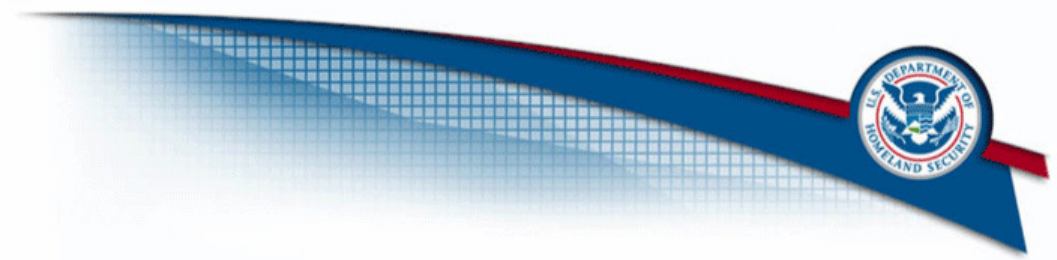




Welcome To
Chemical-Terrorism Vulnerability Information **CVI**
Authorized User Training

[Click Here To Launch Training](#)



CVI Authorized User Training

- [Introduction](#)
- [What information qualifies as CVI](#)
- [Access to CVI](#)
- [Products Derived from CVI](#)
- [Handling CVI](#)
- [Summary](#)
- [Knowledge Assessment](#)



Chemical-Terrorism Vulnerability Information CVI

AUTHORIZED USER TRAINING

GLOSSARY

RESOURCES

HELP

BACK

NEXT

Chemical-Terrorism Vulnerability Information Authorized User Training

Page 1 of 26



Chemical-Terrorism Vulnerability Information Authorized User Training



Introduction

Getting Started

Page 2 of 26

This training provides an overview a Sensitive But Unclassified designation titled "Chemical-Terrorism Vulnerability Information (CVI). CVI is used to protect information that describes the nation's vulnerabilities to terrorist attacks on facilities manufacturing, using, or storing explosive, reactive, or toxic chemicals. This training will describe the details for safeguarding and handling CVI. Successful completion of this training will prepare you to successfully participate in the Chemical Security Program.

Completion of this training is a necessary first step for all individuals who access CVI.

This training will take approximately 20 – 35 minutes to complete.

Upon successful completion of the training, your name will be added to the database of authorized users.

This training does not make any determination on your need to know CVI. The holder of CVI will make this decision each time a request is made.

Introduction

Purpose

At the end of the training, you will be able to answer the following questions:

What is the legislative foundation of the Chemical Security Program?

What information qualifies as CVI?

Who is authorized to access CVI?

What are the procedures for safeguarding CVI?

What are the consequences of mishandling CVI?



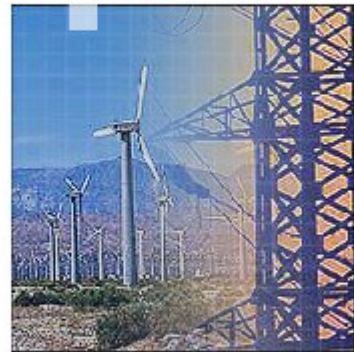
Introduction

Critical Infrastructure

Page 4 of 26

The Department of Homeland Security has the responsibility for protecting the nation's critical infrastructure. Critical infrastructure includes our transportation systems, telecommunications, and our public health systems among others. Critical infrastructure also includes our chemical manufacturing industry. Chemical Manufacture and use is one of 17 critical infrastructure of key resource sectors identified by DHS. DHS recognizes that chemical plants could be targets for terrorists seeking to inflict damage local populations or disrupt our nation's economy. The theft of certain chemicals could help terrorists create explosives or chemical weapons of mass destruction. DHS wants to ensure that all chemical facilities that meet certain criteria meet minimum standards for safety and physical security.

DHS and its partners across Federal, state, and local governments need information about chemical facilities in order to protect the nation from terrorist attacks, assist in the identification of vulnerabilities, and aid in the response when an attack or natural disaster occurs.



Introduction

Page 5 of 26

Legislative Authority for Chemical Facility Anti-Terrorism Standards

On September 8, 2006, the Secretary for the Department of Homeland Security requested that Congress provide the department with regulatory authority to establish and require implementation of risk-based performance standards for the security of our nation's high-risk chemical facilities.

Congress took action on this request, and on October 4, 2006, the President signed into law the Appropriations Act of 2007 which provides the Department with the authority to regulate the security of high-risk chemical facilities. See Public Law 109-295, Section 550 as a reference.

On April 9, 2007, the interim final rule, 6 CFR Part 27, was published in the Federal Register. Subpart D of the rule establishes the standards and requirements that covered persons must follow to comply with CVI safeguarding requirements.

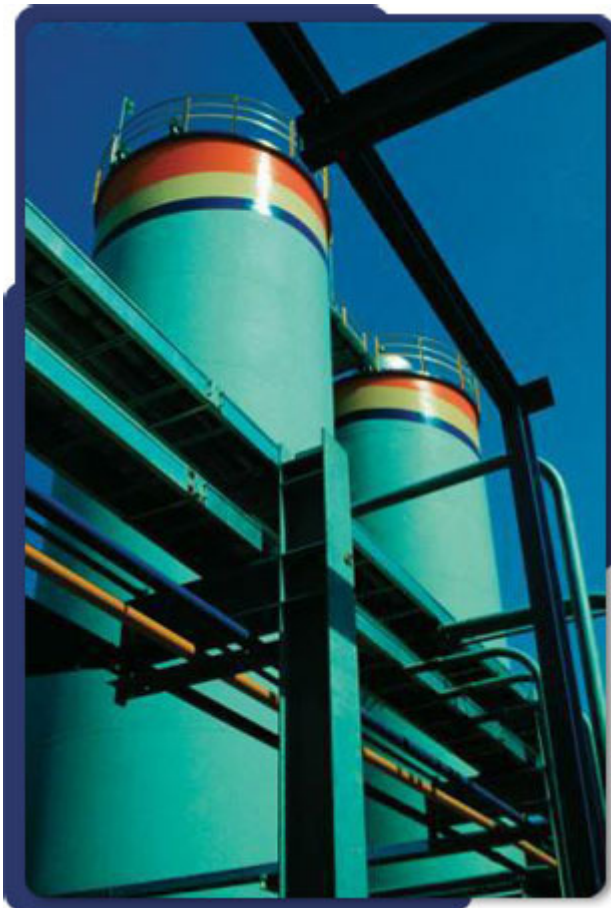
Introduction

Assurance for Protection

Chemical facilities must know that the information they share will be properly protected. Information designated as CVI will be exempt from public disclosure under Federal, state, and local laws.

As someone who may use CVI, you must understand that the public release of this information may compromise the security of these facilities or provide competitors with an advantage they would otherwise not have.

Chemical facilities must also understand that sharing this information with people that do not have a need to know has the opportunity to compromise homeland security. Making an informed decision on who has a need to know is a good practice to assure that CVI is only held and used by responsible authorities.



What information qualifies as CVI?

CVI Definition

6 CFR Part 27 identifies the following information as qualifying for CVI designation.

Top Screen from Chemical Self Assessment Tool (CSAT)

Initial determination by Assistant Secretary that a chemical facility presents a high level of security risk

Request for re-determination

Objection to an initial determination

Final determination on security risk

Security Vulnerability Assessment (SVA)

Alternative Security Plan

Site Security Plan (SSP)

Notice of Placement in a Risk Tier

Letter approving SVA

Notice of Deficiency for SVA

Letter of Authorization for SSP

Letter of Approval for SSP

Notice of Deficiency for SSP

Inspection Findings/Correspondence

Training Records

Exercise and Drill Records

Incidents and breaches of security

Maintenance, calibration, and testing of security equipment

Security Threats

Audit Records

Sensitive correspondence between regulated facility and DHS

Order of Compliance as describes actions for coming into compliance

Responses to Compliance Orders

Objections

Appeals

Any other information the Secretary believes is pertinent to chemical facility anti-terrorism standards

As an authorized user, it is your responsibility to safeguard this information at all times.

The submitter must also indicate whether or not the information is required to be submitted to a non-DHS Federal Agency, and if so, the submitter must specify the agency and the law or regulation requiring the information.

Information that falls into any one of these categories may be designated as CVI by either the chemical facility or the Department.

Chemical Terrorism Vulnerability Information

Chemical Security Assessment Tool
Top Screen

Facility Name:

Physical Location

Primary Contact

Chemicals stored on site:

Average daily volume stored: (gal)

Chemicals manufactured on site:

Security Plan Developed (Y/N)

Chemical Terrorism Vulnerability Information

What are the sources for CVI?

Page 8 of 26

Activities Associated with Chemical Security

The previous slide provided a list of items that qualify as CVI. Some of these items may be produced by the chemical facility while others are the product of DHS actions

Chemical facilities are required to complete a Chemical Security Assessment available at [CSAT](#). The information provided to the Chemical Security Assessment Tool will create a report that DHS will use for determining the risk profile for the facility. This report and any correspondence qualify as CVI. Remember that only those portions of letters that refer to CVI are protected from public disclosure.

Chemical facilities that qualify as high risk facilities will be the first to submit site security plans. These and any correspondence qualify as CVI

Chemical facilities may also create CVI as part of their on-going security activities including audits, equipment tests, and monitoring.

DHS will send inspectors to chemical facilities to ensure that the stated site security plans are being implemented as stated. The inspection reports and any subsequent correspondence regarding the inspection may be designated as CVI.



Access to CVI

Using and Sharing CVI

When using CVI, you are responsible for protecting the information and any CVI derivative products from unauthorized disclosure.

CVI and derivative products cannot be shared with unauthorized users.

In general, an authorized user must:

- For government employees and contractors outside the Department of Homeland Security, CSCD will not grant access to CVI until that person's organization has entered into a Memorandum of Agreement with CSCD.

- Be engaged in homeland security duties

- Have a need to know for that specific information as determined by the holder of the information

- Complete CVI Authorized User Training

- Have signed a Non Disclosure Agreement (NDA), if a non-Federal employee

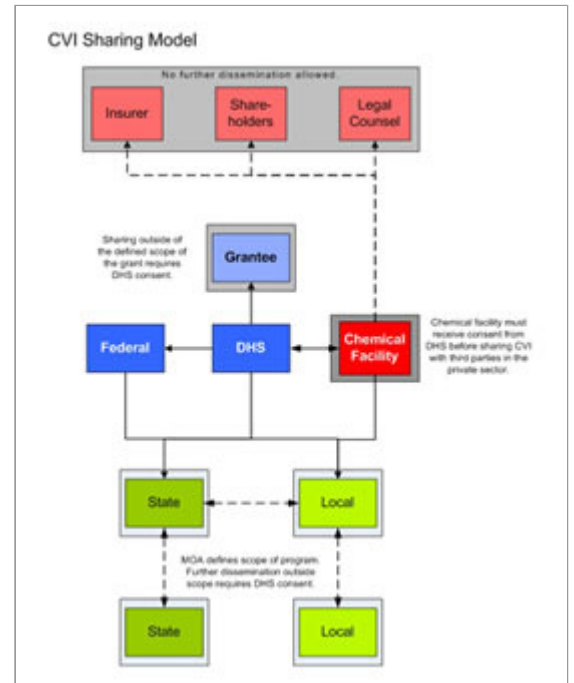
- Contractors must whenever and to whatever extent possible, amend their contract to include a CVI-specific special condition.

- Completed a background check if required by the Director of the Chemical Security Compliance Division (CSCD).

CSCD will maintain a list of authorized users. If you are unsure whether a person is authorized to receive CVI, please contact the CSCD Help Desk. A customer service representative can confirm if a person is authorized to receive CVI. The determination whether the requesting person has a need to know is different for each stakeholder group. Federal employees may determine need to know for any authorized user. State and local officials must receive the consent of the state CVI Security Officer before sharing. Chemical facility employees with seek the consent of their CVI Point of Contact.

Chemical facilities holding CVI may not share this information outside their corporate structure without the written consent of the CSCD Director. Anyone granted access must sign a non-disclosure agreement substantially similar to the one non-Federal employees sign. These third party recipients may not disseminate this information any further.

The recipient of CVI must destroy this information when no longer needed.



[CLICK GRAPHIC TO ENLARGE](#)

AUTHORIZED USER TRAINING

GLOSSARY

RESOURCES

HELP

Access to CVI

Marking Information as CVI

Page 10 of 26

Authorized users are responsible for applying the appropriate markings to CVI.

The CVI Cover Sheet must be affixed to the front and back covers of any document containing CVI and must remain with the document permanently. If the information is presented electronically, this information shall be displayed prior to an individual accessing the information.

When CVI is included in a classified product, the CVI Cover Sheet is placed immediately behind the classified Cover Sheet.

Anyone creating new CVI must include a tracking number with the information. Any derivative materials will refer to the tracking number associated with the source material. The numbering convention used for tracking numbers is available in the CVI Procedures Manual.

All CVI shall include at the beginning of the document a distribution limit statement as follows, "WARNING: This record contains Chemical-terrorism Vulnerability Information that is controlled under 6 CFR 27.400. No part of this record may be disclosed to persons without a 'need to know,' as defined in 6 CFR 27.400(e), except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For DHS, public disclosure is governed by 6 CFR 27.400(g).

All pages in a document designated as CVI shall have the words -

Chemical-terrorism Vulnerability Information

placed in the header and footer of each page.

Information stored electronically must demonstrate similar methods for identifying any shown information as CVI. These computer systems must also be able to limit access to only those individuals that have a need to know. Any electronic systems must either comply with Federal standards for storing Sensitive But Unclassified information or demonstrate a similar standard for protection.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION
Requirements for Use
Nondisclosure

This document contains Chemical-Terrorism Security and Vulnerability Information (CVI). In accordance with the Freedom of Information Act (5 U.S.C. 552), State or local disclosure rules and use in civil litigation proceedings. Unauthorized release may result in civil penalty, imprisonment or other action. Safeguard CVI from unauthorized disclosure.

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

In addition to agreeing to not further disclose this information, individuals seeking access to CVI must meet the following requirements:

- Be assigned to homeland security duties related to the critical infrastructure;
- Demonstrate a valid need-to-know.

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 an eligible individual who meets the access requirements listed above, or all cover, the recipient must accept the terms for Non-Disclosure Agreement before being given access to CVI. Hand delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit. Email: Exception should be used whenever, when this is impractical or unavailable you may transmit CVI over regular email channels, if acceptable to you, provide CVI as a password protected attachment and provide the password under separate cover. Do not send CVI to personal, non-employment related email accounts. Inform the recipient forwards or disseminates CVI via email, place that information in an attachment.

Marking: CVI must be clearly and prominently marked. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to allow evidence of tampering, and then placed in a second envelope that has no marking or is to identify the contents as CVI. Envelope or container must bear the complete name and address of the sender and address. Envelope will have no other markings that indicate the contents are CVI and must bear the following below the return address: **RESTRICTED - DO NOT REPRODUCE - DETAILS TO BE KEPT SECRET.** Allow for the aforementioned requirements for marking CVI.

Disposal: You are encouraged, but not required, to use a secure fax, 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: You are encouraged, but not required, to use a secure telephone line. Equipment: Use rubber gloves to discard CVI only in urgent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing CVI. Clear copy machine malfunction and ensure all paper parts are checked for CVI. Destroy all unusable pages immediately.

Disposition: Destroy (i.e. shred or burn) this document when no longer needed. Not laptops or CD/DVD, delete file and empty recycle bin.

Derivative Products

You may use CVI 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:

- is proprietary, business sensitive, or trade secret;
- relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- is otherwise not appropriate in the public domain.

Tracking Number

Mark any newly created document containing CVI with "Restricted Critical Infrastructure Information" on the top and bottom of each page that contains CVI. Mark "CVI" beside each paragraph containing CVI. Place a copy of this page over all newly created documents containing CVI. The CVI Tracking Number(s) of the source document(s) must be included on the derivatively created document in the form of an enclosure.

More information regarding creating derivative products is available at ...

Tracking Number

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

[CLICK GRAPHIC TO ENLARGE](#)

Access to CVI Storage Requirements

Page 11 of 26

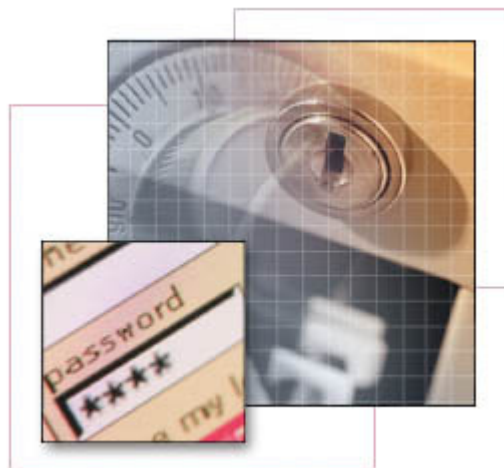
As a general rule, Hard copies of CVI should be placed in a locked storage device when not in use. This may include a safe, file cabinet, or desk drawer.

If you work in a classified open storage area and ALL members of the staff in that area are CVI authorized users, you may leave information on your desk unattended as long as the CVI Cover Sheet is placed over the information.

Users with workstations that include computers must use the screen locking and log-off features, or turn off his/her computer at the end of a work session.

Federal information systems storing CVI must comply with NIST Standard 4300A. State and local governments seeking to store CVI electronically must provide similar protections. This

requirement will be stated in the Memorandum of Agreement that must be signed before access to CVI is provided. Anyone seeking to store CVI electronically is encouraged to contact the Chemical Security Help Desk to learn more about IT system requirements.



Access to CVI Transmitting CVI

Page 12 of 26

If you are transmitting CVI via any form of telecommunications, the following measures should be used:

Encryption is required when transmitting CVI over the internet, high-frequency, or other radio signals (including cellular telephones). In some circumstances, mission accomplishment may require the transmission of CVI over these technologies without encryption. *However*, absence of encryption capability does not justify routine unencrypted transmission of CVI through these public channels.



Encryption is not required when CVI is discussed over wire line telecommunications networks or when transmitted via fax. When faxing CVI, ensure that an individual authorized to access CVI is standing by at the destination to receive the facsimile.

If you choose to send CVI by US Postal Service or Commercial Carrier, you must provide double protection to any document or electronic storage device, e.g. compact disk. Ensure the CVI has the cover sheet or similar warning attached. An outer envelope or wrapping should not identify the information as CVI. Information may only be sent to another authorized user. Check with the CSCD Help Desk if you are unsure the recipient is an authorized user.

Any time you share CVI, you must keep a log of who received the information. Include in the log the following information:

- Date CVI was shared

- Tracking number(s) of the CVI shared

- Who received the CVI

- Contact information for the recipient

- How CVI was sent to the recipient

- Evidence of receiving prior written authorization from CSCD Director (if required)

Access to CVI

Page 13 of 26

Access to CVI - Working with CVI while in Temporary Duty Status

If you DO NOT work in a classified open storage area;

CVI that is not in your immediate possession or use must be:

- Be under the control of an authorized person at all time while in transit (e.g., may not be placed in checked baggage)

- Must be placed in an opaque envelope and sealed while in transit; CVI should not be viewed if people without a need to know may view or have access to this information

- When traveling by car, properly packaged materials containing CVI may be locked in the trunk when the traveler is away from the vehicle

- In a hotel, if a room safe is available and suitable, the room safe is the preferred method for protecting materials containing CVI while in temporary duty status (e.g., hotel or guest offices). Otherwise, take other suitable precautions available to protect materials containing CVI from unauthorized disclosure and to reveal evidence of tampering. Precautions similar to those used for protecting personal valuables while traveling may be used (e.g., locked in a briefcase or suitcase within a locked room).

- Materials containing CVI must always have a cover sheet attached and must not be displayed when the materials containing CVI is not in use;

Workstations must:

- Use the screen locking features, be logged off, or be turned off, when not in use during your business day

- Be logged off a the end of your business day

CVI Work Products

Types of Work Products

An authorized user may on occasion need to create products that contain or are based upon CVI. These products are subject to the same handling, storage and marking requirements as the original CVI.

The two primary categories of CVI work products are:

- sanitized information
- derivative products which may be unclassified or classified.



Products Derived from CVI Sanitized Information

Page 15 of 26

CVI may be used to prepare information for public release. Examples include advisories, alerts, and warnings issued to the public or a foreign government. This information product must be sanitized before its release.

The author should consider the following points before disseminating the sanitized information.

Is proprietary, business-sensitive, or trade-secret information included?

Have I identified the submitting person or entity (explicitly or implicitly)? or

Have I provided information otherwise not customarily in the public domain?

Products Derived from CVI Sanitized Information

Page 16 of 26

When appropriate and necessary, the author should contact the chemical facility representative to ensure that the product does not contain proprietary, business-sensitive, or trade-secret information.

If the author finds the same information through open sources, he may use that information without coordinating its release with the chemical facility.



Products Derived from CVI Unclassified Products

Page 17 of 26

All users must follow these guidelines when preparing an unclassified derivative products from CVI:

Insert the text "Chemical-terrorism Vulnerability Information" in the header and footer in a font larger than the document text

Mark each paragraph, table, graphic, figure, etc., containing Cvl parenthetically as "CVI". (All other paragraphs tables, graphics, figures, etc, are not portion-marked.)

Include the CVI Tracking Number on each corresponding page

Include the Distribution Limitation Statement on the outside front and back cover

Affix a CVI Cover Sheet to the derivative product

Counter-terrorism Vulnerability Information

Section 550 of Public Law (PL) 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) authorizes DHS to employ a SBU designation to identify information created and used to manage chemical facility anti-terrorism standards.

(CVI)In the context of this Manual, pursuant to the chemical facility anti-terrorism standards defined in the interim final rule (6 CFR Part 27), this SBU designation is referenced as "Chemical-terrorism Vulnerability Information" or "CVI." Section 550(c) stipulates that information developed under this program (including vulnerability assessments, site security plans, and other security related information, records, and documents) shall be given protections from public disclosure. (CVI)

Tracking #: 021-276-335

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).

[CLICK GRAPHIC TO ENLARGE](#)

Products Derived from CVI Classified Products

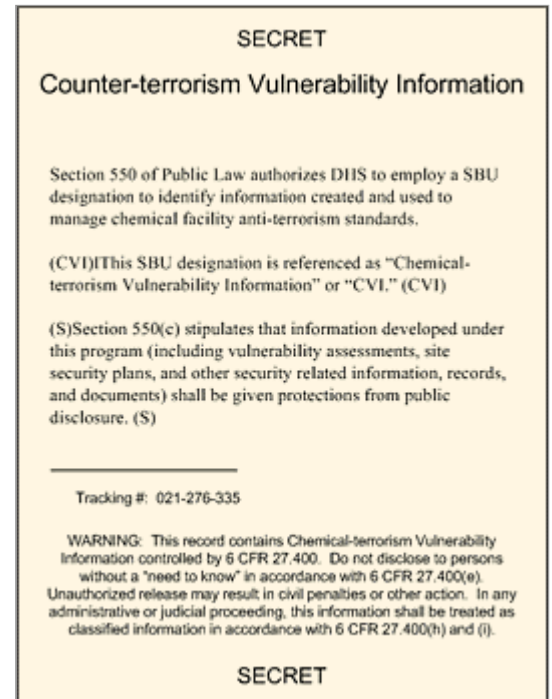
Classified CVI derivative products should be handled and protected in accordance with the safeguarding and handling requirements for both CVI and the highest level of classification within the product. All users must follow these guidelines when preparing a classified CVI derivative product, in addition to the procedures required by the classified designation:

Insert the text "Chemical-terrorism Vulnerability Information" in the header and footer in a font larger than the document text

Each paragraph, table, graphic, figure, etc., containing CV must be marked as "CVI". All other paragraphs, tables, graphics, figures, etc. are not portion marked. Where information in the paragraph, table, graphic figure, etc., are both CVI and Classified, it must be double-marked [e.g.,(S)(CVI) or (TS)(CVI)]. This double marking is necessary because subsequent declassification will eliminate only the requirement for protecting the data as classified information. It will NOT eliminate the requirements for protecting CVI

Include the CVI Tracking Number in an endnote

Affix a CVI Cover Sheet to the derivative product. Place CVI Cover Sheet immediately behind the classified Cover Sheet



[CLICK GRAPHIC TO ENLARGE](#)

Destroying CVI

Directions

Page 19 of 26

Authorized users shall destroy copies of CVI they have received when no longer needed to achieve homeland security duties.

Suggested methods include:

"Hard Copy" materials will be destroyed by crosscut shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.

All information stored in the DHS information collection database will be deleted and destroyed according to processes defined by the DHS IT Security Office.

CVI received or originally created by CSCD may only be destroyed in accordance its record schedule established under the Federal Records Act.



Oversight of CVI

Page 20 of 26

Government's Obligations Under the Memorandum of Agreement

Authorized users must safeguard CVI according to the requirements of the CVI Procedures Manual. In addition, the Memorandum of Agreement signed between the Director of CSCD and a government entity obligates it to undertake the following responsibilities

- Appoint a Security Officer to provide oversight and serve as the initial resource for CVI questions.

- Identify or establish authorities to initiate enforcement action against anyone who may knowingly misuses CVI.

- Submit an annual report summarizing how CVI was used by the government entity.

Failure to implement the terms of the Memorandum of Agreement will result in its termination. The nonconforming government entity will be required to return all CVI and may lose any privileges to access CVI in the future.

D

Oversight of CVI

Role of the Security Officer

CVI Security Officers with government agencies that signed an MOA have the following responsibilities:

Demonstrate full familiarity with the minimum requirements for protecting CVI according to Section 550(c) and any properly promulgated regulations, and the procedures established in this Manual

Help authorized users determine need to know and whether an individual is currently an authorized user

Assist authorized users to amend contracts requiring compliance with Section 550(c), the regulations, and this Manual

Ensure that authorized users understand the appropriate procedures for marking CVI work products, including derivative materials, alerts, warnings and advisories, are used, handled, and disseminated appropriately and properly safeguarded

Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the handling, use, and storage of CVI

Coordinate the preliminary investigation into any suspected or actual misuse, loss or unauthorized dissemination of CVI or any suspicious or inappropriate requests for CVI

Ensure that the appropriate Disclosure Office is aware that CVI is Federal information so that Disclosure Officers are prepared to make an appropriate response to requests for CVI under their respective disclosure laws. The State or local Disclosure Officers must inform requestors that CVI is Federal information and that the Section 550(c) explicitly protects CVI from disclosure under all disclosure laws.

Coordinate promptly and appropriately with the CSCD CVI Security Officer regarding any request, challenge, or complaint arising out of the implementation of the DHS CVI protection program

Participate in meetings with CVI Officer working groups, and other coordination activities regarding CVI
Initiate, facilitate, and promote activities to foster and maintain awareness of CVI policies and procedures

To the extent practicable, remind individuals of their post-employment CVI responsibilities

Complete and file an annual report with the CSCD Director by February 1 of each year



Sharing CVI Under Exigent Circumstances Procedures

Page 22 of 26

In the event of emergency or exigent circumstances, dissemination or access to CVI can be granted without meeting the provisions of this Section, provided a record is kept and immediately submitted to the CSCD CVI Security Officer (e.g., within less than 24 hours), including:

- Date CVI was shared
- Who received the CVI
- Contact information for the recipient
- How CVI was sent to the recipient
- Reason for emergency or exigent dissemination/access

Within five business days following receipt of notice of emergency or exigent dissemination/access being granted, the CSCD CVI Security Officer will contact the recipient and ensure the recipient meets all of the requirements for an authorized user.

Responding to Public Disclosure Requests Procedure

Page 23 of 26

Under Section 550 of Public Law 109-295, information designated as CVI qualifies for exemption from disclosure under the Freedom of Information Act and similar state or local sunshine laws.

Any requests for public disclosure should be referred to the CSCD Director and the appropriate DHS Disclosure Officer. All CVI is protected from disclosure, however, the portions of derivative products not marked as CVI may be released pending a review by the DHS Disclosure Officer and consultation with the affected chemical facility.

Reporting Disclosure Violations Authorized User Responsibilities

Page 24 of 26

Any violations of the procedures could endanger the national security of the United States. If CVI is not handled in accordance with the law, the implementing regulation and stated procedures, the release of information will compromise the security of the nation's chemical facilities. You are responsible for immediately reporting to your CVI Security Officer the actual, suspected, or alleged violation of security procedures, the loss or misplacement of CVI, and any unauthorized disclosure. The CVI Officers must notify the CSCD Director and the DHS Inspector General.

Employee reports regarding a manager's alleged improper use or disclosure of CVI may be made directly to the CSCD Director or the DHS Inspector General.



Consequences for Procedure Violations Penalties for Federal, State and Local Employees, Contractors

Page 25 of 26

A Federal employee who knowingly publishes, divulges, discloses CVI in any manner or to any extent not authorized by law, shall be fined under Title 18, imprisoned not more than one year, or both, and shall be removed from office of employment.

State and local employees will be penalized or fined under the authorities identified in the Memorandum of Agreement between DHS and the government agency in question.

A contractor's employee will face possible termination and the contractor will face possible termination of the contract.



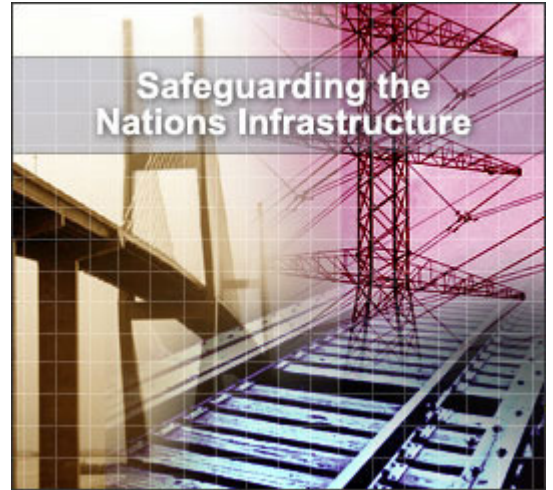
Summary

Page 26 of 26

CVI Authorized User

Chemical facilities expect that the information provided to DHS will be protected from public disclosure or misuse by government.

DHS depends on the accurate and complete submission of critical infrastructure information to ensure the safety of the nation and the ability to prevent and respond to terrorist threats. Continued proper use and handling of CVI will assure the private sector that the government can be trusted to use sensitive information responsibly.



GLOSSARY

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Access - The ability or opportunity to gain knowledge of information.

Authorized User - a covered person who has:

Been found by the holder of the CVI to have a need to know as defined below;

In the case of non-Federal employees, signed an applicable Non-Disclosure Agreement (NDA);

Completed all DHS-approved training/awareness requirements; and

Completed any required background checks or other requirements for personal identification or trustworthiness that may be required by DHS.

Individuals that are not government employees or their contractors may only become authorized users if they are directly employed or under contract to a regulated chemical facility. Those individuals in the private sector that receive consent to hold CVI are not authorized users and may not further disseminate this information.

[return to top](#)

C

Chemical 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 term chemical facility or facility shall also refer to the owner or operator of the chemical facility. Where multiple owners and/or operators function within a common infrastructure or within a single fenced area, the Assistant Secretary may determine that such owners and/or operators constitute a single chemical facility or multiple chemical facilities depending on the circumstances.

Chemical Security Assessment Tool (CSAT) - a suite of four applications, including User Registration, Top-Screen, Security Vulnerability Assessment, and Site Security Plan, through which the Department of Homeland Security will collect and analyze key data from chemical facilities.

Chemical-terrorism Vulnerability Information (CVI) - information used to determine chemical facility readiness to deter, mitigate, or respond to a terrorist attack. CVI includes vulnerability assessments, site security plans, inspection findings, self-audits, sensitive portions of enforcement-related documents, and correspondence between chemical facilities and the Federal government. The Secretary of Homeland Security, in his discretion may determine additional information warrants protection as CVI.

Critical Infrastructure - Systems and assets, whether physical or virtual, so vital to the United States that if incapacitated or destroyed, it would debilitate security, national economic security, national public health or safety, or any combination thereof.

Critical Infrastructure Information - Information not customarily in the public domain and related to the security of critical infrastructure or protected systems concerning:

(A) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety, (B) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

[return to top](#)

D

Designate/Designation - Designate/designation refers to an original determination made by the Secretary or his/her designee that information not otherwise categorized as CVI under the regulations (Section 27.400(b)(1) through (8)), qualifies as CVI under Section 27.400(b)(9).

[return to top](#)

E

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.

[return to top](#)

N

Need to Know - The determination made by an authorized user of CVI that a prospective recipient requires access to specific information to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official homeland security duties.

The determination made by an authorized user of CVI that a prospective recipient requires access to specific information to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official homeland security duties. A person, including a state or local official, has a need to know in each of the following circumstances:

When the person requires access to specific materials containing CVI to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by DHS.

When the person needs the information to receive training to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by DHS.

When the information is necessary for the person to supervise or otherwise manage individuals carrying out chemical facility security activities approved, accepted, funded, recommended, or directed by the DHS.

When a person needs the information to provide technical or legal advice to a covered person regarding chemical facility security requirements of Federal law.

In addition:

A Federal, state or local governmental employee has a need to know if access to the information is necessary for performance of the employee's official homeland security duties.

A person 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 specifically related to chemical security.

Nothing shall prevent the DHS from determining, in its discretion, that a person not otherwise listed above has a need to know CVI in a particular circumstance. For some specific CVI, the CSCD Director may restrict access to only specific persons or classes of persons that have a need to know.

[return to top](#)

[Close](#)

Resources

[Download Adobe Acrobat Reader](#)

[6 CFR Part 27 - Chemical Facility Anti-Terrorism Standards](#)

[2007 DHS Appropriations, Public Law 109-295, Section 550](#)

[CVI Website](#)

[DHS Interactive](#)

[Executive Order 12958 - Classified National Security Information](#)

Chemical-terrorism Vulnerability Information Procedures Manual

Available from the Chemical Security Compliance Division:

Department of Homeland Security

Mail Stop 8100

245 Murray Lane, SW, Building 410

Washington, DC 20528-0001

Phone: 703-235-0000

Email: CVI-info@dhs.gov

Select [Close](#) to return to the main page.

Help

Courseware Requirements

This training was designed for the minimum desktop and laptop configurations:




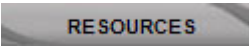
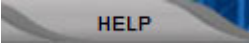
Screen resolution of 1024 X 768

Minimum Window 95 Sp3/98/ME/2000/XP

Minimum Internet Explorer 5.5 or higher or Netscape 4.75 or higher

Macromedia Flash 7.0 plug-in

Course Navigation

| Feature | Description |
|--|---|
|  | The BACK button displays the previous content screen. |
|  | The NEXT button displays the next content screen. |
|  | The Page Indicator displays the number of the current screen in relation to the total screens in the topic. |
|  | The RESOURCES button provides links to downloads and documents referred to in the training. |
|  | The HELP button provides access to course-related information. |

Select [Close](#) to return to the main page.

Knowledge Assessment

Question 1

Page 1 of 6

What is the first step that must be completed before a state employee may gain access to CVI?

Select the correct answer and then click **Check Your Answer**.

- Employee completes a background check
- The employee signs a non-disclosure agreement
- The employee calls the chemical facility and asks for a copy
- The employee's state agency signs a Memorandum of Agreement with DHS

**Check Your Answer****Reset**

Knowledge Assessment

Question 1

Page 1 of 6

What is the first step that must be completed before a state employee may gain access to CVI?

Select the correct answer and then click **Check Your Answer**.

- Employee completes a background check
- The employee signs a non-disclosure agreement
- The employee calls the chemical facility and asks for a copy
- The employee's state agency signs a Memorandum of Agreement with DHS

**Check Your Answer****Reset**

Correct! Access may only be granted after a government component has signed a Memorandum of Agreement that explains the state's obligations for safeguarding CVI.

Knowledge Assessment

Question 2

Page 2 of 6

You are responsible for sanitizing a CVI derivative product to be disseminated to the public by removing:

Select all that apply and then click **Check Your Answer**.

- The identity of the submitting person or entity and any proprietary or business-sensitive information.
- Any other information not customarily found in the public domain.
- Any information that implicitly or explicitly relates to the submitting person or entity.
- Any information that can be found by searching the Internet.

**Check Your Answer****Reset**


Knowledge Assessment

Question 2

You are responsible for sanitizing a CVI derivative product to be disseminated to the public by removing:

Select all that apply and then click **Check Your Answer**.

- The identity of the submitting person or entity and any proprietary or business-sensitive information.
- Any other information not customarily found in the public domain.
- Any information that implicitly or explicitly relates to the submitting person or entity.
- Any information that can be found by searching the Internet.

 **Check Your Answer**

Reset

Correct! When creating a sanitized work product, you must ensure that it does not contain the identity of the submitting entity, implicitly or explicit, does not contain proprietary or business-sensitive information or any other information not customarily in the public domain.

Knowledge Assessment

Question 3

Page 3 of 6

When transporting CVI outside of your work space, how should it be safeguarded?

Select the correct answer and then click **Check Your Answer**.

- Contained within a double covering. The outer cover is plain with the inner cover being the CVI cover page.
- In a single sealed envelope addressed to an authorized user but with NO markings indicating it is CVI.
- In two envelopes with the outer envelope addressed to an authorized user and with a CVI Cover Sheet attached to the outside of the envelope.
- In any available envelope addressed to an authorized user.

**Check Your Answer****Reset**

Knowledge Assessment

Question 3

When transporting CVI outside of your work space, how should it be safeguarded?

Select the correct answer and then click **Check Your Answer**.

- Contained within a double covering. The outer cover is plain with the inner cover being the CVI cover page.
- In a single sealed envelope addressed to an authorized user but with NO markings indicating it is CVI.
- In two envelopes with the outer envelope addressed to an authorized user and with a CVI Cover Sheet attached to the outside of the envelope.
- In any available envelope addressed to an authorized user.



Check Your Answer

Reset

Correct! CVI must be transported with two coverings with a plain outer cover and with CVI cover page serving as the inner cover.

Knowledge Assessment

Question 4

Page 4 of 6

Your co-worker went to lunch and left CVI openly exposed (no cover sheet) on his desk. What should you do?

Select the correct answer and then click **Check Your Answer**.

- You ignore the violation because you don't want to get your co-worker in trouble.
- You report the violation to your manager because CVI is not to be openly exposed under any circumstances.
- You don't do anything, since you work in a classified open storage area.
- You look over the information, since you are an authorized user.

**Check Your Answer****Reset**

Knowledge Assessment


Question 4

Page 4 of 6

Your co-worker went to lunch and left CVI openly exposed (no cover sheet) on his desk. What should you do?

Select the correct answer and then click **Check Your Answer**.

- You ignore the violation because you don't want to get your co-worker in trouble.
- You report the violation to your manager because CVI is not to be openly exposed under any circumstances.
- You don't do anything, since you work in a classified open storage area.
- You look over the information, since you are an authorized user.

 **Check Your Answer**

Reset

Correct! You are obligated to report the violation to your manager because CVI is not to be openly exposed under any circumstances.

Knowledge Assessment

Question 5

The unclassified report you created contains CVI. Which of the following headers is correct?

SECRET
Chemical-terrorism Vulnerability
Information

(CVI) Sensitive information here.

Non-sensitive information
provided in original submission.

(CVI) Sensitive information
provided again.

Chemical-terrorism Vulnerability
Information
SECRET

A.

SECRET

(CVI) Sensitive information here.

Non-sensitive information
provided in original submission.

(CVI) Sensitive information
provided again.

SECRET

B.

Chemical-terrorism Vulnerability
Information

(CVI) Sensitive information here.

Non-sensitive information
provided in original submission.

(CVI) Sensitive information
provided again.

Chemical-terrorism Vulnerability
Information

C.

Select the correct answer and then click **Check Your Answer**.

A

B

C



Check Your Answer

Reset

- CVI Authorized User Training
 - [Introduction](#)
 - [What information qualifies](#)
 - [Access to CVI](#)
 - [Products Derived from CVI](#)
 - [Handling CVI](#)
 - [Summary](#)
 - [Knowledge Assessment](#)

SECRET

Chemical-terrorism Vulnerability Information

(CVI) Sensitive information here.

Non-sensitive information provided in original submission.

(CVI) Sensitive information provided again.

Chemical-terrorism Vulnerability Information

SECRET

A.

SECRET

(CVI) Sensitive information here.

Non-sensitive information provided in original submission.

(CVI) Sensitive information provided again.

SECRET

B.

Chemical-terrorism Vulnerability Information

(CVI) Sensitive information here.

Non-sensitive information provided in original submission.

(CVI) Sensitive information provided again.

Chemical-terrorism Vulnerability Information

C.

Select the correct answer and then click **Check Your Answer**.

A

B

C

Correct. The correct answer is C. Documents containing CVI must have "Chemical-terrorism Vulnerability Information" in the header and footer. Each paragraph containing CVI must also be marked (CVI).

Knowledge Assessment Congratulations

Page 6 of 6

Congratulations! You have finished CVI Authorized User Training.

Click the link below to view the Non-Disclosure Agreement. Once open, print th NDA, complete the appropriate fields, and sign the form.

[Non-Disclosure Agreement](#)

Now click below to print your certificate of completion. You will need to fill out a form before the certificate is available.

[Certificate of Completion](#)

Fax the completed and signed Non-Disclosure Agreement, the cover sheet and certificate of completion to the PCII Program Office, (703) 288-4058.

**DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT FOR CVI**

I, , an individual official, employee, consultant, or subcontractor of or to (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

I hereby acknowledge that I am familiar with, and I will comply with all requirements of the Chemical Security Compliance Program set out in Section 550 of PL 109-295, as amended, 6 CFR Part 27, as amended, the applicable CVI Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the Director of the DHS Chemical Security Compliance Division (CSCD) or his/her designee.

I hereby acknowledge that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the CVI to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the CVI.

I understand and agree to the following terms and conditions of my access to CVI indicated above:

1. I hereby acknowledge that I have received a security indoctrination / training concerning the nature and protection of CVI to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing CVI have been approved for access to it, and that I understand these procedures.
2. By being granted conditional access to CVI, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to CVI to which I am granted access.
3. I acknowledge that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with terms of this Agreement and the laws, regulations and/or directives, applicable to the information to which I am granted access. I understand that DHS may conduct inspections of my place of business pursuant to established procedures for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding of CVI under this Agreement. In the case of non-DHS Federal agencies inspections will be conducted in coordination with the appropriate Federal officials.

4. I will not disclose or release any CVI provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such CVI, I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the CVI. I will honor and comply with any and all dissemination restrictions cited to me by the proper authority.
5. (a) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the Chemical Security Compliance Program, whichever occurs first, I will surrender promptly to the DHS CSCD CVI Security Officer or his/her designee, or to the appropriate corporate, component or authorized entity Security Officer, CVI of any type whatsoever that is in my possession.
(b) If the Authorized Entity is a United States Government contractor performing services in support of the Chemical Security Compliance Program, I will not request, obtain, maintain, or use CVI unless the DHS CSCD CVI Security Officer or his/her designee has provided approval in writing.
6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, unless such alteration or removal is authorized by the DHS CSCD CVI Security Officer or his/her designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.
7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for CVI, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation that I have knowledge of, whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.
8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.
9. With respect to CVI, I hereby assign to the entity owning the CVI and the United States government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of CVI not consistent with the terms of this Agreement.
10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context,

the United States Government and, with respect to CVI, the Authorized Entity, may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of DHS, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.
12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.
13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.
14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783 (b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.
15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.
16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT
Acknowledgment

I make this Agreement in good faith, without mental reservation or purpose of evasion.

SIGNATURE: _____ Date _____

Name:

Organization:

Business Address:

Telephone:

E-mail:

WITNESS: _____ Date _____

Name:

Organization:

Business Address:

Telephone:

E-mail:

Certificate of Completion

Paperwork Burden Disclosure Notice

Page 1 of 3

The public reporting burden for this form is estimated to be 30 minutes. The burden estimate includes time for reviewing instructions, providing information to register you as a CVI authorized user, and submitting this information to DHS. Send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: Information Collections Management, Attention: Sabrina Nelson, DHS Desk Officer, U.S. Department of Homeland Security, GSA Bldg, 7th & D Street. SW mail Stop 3725-1 Washington, D.C. 20528 (Paperwork Reduction Project (1670_XXXX)). You are not required to respond to this collection of information unless a valid OMB control number is displayed in the upper right corner of the form asking for personal information at the conclusion of this training.