38 U.S.C. § 5701

(5) Confidentiality of Medical Quality Assurance Records, 38 U.S.C. § 5705

(6) Confidentiality of Certain Medical Records, 38 U.S.C. § 7332

(7) Health Insurance Portability and Accountability Act (HIPAA) Regulations, 45 CFR Parts 160 and 164

(8) Federal Acquisition Regulation (FAR), 48 CFR Part 52

(9) Whistleblower Protection Act of 1989, 5 U.S.C. 2302(b)(8)-(9), Pub. 101-12

b. Executive Orders, Presidential Directives and Memorandums: EO 13556, Controlled Unclassified Information (Nov. 4, 2010)

c. National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS):

(1) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

(2) NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

(3) NIST 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

(4) NIST 800-88, Guidelines for Media Sanitization

(5) FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

(6) FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

d. VA Directives and Handbooks:

(1) VA Directive 0730, Security and Law Enforcement

(2) VA Handbook 0730, Security and Law Enforcement

(3) VA Directive 6300, Records and Information Management

(4) VA Handbook 6300.1, Records Management Procedures

(5) VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act

(6) VA Directive 6500, VA Cybersecurity Program

(7) VA Handbook 6500, Risk Management Framework for VA Information Systems: VA Information Security Program

(8) VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information

(9) VA Directive 6502, VA Enterprise Privacy Program

(10) VHA Directive 1605, VHA Privacy Program

(11) VHA Directive 1605.01, Privacy and Release of Information

(12) VHA Directive 1605.2, Minimum Necessary Standard for Access, Use, Disclosure and Requests for Protected Health Information

(13) VHA Directive 1605.5, Business Associate Agreements

(14) VHA Directive 1907.01, Health Information Management and Health Records

(15) VHA Directive 1907.08 Health Care Information Security Policy and Requirements

e. Supplemental Resources:

(1) NARA CUI Registry: https://www.archives.gov/cui

(2) VA CUI Intranet Site: https://vaww.oit.va.gov/services/cui

## 6. DEFINITIONS.

a. **Agency**: Any "executive agency," as defined in 5 U.S.C. § 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI. Agency may also be referred to as Federal agency, executive agency and executive branch agency, or may refer to VA in this directive.

b. **Agreements and arrangements**: Any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, purchase card orders and information-sharing agreements or arrangements.

c. **Authorized Holder**: An individual, organization, or group of users that is permitted to designate or handle CUI, consistent with the guidelines in this directive, EO 13556, 32 CFR Part 2002 and the CUI Registry as permitted by a

lawful government purpose, based on the job function, organizational purpose, or need of the authorized holder.

d. **Classified Information**: Information that has been determined pursuant to EO 13526, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require agencies to mark with classified markings and protect against unauthorized disclosure.

e. **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 U.S.C., SEC. 3542].

f. **Controlled Environment**: Any area or space that an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) to protect CUI from unauthorized access or disclosure.

g. **Control Level**: A general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.

h. **Controlled Unclassified Information (CUI)**: Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that an LRGWP requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

i. **Controls**: Safeguarding or dissemination controls that an LRGWP requires or permits agencies to use when handling CUI. The authority may specify the controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information.

j. **CUI Basic**: The subset of CUI for which the authorizing LRGWP does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR Part 2002 and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified in this section) and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

k. **CUI Categories**: Types of information for which LRGWP require or permit agencies to exercise safeguarding or dissemination controls and which the CUI EA has approved and listed in the CUI Registry. The controls for any CUI Basic Categories are the same, but the controls for CUI Specified Categories can differ from CUI Basic ones and from each other. If dealing with CUI that falls into a CUI Specified Category, review the controls for that Category on the CUI Registry.

l. **CUI Category Markings**: Markings approved by the CUI EA for the Categories listed in the CUI Registry.

m. **CUI Executive Agent (EA)**: The EA for CUI is NARA, which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with EO 13556. NARA has delegated this authority to the Director of ISOO.

n. **CUI Program**: The executive branch wide program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization and procedures for CUI, established by EO 13556, 32 CFR Part 2002 and the CUI Registry.

o. **CUI Program Manager (PM)**: An agency official, designated by the agency head or CUI SAO, to serve as the official representative to the CUI EA on the agency's day-today CUI Program operations, both within VA and in interagency contexts.

p. **CUI Registry**: The online repository for all information, guidance, policy and requirements on handling CUI, including everything issued by the CUI EA other than 32 CFR Part 2002. Agencies and authorized holders must follow the requirements in the CUI Registry. Among other information, the CUI Registry identifies all approved CUI Categories, provides general descriptions for each, identifies the basis for controls and sets out handling procedures.

q. **CUI Senior Agency Official (SAO)**: A senior official designated in writing by an agency head and responsible to that agency head for implementation of the CUI Program within that agency. The CUI SAO is the primary point of contact for official correspondence, accountability reporting and other matters of record between VA and the CUI EA.

r. **CUI Specified**: The subset of CUI in which the authorizing LRGWP contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which LRGWP include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing LRGWP do not provide specific requirements.

s. **Decontrolling**: Occurs when an authorized holder removes safeguarding or dissemination controls from CUI that no longer requires such controls, as described in this directive.

t. **Designating CUI**: Occurs when an authorized holder determines that a specific item of information falls into a CUI Category. The authorized holder who designates the CUI must make recipients aware of the information's CUI status.

u. **Designating Agency**: The executive branch agency that designates or approves the designation of a specific item of information as CUI.

v. **Disseminating**: Occurs when authorized holders provide access, transmit or transfer CUI to other authorized holders through any means, whether internal or external to an agency.

w. **Document**: Any tangible thing which constitutes or contains information. It also refers to the original and any copies (whether different from the originals or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events and including, but not limited to correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits and containers, the labels on them and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter and other data compilations from which information can be obtained, including materials used in data processing.

x. **Federal Information System**: Any information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. An information system operated on behalf of an agency provides information processing services to the agency that the government might otherwise perform itself but has decided to outsource. This includes systems operated exclusively for government use and systems operated for multiple users (multiple Federal agencies or government and private sector users). Information systems that a non-executive branch entity operates on behalf of an agency are subject to the requirements of this part as though they are the agency's systems and agencies may require these systems to meet additional requirements the agency sets for its own internal systems. An information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

y. **Handling**: Any use of CUI, including but not limited to, marking, safeguarding, transporting, disseminating, re-using and disposing of the information.

z. **Lawful Government Purpose**: Any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

aa. **Legacy Material**: Unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

bb. **Limited Dissemination**: Any CUI EA approved control that agencies may use to limit or specify CUI dissemination.

cc. **Misuse of CUI**: When CUI is used in a manner inconsistent with the policy contained in EO 13556, 32 CFR Part 2002, the CUI Registry, agency CUI policy, or the applicable LRGWP 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.

dd. **Moderate Confidentiality Impact Value**: A value as defined by FIPS 199 that is set on information in which the loss of confidentiality could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

ee. **National Security System**: A special type of information system (including telecommunications systems) whose function, operation, or use is defined in National Security Directive 42 and 44 U.S.C. § 3542(b)(2).

ff. **Non-executive Branch Entity**: A person or organization established, operated and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations. Non-executive branch entity does not include foreign entities, nor does it include individuals or organizations when they receive CUI information pursuant to Federal disclosure laws, including the FOIA and the Privacy Act of 1974.

gg. **Non-Federal information system**: Any information system that does not meet the criteria for a Federal information system. Agencies may not treat non-Federal information systems as though they are agency systems, so agencies cannot require that non-executive branch entities protect these systems in the same manner that the agencies might protect their own information systems. When a non-executive branch entity receives Federal information only incidental to providing a service or product to the government other than processing

services, its information systems are not considered Federal information systems. NIST SP 800-171 defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. NIST SP 800-172, which serves as a supplement to 800-171, provides additional safeguards for Agencies to apply at their discretion. Agencies must use NIST SP 800-171 and should use NIST SP 80-172, when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing LRGWP listed in the CUI Registry for a CUI Specified category prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

hh. **On behalf of an agency**: Occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information and those activities are not incidental to providing a service or product to the government.

ii. **Protection**: Includes all controls an agency applies or must apply when handling information that qualifies as CUI.

jj. **Public Release**: Occurs when the agency that originally designated information as CUI makes that information available to the public through the agency's official public release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release. Releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request also does not automatically constitute public release, although it may if that agency ties such actions to its official public release processes. Even though an agency may disclose some CUI to a member of the public, the government must still control that CUI unless the agency publicly releases it through its official public release processes.

kk. **Records**: All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

ll. **Required or permitted (by an LRGWP)**: The basis by which information may qualify as CUI. If a LRGWP requires that agencies exercise safeguarding or dissemination controls over certain information, or specifically permits agencies the discretion to do so, then that information qualifies as CUI. The term 'specifically permits' in this context can include language such as “is exempt from” applying certain information release or disclosure requirements, “may” release or disclose the information, “may not be required to” release or disclose

the information, “is responsible for protecting” the information and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions and powers, regardless of the source. The CUI Registry reflects all appropriate authorizing authorities.

mm. **Restricted Data (RD)**: A type of information classified under the Atomic Energy Act, defined in 10 CFR part 1045, Nuclear Classification and Declassification.

nn. **Re-use**: Incorporating, disseminating, restating, or paraphrasing CUI from its originally designated form into a newly created document.

oo. **Self-inspection**: An agency’s internally managed review and evaluation of its activities to implement the CUI Program.

pp. **Unauthorized Disclosure**: Occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.

qq. **Uncontrolled Unclassified Information**: Information that neither EO 13556 nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.