Guidance Document

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

Document Summary: The following document, issued by the Cybersecurity and Infrastructure Security Agency (CISA), describes in detail how to identify, handle, and safeguard information developed by private and public entities that meets the definition of Chemical-terrorism Vulnerability Information (CVI).

Document Title: Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information (CVI)

Issued by: Infrastructure Security Compliance Division, Cybersecurity and Infrastructure Security Agency

Date of Issuance/Revision: September 2008

Affected parties: Individuals attempting to access, handle, and safeguard information that is or should be considered CVI.

Statutory or regulatory provisions interpreted: 6 CFR 27.400

Document Identification Number: CISA-CFATS-001

Link: www.cisa.gov/publication/safeguarding-cvi-manual

Safeguarding Information Designated As Chemical-Terrorism Vulnerability Information (CVI)

Revised Procedural Manual

September 2008

Homeland Security

Table of Contents

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under OMB's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

1.0 Purpose

The Department of Homeland Security (DHS) issues this Manual to provide guidance on how to identify, handle and safeguard information developed by private and public entities under Section 550 of Public Law 109-295 and its implementing regulations, the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27. Pursuant to CFATS, this information is known as Chemical-terrorism Vulnerability Information, or CVI.

This Manual updates and replaces the DHS CVI Procedural Manual issued in June 2007.

Any CVI-related questions not addressed in this Manual should be directed to the DHS Chemical Security Assessment Tool (CSAT) Helpdesk at 866-323-2957 or CSAT@dhs.gov.

2.0 Scope

This Manual is relevant for anyone authorized to possess or receive CVI (including chemical facility officers, employees, representatives and contractors, and Federal, state, local and tribal government employees and contractors), as well as anyone who obtains what they reasonably should know is CVI.

3.0 Authorities

Section 550(c) of Public Law 109-295, entitled *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes* (Oct. 4, 2006), directs DHS to protect from public disclosure "information developed under [Section 550], including vulnerability assessments … and other security related information, records and documents …." As required by Section 550, DHS promulgated CFATS as an interim final rule in April 2007. *See* 6 CFR Part 27; 72 Fed. Reg. 17688.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

4.0 Definitions

For purposes of this Manual, the following definitions apply:

Assistant Secretary - The Department of Homeland Security Assistant Secretary for Infrastructure Protection or designee.

Authorized User– Any person who has: [1]

- completed DHS on-line CVI training, which includes obtaining an Authorized User number, or equivalent measures approved by DHS; and
- complied with any background checks or other requirements for personal identification or trustworthiness that DHS may require under 6 CFR §§ 27.400(e)(2)(iii), and 27.400(e)(3).

Automated Information Systems – Any computer-based system that either:

- enables a facility to submit CVI to DHS (e.g., via the DHS Chemical Security Assessment Tool or CSAT); or
- allows for the electronic storage and transmission of CVI.

Chemical Facility or Facility – Any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department. As used herein, the terms chemical facility or facility shall also refer to the owner or operator of the chemical facility.

Chemical-terrorism Vulnerability Information (CVI) – Information listed in 6 CFR § 27.400(b) of the CFATS regulations, as well as derivative products developed from other CVI documents. (*See* Chapter 9.1.)

Covered Facility – A chemical facility determined by the Assistant Secretary to present a high level of security risk. (*See* 6 CFR § 27.105.)

Covered Person – A person who meets the regulatory definition set forth in 6 CFR § 27.400, specifically, anyone who:

- has a "need to know," as described in 6 CFR § 27.400(e), or
- otherwise receives or gains access to what they know or should reasonably know constitutes CVI.

[1] As provided by 6 CFR § 27.400(e)(3), DHS has determined that, except under emergency or exigent circumstances, successful completion of DHS-provided CVI training is a necessary and appropriate condition for any individual's access to CVI. DHS reserves the right under 6 CFR § 27.400(e)(2)(iii) to require non-disclosure agreements in the future, as appropriate, as a condition for becoming an Authorized User or otherwise obtaining access to CVI.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

Emergency or exigent circumstances – Circumstances that may include the existence of a threat to public health or public safety or other unique circumstances that warrant immediate action to provide access to CVI.

Infrastructure Security Compliance Division (ISCD) – The Division within the Office of Infrastructure Protection responsible for executing the Department of Homeland Security's responsibilities pursuant to P.L. 109-295 and its implementing regulations at 6 CFR Part 27. Unless otherwise specified, all references in this Manual to DHS refer to ISCD.

Need to Know – The determination that a prospective recipient requires access to specific CVI to perform or assist in a lawful and authorized function, as specified in 6 CFR § 27.400(e).

Secretary – The Secretary of the Department of Homeland Security or any person, officer or entity within the Department to whom the Secretary has delegated authority under Section 550.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

5.0 What is CVI

5.1 Information Designated as CVI

Consistent with Section 550(c), information is CVI only if it was developed and/or submitted to DHS pursuant to Section 550(c) and the CFATS regulation. Under CFATS, the following information (whether written, verbal, electronic, or digital) is CVI:

§27.400(b)(1): Security Vulnerability Assessments under §27.215

§27.400(b)(2): Site Security Plans under §27.225

§27.400(b)(3): Documents relating to the Department's review and approval of Security Vulnerability Assessments and Site Security Plans, including Letters of Authorization, Letters of Approval, and responses thereto; written notices; and other documents developed pursuant to §§27.240 or 27.245

§27.400(b)(4): Alternative Security Programs under §27.235

§27.400(b)(5): Documents relating to inspections or audits under §27.250

§27.400(b)(6): Any records required to be created or retained by a covered facility under §27.255[2]

§27.400(b)(7): Sensitive portions of orders, notices or letters under §27.300

§27.400(b)(8): Information developed pursuant to §§27.200 or 27.205 (such as the CSAT Top Screen and the determination by the Assistant Secretary that a chemical facility presents a high level of security risk)

§27.400(b)(9): Other information developed for chemical facility security purposes that the Secretary, in his discretion, determines is similar to the information protected in §27.400(b)(1) through (8)

Facilities shall designate information about the facility that is specified in 6 CFR § 27.400(b)(1)-(8) as CVI. The process for a facility to seek designation of CVI under § 27.400(b)(9) is described in Chapter 5.3.

[2] See Chapter 5.2

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

5.2 Information Not Considered CVI

Section 550 states that its requirements "shall not be construed to supersede, amend, alter, or affect any Federal law that regulates the manufacture, distribution in commerce, use, sale, other treatment, or disposal of chemical substances or mixtures." Sec. 550(f), Pub. L. No. 109-295. In other words, Section 550 not interfere with any statutory, regulatory, or other obligations a facility may have to any other Federal agency. This principle is reflected in the CFATS regulation at § 27.405(a)(1), and in the preamble to that regulation at 72 FR 17688, 17714 (April 9, 2007).

Thus, information that a facility develops in accordance with other statutory or regulatory obligations, or information that pre-dates DHS regulation under Section 550, is *not* CVI.

Other statutory or regulatory information: Information that a facility developed or develops under regulatory regimes unrelated to a Section 550 and CFATS is *not* CVI. This is so even if this information is later incorporated into a separate document relating to compliance with Section 550 and CFATS, making the latter document CVI.

Pre-existing information: Other than the Top Screen (which is considered CVI under 6 CFR § 27.400(b)(8)), documents that a facility created prior to DHS determining the facility to be "high risk" under CFATS - i.e., documents not developed or submitted pursuant to Section 550(c) or the CFATS regulation - are *not* CVI. In other words, the CVI requirements are not retroactive, and a facility need not go back through its pre-existing files to mark already existing documents.

A specific question has been raised about the status of records (e.g., a logbook, computer, or system) that CFATS requires facilities to create or retain under 6 CFR § 27.255, and which a facility may historically have created for business reasons unrelated to CFATS. (This could include, for example, records related to training and to maintenance, calibration and testing of security equipment, as described in §§ 27.255(a)(1) and 27.255(a)(4), respectively.) As stated above, *pre-existing* records that a facility developed for its own business purposes prior to DHS determining the facility to be high risk are not CVI. However, any such records that a facility updates or creates *after* DHS determines the facility to be high risk are subject to the CVI requirements.

Examples:

(a) Information developed in accordance with other statutory or regulatory obligations:
The Department of Commerce administers the Chemical Weapons Convention Implementation Act (22 U.S.C. 6701, et seq.) through its Chemical Weapons Convention Regulations (15 CFR§§ 710-721). That Act and its implementing regulations require chemical facilities to supply information to foreign officials from the Organization for the Prohibition of Chemical Weapons (OPCW) to comply with the requirements of the Chemical Weapons Convention (CWC). This information is supplied to foreign officials at the OPCW through submission of declarations to the U.S Government that are then provided to the OPCW. This information is also supplied directly, as requested, to OPCW inspectors during CWC inspections in the

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

United States. Information submitted by chemical facilities complying with these obligations would not be CVI, even if the information is also incorporated in a separate CVI document.

(b) Information, not listed in 6 CFR § 27.255, that a facility developed for its own business purposes: If a facility possesses an inventory control document indicating the possession of certain quantities of a chemical that is also a chemical of interest under CFATS, that inventory control document and the information in it would not itself be considered CVI even if the information in the inventory control document is later incorporated in a document (e.g. a Top Screen or Security Vulnerability Assessment) that would itself be CVI and subject to all CVI protections..

5.3 Request for Determination of CVI

If a facility develops information that could, in the facility's judgment, compromise facility security if publicly disclosed, and that information is not listed as CVI under 6 CFR § 27.400(b)(1)-(8), the facility may request a CVI designation from DHS under 6 CFR § 27.400(b)(9). The facility should send the information in question to DHS marked as CVI. Until DHS makes a final determination, DHS and the facility will handle and protect the information as though it is CVI.

DHS will communicate its final determination to the appropriate individual at the requesting facility. DHS will maintain a record of each request for CVI designation, including the date, subject or title of the request, and a synopsis of the information.

Other Federal, state, and local government agencies do not have the authority to designate as CVI information independently obtained from chemical facilities under other regulatory programs.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

6.0 Need to Know

Access to CVI requires that an individual: (1) has a "need to know" the information; and (2) is an Authorized User. Under 6 CFR § 27.400(e), a person (including a State, local, or tribal official) has a need to know when:

- that person requires access to specific CVI to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by DHS,
- that person needs the CVI to receive training to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by DHS,
- that person needs the CVI to supervise or otherwise manage individuals carrying out chemical facility security activities approved, accepted, funded, recommended, or directed by the DHS,
- that person needs the CVI to provide technical or legal advice to a covered person, who has a need to know that CVI, regarding chemical facility security requirements of Federal law, or
- when DHS determines that access by that person to specific information is required under 6 CFR §§ 27.400(h) or (i) in the course of judicial or administrative proceedings.

In addition, as provided by 6 CFR §§ 27.400(e)(2), (4) and (5):

- A Federal employee has a need to know if access to the information is necessary for performance of the employee's official duties.
- A contractor acting in the performance of a contract with or grant from DHS has a need to know if access to the information is necessary to performance of the contract or grant.
- Notwithstanding the other provisions of the rules, DHS may determine that only specific persons or classes of persons have a need to know specific CVI.
- Nothing shall prevent DHS from determining, in its discretion, that a person or class of persons not otherwise listed above has a need to know CVI in a particular circumstance.

Any disputes between persons and facilities about whether an individual seeking access to the CVI has a need to know should be referred to DHS for resolution. In particular, any dispute between facilities and State, local or tribal officials about whether a given official has a need to know specific CVI should be referred to the DHS chemical facility security inspector responsible for working with the facility in question. *See* Chapter 7.2 below.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

7.0 Access to and Disclosure of CVI

Access to and/or disclosure of CVI is based on the following general principles:[3]

1. CVI may only be disclosed to Authorized Users with a need to know.

2. A need to know should be assessed on a case-by-case basis (including an individualized assessment of the documents involved).

3. A covered person in possession of CVI should take reasonable steps to confirm that any individual seeking access to CVI is an Authorized User and has a need to know.

7.1 Facilities Disclosing CVI within a Facility and among other Private Sector Entities

A facility may disclose CVI to any of the facility's board members, officers, and employees who are Authorized Users and have a need to know. Likewise, a facility may disclose CVI to any private sector third parties who are affiliated with the facility - e.g., outside attorneys, accountants, consultants, trade association employees - so long as they are Authorized Users with a need to know.

All covered persons must comply with the handling and safeguarding requirements for CVI outlined in 6 CFR § 27.400. They should be familiar with the guidance provided by this Manual and any other guidance DHS may provide in the future. And they should be aware that divulging information without proper authority could result in an administrative compliance order or civil penalties or other enforcement or corrective actions by DHS (e.g., revocation of CVI Authorized User status). *See* 6 CFR §§ 27.300(b)(3), 27.400(j).

Under 6 CFR § 27.400(d), covered persons must notify DHS of any unauthorized releases of CVI and refer to the Department any requests for access to CVI by persons without a need to know. In addition, chemical facilities and other entities or persons are encouraged to contact DHS about any actual or suspected misuse of or unauthorized access to CVI. Information about such actual or suspected incidents may be reported to

[3] As provided in Chapter 9.5 of this Manual, CVI may be disclosed without meeting all of the procedures or requirements described in this Chapter as necessary to meet exigent or emergency circumstances.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

the DHS chemical facility security inspector assigned to the area in which the incident occurred or to the CSAT Helpdesk at 866-323-2957 or CSAT@dhs.gov. *See* Chapter 10.0.

Notification and tracking of disclosures: Facilities do not need to notify DHS of proper disclosures of CVI (i.e., disclosures to Authorized Users with a need to know). Nonetheless, DHS encourages facilities to maintain a Tracking Log of the receipt and disclosure of all CVI. *See* Appendix D.

Chemical facilities should also consider the following:

1. Appointing a CVI Point of Contact (POC) to provide oversight and assistance to individuals within the facility;

2. Implementing procedures to ensure that CVI is used, handled, safeguarded and disclosed appropriately; and

3. Establishing a self-inspection program to include periodic review and assessment of the handling, use, and storage of CVI.

7.2 Facilities Disclosing CVI to State, Local, Tribal Agencies

Facilities may disclose CVI to officials in State, local, and tribal agencies (e.g., local county emergency managers and local police officials) who are Authorized Users and have a need to know.[4]
The determination that a State, local, or tribal official is an Authorized User and has a need to know will be made by the DHS chemical facility security inspector assigned by DHS to the area in which the facility is located. The DHS inspector will provide the public official with documentation of that determination. The facility may rely on this documentation.

Once the DHS inspector has made the determination that the public official is an Authorized User with a need to know CVI from a specific facility, the facility and public official should discuss: (1) which portions of CVI documents the official needs to execute his responsibilities; and (2) how the facility should disclose those documents (e.g., providing the official a copy of the document or arranging an on-site review). In the event of any disagreement between the facility and the public official regarding the precise CVI to be disclosed or the method of disclosure, DHS encourages the parties to refer the matter to the DHS chemical facility inspector for resolution.

All covered persons, including Federal, State, local and tribal government officials, must comply with the handling and safeguarding requirements for CVI outlined in 6 CFR § 27.400. They should be familiar with

[4] With the exception of State Homeland Security Advisors (HSAs), DHS encourages State and other non-federal public officials seeking access to specific CVI to obtain the CVI from the facility and not from other government agencies. DHS expects that State HSAs typically will request and obtain relevant CVI directly from DHS. *See* Chapter 7.3.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

the guidance provided by this Manual and any other guidance DHS may provide in the future. And they should be aware that unauthorized disclosure of CVI could result in an administrative compliance order or civil penalties or other enforcement or corrective actions by DHS. 6 CFR §§ 27.300(b)(3) and 27.400(j).

Under 6 CFR § 27.400(d), covered persons also must notify DHS of any unauthorized releases of CVI and refer to the Department any requests for access to CVI by persons without a need to know. In addition, State, local and tribal agencies are encouraged to notify DHS of any suspected or actual misuse of CVI and of any suspicious or inappropriate attempts to gain access to CVI. Information about actual or suspected incidents may be reported to the DHS chemical facility security inspector assigned to the area in which the incident occurred or to the CSAT Helpdesk at 866-323-2957 or CSAT@dhs.gov. *See* Chapter 10.0.

Notification and tracking of disclosures: When a facility properly discloses CVI to a public official, the facility does not need to notify DHS of the disclosure. DHS encourages both the public official or agency to maintain a CVI Tracking Log. *See* Appendix D.

All government agencies should also consider:

1. Appointing a CVI Point of Contact (POC) to provide oversight and assistance to individuals within the agency;

2. Implementing procedures to ensure that CVI is used, handled, safeguarded and disclosed appropriately; and

3. Establishing a self-inspection program to include periodic review and assessment of the handling, use, and storage of CVI.

NOTE: State, local, and tribal officials, including first responders, must have access to any information that is necessary to plan for and respond to an emergency event at a chemical facility. It is equally important that this information is available in a form that is readily accessible and easily disseminated. Accordingly, to the extent possible, facilities should provide information to State, local and tribal entities in non-CVI form. In many cases, a facility can provide a product that contains all of the necessary operational and facility-specific information and excludes CVI.

Furthermore, where non-CVI documents are not sufficient, DHS encourages facilities and public officials to cooperate to limit the scope of CVI shared to that which State, local and tribal officials need to accomplish their mission. This may include sharing only a portion of a CVI document and redacting or deleting the rest. For example, DHS expects that State, local, and tribal officials ordinarily will need to see or obtain access only to portions of a Security Vulnerability Assessment or Site Security Plan, rather than the entire document.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

7.3 Access to CVI by State Homeland Security Advisors and Non-DHS Federal Agencies

State Homeland Security Advisors (HSAs)

DHS expects that State HSAs will request CVI about facilities within their jurisdiction and adjoining counties directly from DHS. The Department will provide CVI to HSAs (or designees in the HSAs' immediate offices) provided they are Authorized Users and have a need to know. DHS believes that, in light of their homeland security mission, HSAs have a need to know CVI related to covered facilities within their jurisdiction and adjoining counties in adjacent States. This need to know is limited, however, to CVI relating to facilities that DHS determines are "high risk" and thus covered under Section 550. Thus, for example, HSAs typically will not have a need to know Top-Screen information relating to facilities that DHS determines are not high risk. In addition, because State officials other than HSAs do not necessarily have a need to know CVI for every high-risk facility in their State, all State officials (other than HSAs) should seek CVI in the manner described in Chapter 7.2 above, rather than from HSAs. DHS will determine the need to know for those State officials on a case-by-case basis.

Non-DHS Federal Agencies

DHS encourages other Federal agencies to seek CVI directly from DHS, as opposed to individual facilities, so that DHS can determine whether the requesting individual is an Authorized User and has a need to know the specific CVI requested. DHS is coordinating with other relevant Federal agencies to reach agreement on what types, if any, of CVI they have a need to know in connection with their official duties. *See* 6 CFR § 27.400(e).

In the event that a non-DHS Federal agency or official approaches a facility directly for access to CVI, the facility should provide such access in accordance with the requirements of CFATS and the principles in Chapter 7.0 above. The facility should notify DHS of the disclosure after the fact.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

8.0 General Handling Procedures

Pursuant to Section 550(c) and 6 CFR § 27.400, CVI must be appropriately designated, withheld from public disclosure, and physically controlled and protected. Copies of CVI or derivative products are subject to the same protections as original CVI.

8.1 Storage

Section 27.400(d) requires that a covered person take reasonable steps to safeguard CVI in that person's possession. Consistent with that requirement:

- The workspace where CVI is stored typically should have controls to limit access (e.g., keys, key cards, badges, swipe cards) to prevent unauthorized access by members of the public, visitors, or other persons without a need to know. This may include a locked room or an area where access is controlled by a guard, cipher lock or card readers.

- When unattended, materials containing CVI must, at a minimum, be stored in a secure container. Examples of such containers may include a safe, locked file cabinet, locked desk drawer, locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment.

- When CVI is managed within an area authorized for open storage of classified material, it generally is not necessary to store CVI in a locked container. However, in accordance with 6 CFR § 27.400(f), such materials must have a CVI cover sheet to prevent unauthorized access and should be segregated from classified materials to the extent possible (i.e., separate folders, separate drawers, etc.).

Furthermore, IT systems or AIS used to handle, store, or transmit materials containing CVI should have operational and technical controls in place to ensure that only Authorized Users with a need to know can access such materials and to prevent loss or theft of CVI. The computer systems should provide appropriate markings and warnings for any displayed CVI, in accordance with 6 CFR § 27.400(f).

Consistent with 6 CFR § 27.400(d), computers and other media used to handle, store, or transmit materials containing CVI should be stored and protected to prevent unauthorized access and unauthorized disclosure. Storage and control of DHS or DHS contractor/consultant computers and other media containing CVI will

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

8.2 Marking Materials Containing CVI

Pursuant to Section 550 and 6 CFR § 27.400(f), CVI must be marked so that individuals are aware of its sensitivity and protection requirements. Regardless of form (e.g. written, verbal, electronic, or digital), all CVI - including any copies or materials derived from CVI - must be marked appropriately.

For paper records containing CVI, as required by 6 CFR § 27.400(f), place the below protective marking on the top of the document and the distribution limitation statement on the bottom of: (1) the outside of any front and back cover, including a binder cover or folder; (2) any title page; and (3) each page of the document.

The protective marking is: **Chemical–terrorism Vulnerability Information.**

The distribution limitation statement is:

> **WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 CFR 27.400. Do not disclose to persons without a "need to know" in accordance with 6 CFR § 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR §§ 27.400(h) and (i).**

In accordance with 6 CFR § 27.400(f)(4), in the case of non-paper records that contain CVI, including motion picture films, videotape recordings, audio recordings, and electronic and magnetic records, a covered person must mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

Consistent with 6 CFR § 27.400(f)(4) and (d)(1), CVI contained on electronic and magnetic media should have the protective marking and distribution limitation statement applied to the beginning and end of the electronic and magnetic text. The protective marking and distribution limitation statement should be displayed in such a manner that both are fully visible on the screen or monitor when the text is viewed.

Electronic CVI should have an electronic watermark or banner stating that CVI is being displayed.

All electronic storage devices (e.g., external hard drives or thumb drives) that contain CVI should be marked with the protective marking. The protective marking and distribution limitation statement should also be applied to each side of the disk and the disk sleeve/jacket, on the non-optical side of the CD-ROM and both sides of the CD-ROM case. If the electronic/magnetic text has a soundtrack, audible warnings that describe the protective marking and distribution limitation statement should, if possible, be included in the introduction and at the end of this text.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

As provided in 6 CFR § 27.400(d)(6), if any covered person receives a record or verbal transmission containing CVI that is not marked as required, this person must:

- Mark the record as specified in § 27.400(f);
- Inform the sender of the record that the record must be marked as specified in § 27.400(f); and
- For verbal transmissions, make reasonable efforts to memorialize the information and inform the speaker that the information warrants CVI protection.

If CVI or material containing CVI cannot be marked directly, the cases or containers in which CVI is stored (e.g., CD cases) should include the protective marking and distribution limitation statement.

Consistent with 6 CFR § 27.400(f), when CVI is removed from an authorized storage location (see Chapter 9.1) within the workplace and persons without a need to know are present, or where casual observation would reveal materials containing CVI, a cover sheet (see 6 CFR § 27.400(f) and Appendix C to this Manual) should be used to prevent unauthorized or inadvertent disclosure. When transmitting CVI, an appropriate cover sheet must be placed on the front and back of the transmittal letter, report, or document.

NOTE: DHS, along with all Executive Branch agencies, is currently evaluating the potential impact of the President's May 9, 2008 memorandum to the heads of all Executive Departments and Agencies entitled "Designation and Sharing of Controlled Unclassified Information (CUI)." The memorandum directed federal agencies to adoption CUI as the "single, categorical designation henceforth throughout the executive branch for . . . most information heretofore referred to as 'Sensitive But Unclassified' (SBU)."

The presidential memorandum expressly exempts CVI; that is, the CVI program and CVI designation will continue to exist. It is conceivable that certain markings, safeguarding requirements, and disclosure limitations for CVI may be revised in the future, however, in light of the President's memorandum. In that event, the CVI Procedural Manual would be updated appropriately.

8.3 Transmission of Hard Copy Materials

8.3.1 Postal Service or Commercial Carriers

Consistent with 6 CFR §§ 27.400(d) and 27.400(f), the United States Postal Service and commercial carriers may be used to transport CVI. For U.S. Postal Service, a return receipt or other tracking process should be used. Commercial delivery services should provide a tracking mechanism that documents the departure and receipt of the package.

In addition, CVI should have an appropriate inner cover or envelope and it should be placed in an opaque, unmarked, envelope. The CVI cover page may serve as the inner envelope. The outer envelope should bear the complete name and address of the intended recipient, who must be an Authorized User with a need to know. The envelope should include a notation that if the intended recipient is not at the specified address,

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

the package shall not be forwarded to another address and must be returned to the sender. The outer envelope should not identify the contents as CVI.

8.3.2 Inter-Office Mail

Consistent with 6 CFR § 27.400(f), materials containing CVI may be transferred in an inter-office mail system so long as the measures set forth in above in Chapter 8.3.1 are followed.

8.4 CVI in Transit or Use at a Temporary Duty Station

Consistent with 6 CFR § 27.400(d), CVI must be safeguarded when in transit or in use at a temporary duty station. The following are examples of appropriate safeguards. CVI should:

1. Remain under the control of the authorized person at all times (e.g., not placed in checked baggage).
2. Be placed in an opaque envelope and sealed; CVI should not be viewed or displayed where people without a need to know may view the information.
3. Be locked in the trunk when traveling by car and when the authorized person is away from the vehicle.
4. Be locked in a hotel room safe, if possible. Otherwise, remain secure in a locked briefcase or suitcase within a locked room, for example.

8.5 Electronic Transmission

8.5.1 Transmittal by Facsimile (Fax)

CVI may be sent via non-secure fax, although use of a secure fax machine is highly encouraged. Consistent with 6 CFR §§ 27.400(d)-(e), when a non-secure fax is used, the sender should:

1. Confirm that the person receiving the CVI at the other end is an Authorized User with a need to know.
2. Coordinate with the recipient to ensure the facsimile number of the recipient is current and valid.
3. Contact the recipient to ensure that the materials faxed will not be left unattended.
4. Use a cover sheet for the transmitted information that clearly identifies the sender's name and telephone number and contains a warning that if the message is received by other than the intended recipient, the individual receiving the message should immediately notify the sender for disposition instructions.
5. Ensure that the CVI is properly marked in accordance with 6 CFR § 27.400(f) and Appendix C.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

8.5.2 Transmittal via E-Mail

CVI may be transmitted by e-mail, provided that transmission is consistent with 6 CFR §§ 27.400(d)-(e). The following are examples of steps that if taken would be consistent with the regulations:

1. CVI transmitted via e-mail should be protected by encryption or transmitted within secure communications systems. Where this is impractical or unavailable, CVI may be transmitted over non-secured e-mail accounts as a properly marked, encrypted attachment (e.g., PKZip or WINZip) or as a properly marked, password-protected attachment with the password provided in a separate e-mail. CVI should never be included in the subject or body of an e-mail transmission.
2. Due to inherent vulnerabilities, materials containing CVI should not be sent to personal e-mail accounts such as Hotmail or Gmail.

8.6 Telephone and Other Verbal Communications

When discussing CVI over a telephone, the following are examples of precautions that may be taken to comply with 6 CFR §§ 27.400(d)-(e):

1. The use of a Secure Telephone Unit (STU III) or Secure Telephone Equipment (STE).
2. Because the risk of interception and monitoring of conversations is greater when using cellular telephones and cordless telephones, avoid use of these devices unless the circumstances are exigent or the transmissions are encoded or otherwise protected.

In any case, the caller must take reasonable steps to ensure that the person to whom they are communicating the CVI is an Authorized User with a need to know.

More generally, when communicating CVI verbally:

1. The individual providing the information should inform the receiving individual that the information is designated as CVI and subject to protection.
2. Any record that may result from such a verbal conversation that contains CVI should be marked CVI in accordance with 6 CFR §§ 27.400(d)(6) and 27.400(f).

8.7 Destruction

Materials containing CVI must be destroyed when no longer needed, except as provided in 6 CFR § 27.400(k). Acceptable methods of destruction include the following:

1. "Hard Copy" materials should be destroyed by crosscut shredding, burning, pulping, or pulverizing to assure destruction beyond recognition and reconstruction.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

2. Electronic storage media should be sanitized appropriately by overwriting or degaussing. (Contact local IT security personnel for assistance if needed.)

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

9.0 Policy and Procedures

9.1 CVI Derivative Products

CVI Authorized Users may develop analytical products that are derived from CVI. Derivative products are subject to the same handling, storage, and marking requirements as the original CVI.

Wherever CVI is paraphrased in an analytical product and the paraphrased information could reveal the source of the submission (e.g., naming the particular facility name or asset) and information related to a facility's security vulnerabilities (e.g., the facility's risk based tier level or identifying a critical infrastructure/asset), that product should be handled as CVI.

9.2 CVI and Classified Products

Derivative products containing CVI may become classified because of the sensitivity of the resulting analysis or other information included in the document. Classification of such products must meet the standards and criteria set forth in Executive Order 12958, *Classified National Security Information* (as amended), and the requirements established in the *Security Classification Guide for Information Collected Pursuant to Section 550 of Public Law 109-295*, DHS SCG PREP – 003, February 2007.

In addition, as provided by Section 550(c) of Public Law 109-295, any CVI used in any enforcement proceeding under CFATS must be treated as classified information.

CVI contained in classified documents retains its CVI marking and does not lose its CVI protection even if the document is subsequently declassified. CVI commingled with classified information must comply with all marking requirements of both CVI and the highest level of classification with which it is commingled, as prescribed in Executive Order 12958 (as amended) and its implementing directives. The CVI markings should be placed below the classified marking at the top of the page and above the classified markings at the bottom of the page. Each paragraph in a classified document containing CVI should be so marked.

9.3 DHS Advisories, Alerts, and Warnings

If DHS uses CVI to prepare advisories, alerts, and warnings regarding potential threats and vulnerabilities to critical infrastructure for disclosure to the private sector, the general public, or foreign governments, such information will be sanitized. For the purposes of the CVI program, "sanitization" means distilling the information in a manner that it does not reveal any information that:

- Exposes vulnerabilities of identifiable critical infrastructure or protected systems;

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

- Is proprietary, business-sensitive, or trade secret;
- Relates specifically to the submitting person or entity (explicitly or implicitly).

When appropriate and necessary, DHS will consult with the submitting entity (or an authorized person on behalf of the submitting entity) to ensure that the advisory, alert, or warning does not contain proprietary, business sensitive, or trade secret information.

9.4 Open Sources

If an Authorized User possesses information from an open source that is coincidentally the same as information that has been designated as CVI, the Authorized User may use the open source information in any work product without identifying it as CVI.

9.5 Emergency or Exigent Circumstances

Notwithstanding other provisions of this Manual, in the event a facility determines that emergency or exigent circumstances (see definition in Chapter 4.0 above) exist, it may disclose or provide access to CVI, as necessary, without first meeting the procedures of this section. A record of the disclosure or access should be kept and submitted to the DHS chemical facility security inspector assigned to the area in which the incident occurred or to the CSAT Helpdesk at 866-323-2957 or CSAT@dhs.gov as soon as is practicable.[5] The record typically should include:

- Date CVI was shared;
- Who received the CVI;
- Contact information for the recipient;
- How CVI was provided to the recipient;
- Reason for emergency or exigent access/disclosure; and
- Justification on need to know.

9.6 Adjudications, Appeals and Administrative or Civil/Criminal Judicial Proceedings

Any requests for CVI for use in administrative adjudications or appeals or in civil or criminal judicial proceedings, *see* 6 CFR § 27.400(i), will be coordinated through the DHS Office of the General Counsel.

[5] As provided by 6 CFR § 27.400(e)(5), DHS has determined that a need to know CVI exists under the emergency or exigent circumstances described in this Manual.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

9.7 Freedom of Information Act (FOIA) and Related Requests

Notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, in accordance with Sec. 550(c) and 6 CFR § 27.400(g), records containing CVI are not available for public inspection or copying, nor does the Department release such records to persons without a need to know.

Further, as provided in 6 CFR § 27.405, no law, regulation, or administrative action of a State or political subdivision thereof, shall have any effect if such law or regulation conflicts with the purposes of this regulation. Requests for CVI under State or local freedom of information or open records laws should be referred to the DHS National Protection and Programs Directorate Disclosure Office. The DHS Office of the General Counsel will consider recommending U.S. Government intervention in litigation relating to the disclosure of CVI on a case-by-case basis.

If a record contains both information that may not be disclosed under Section 550(c) of Public Law 109-295 and information that may be disclosed, the latter information may be provided in response to a FOIA request, provided that the record is not otherwise exempt from disclosure under FOIA and that it is practical to redact the protected CVI from the requested record.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

10.0 Incident Reporting for Potential CVI Violations

When a covered person becomes aware that a person without a need to know has requested CVI or that CVI has been released to a person without a need to know, the covered person must promptly report the incident to the DHS Assistant Secretary for Infrastructure Protection. *See* 6 CFR §§ 27.400(d)(3),(7). Such notifications should be sent to the Assistant Secretary via the CSAT Helpdesk or through the DHS chemical facility inspector assigned to the facility or region in which the incident occurred. In addition, any other loss, compromise or suspected compromise, or unauthorized disclosure of materials containing CVI should be promptly reported to the DHS chemical facility security inspector assigned to the area in which the incident occurred or to the CSAT Helpdesk at 866-323-2957 or CSAT@dhs.gov.

The notification or report should include the date of potential inappropriate CVI request or disclosure and any other relevant facts.

The notification of loss, compromise, suspected compromise, or unauthorized disclosure of materials is not CVI unless the notification itself contains specific CVI.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

Appendix A: Background Checks for CVI

Under 6 CFR § 27.400(e)(3),the Department of Homeland Security may make an individual's access to CVI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding CVI that are satisfactory to the Department. Although no such requirement is in place currently, this appendix is reserved for future guidance on the topic.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under OMB's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

Appendix B: Option to Confirm an Individual is a CVI Authorized User

One method of verifying that an individual requesting CVI is an Authorized User with a need to know is to contact the CSAT Helpdesk. The CSAT Helpdesk can verify if an individual is a CVI Authorized User. The CSAT Helpdesk may be reached at 866-323-2957 Monday through Friday from 7am to 7pm (ET). The CSAT Helpdesk is closed on Federal holidays.

The Helpdesk will ask for the name of the individual, his/her CVI Authorized User number, or other unique personally identifiable information. The CSAT Helpdesk will then confirm whether or not that the individual is a registered CVI Authorized User.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

Appendix C: Front and Back Cover for Material Containing CVI

In accordance with 6 CFR § 27.400(f), the following page format will be used for both the front and back cover of any material containing CVI.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION
Requirements for Use

WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 CFR 27.400. Do not disclose to persons without a "need to know" in accordance with 6 CFR § 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR § 27.400(h) and (i).

By reviewing this cover sheet and accepting the attached CVI you are agreeing to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached CVI.

Access

This information may not be further disclosed except to individuals who meet the following requirements:

- All individuals must be CVI Authorized Users
- All individuals must demonstrate a valid need to know for specific CVI

Handling

Storage:	When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended**.
Transmission:	You may transmit CVI by the following means to a CVI Authorized User with a need to know.
Hand Delivery:	CVI may be hand carried as long as access to the material is controlled while in transit.
Email:	Encryption should be used. If encryption is not available, send CVI as an encrypted attachment or password protected attachment and provide the password under separate cover. Whenever the recipient forwards or disseminates CVI via email, place that information in an attachment. **Do not send CVI to personal, non-employment related email accounts.**
Mail:	USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as CVI. Envelope or container must bear the complete name and address of the sender and addressee. The envelope must bear the following statement below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**."
Fax:	Secure faxes are encouraged, but not required. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.
Telephone:	Secure Telephone Unit/Equipment are encouraged, but not required. Use cellular or cordless phones to discuss CVI only in exigent circumstances. Do not engage in a conversation in a public place or in environments that will allow anyone that does not have a need to know to overhear the conversation.
Reproduction:	Ensure that a copy of this sheet is the first and last page of all reproductions containing CVI. Clear copy machine malfunctions and ensure all paper paths are checked for CVI. Destroy all unusable pages immediately.
Destruction:	Destroy (i.e., shred or burn) this CVI document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use a CVI document to create a product that is released to the public such as an advisory, alert or warning. In this case, the product must not reveal any information that:

- Exposes vulnerabilities of identifiable critical infrastructure or protected systems of a facility;
- Is proprietary, business-sensitive, or trade secret;
- Relates specifically to the submitting person or entity (explicitly or implicitly).

Derivative Products

Mark any newly created document containing CVI with "CHEMICAL-TERRORISM VULNERABILITY INFORMATION" on the top of each page that contains CVI and the distribution limitation statement at 6 CFR § 27.400(f)(3) on the bottom.

Place a copy of this cover page over all documents containing CVI.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.

Appendix D: Example of CVI Tracking Log Contents

Covered persons (including facilities and government agencies) do not need to notify DHS of proper disclosures of CVI (i.e., disclosures to Authorized Users with a need to know). Nonetheless, DHS encourages facilities, government agencies and other covered persons to maintain a Tracking Log of the receipt and disclosure of all CVI.

A Tracking Log which merely reflects the receipt and subsequent dissemination of CVI, and does not itself contain any CVI, is not a CVI document.

A CVI Tracking Log typically would include:

- Date CVI was initially received by the covered person;
- Description of the nature of CVI (e.g., Top-Screen);
- Date(s) CVI was further disseminated by the covered person, if applicable;
- Who received the CVI from the covered person;
- Contact information for the recipient;
- How CVI was sent to the recipient.

This Manual is a guidance document and complies with the applicable procedures for federal agency guidance under the Office of Management & Budget's "Final Bulletin for Agency Good Guidance Practices." This document does not create or confer any new rights or obligations on any person or entity or otherwise operate to bind the public. Any terms of prohibition or command used in this document are derived from Sec. 550 of Pub. L. 109-295 or 6 CFR Part 27.