PROCEDURAL MANUAL
SAFEGUARDING INFORMATION DESIGNATED AS CHEMICAL-TERRORISM VULNERABILITY INFORMATION (CVI)

June 2007

Approved for Release: _____

Lawrence Stanton
Director (Acting), CSCD

_____

Andrew J. Puglia Levy
Deputy General Counsel
Office of the General Counsel

Contents

1.0 Purpose 4
2.0 Scope 4
3.0 Authorities 4
4.0 Definitions 5
5.0 Responsibilities 8
5.1 Chemical Security Compliance Division (CSCD) 8
5.2 Other Federal, State, and Local Agencies 9
5.3 Regulated Chemical Facilities 10
5.4 CVI Security Officers and CVI Points of Contact 10
6.0 Policy and Procedures 15
6.1 General 15
6.2 Information Designated as CVI 15
6.3 Education, Training, and Awareness 16
7.0 Marking Materials Containing CVI 17
8.0 General Handling Procedures 17
8.1 Storage 19
8.2 Transmission of Hard Copy Materials 20
8.3 CVI in Transit or Use at a Temporary Duty Station 21
8.4 Electronic Transmission 21
9.0 Destruction 23
10.0 Dissemination and Access 23
10.1 Dissemination and Access – General 23
10.2 Dissemination and Access - Non-DHS Federal Agencies 27
10.3 Dissemination and Access – Federal Government Contractors 28
10.4 Dissemination and Access – State and Local Agencies 28
10.5 Dissemination and Access – Regulated Chemical Facilities 29
10.6 Dissemination and Access – Derivative Products 30
10.7 Dissemination and Access – DHS Advisories, Alerts, and Warnings 31
10.8 Dissemination and Access – Open Sources 32
10.9 Dissemination and Access – Automated Information Systems 32
10.10 Dissemination and Access – Emergency or Exigent Circumstances 33
10.11 Dissemination and Access – Objections, Appeals and Administrative or Civil/Criminal Judicial Proceedings 33
10.12 Freedom of Information Act (FOIA) Requests 33
11.0 Incident Reporting 34
APPENDIX A: Unique CVI Record Tracking Number 36
APPENDIX B: Individual Non-Disclosure Agreement 37
APPENDIX C: Memoranda of Agreement 42
APPENDIX D: Contract Language 52
APPENDIX E: Marking CVI 53
APPENDIX F: Flowcharts for Sharing CVI 54
APPENDIX G: Front and Back Cover for Material Containing CVI 59

SAFEGUARDING INFORMATION DESIGNATED AS CHEMICAL-TERRORISM VULNERABILITY INFORMATION (CVI)

April 2007

1.0 Purpose

This Manual establishes Department of Homeland Security (DHS) policy regarding the identification and safeguarding of Sensitive but Unclassified (SBU) information authorized under Section 550 of Public Law (PL) 109-295. This information will be referred to as Chemical-terrorism Vulnerability Information (CVI). This procedural manual contains the minimum standards for covered persons to mark, store, control, transmit, and destroy CVI.

2.0 Scope

This manual is applicable to and mandatory for anyone authorized to receive CVI, including but not limited to all DHS employees and contractors, as well as other Federal, state and local government employees and contractors. CVI may also be held by representatives of regulated chemical facilities. This manual defines the procedures for safeguarding CVI from transmission to storage. Authorized users will use this manual to follow the appropriate procedures for creating derivative products and understand the proper steps in sharing the information with other parties.

3.0 Authorities

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. 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.

4.0 Definitions

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

Authorized User – An authorized user is 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 categorized as authorized users since this group is not granted the right to further disseminate this information.

Automated Information Systems – Automated Information Systems (AIS) refers to any computer-based system that either:

- Enables a facility to submit CVI *e.g.*, Chemical Security Assessment Tool (CSAT); or
- Allows for the electronic storage and transmission of CVI.

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 DHS. As used herein, the terms "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 upon the circumstances.

Chemical Security Compliance Division Director – The Director of the DHS Chemical Security Compliance Division (CSCD) or his/her designee.

Chemical-Terrorism Vulnerability Information (CVI) – CVI includes the information designated in the regulations, as shown in Table 1, and any derivative products made from these documents:

Table 1 Records Designated as CVI

Reference	Description	Who Creates?	Who Receives?
27.200	Top Screen	Regulated facility	CSCD

Table 1 Records Designated as CVI			
Reference	**Description**	**Who Creates?**	**Who Receives?**
27.205(a)	Initial determination by Assistant Secretary that a chemical facility presents a high level of security risk	Assistant Secretary or delegated authority	Regulated facility
27.205(b)	Request for re-determination	Regulated facility	Assistant Secretary or delegated authority
27.210(a); 27.215	Security Vulnerability Assessment (SVA)	Regulated facility	CSCD
27.210(a); 27.225	Site Security Plan (SSP)	Regulated facility	CSCD
27.210(b); 27.235	Alternative Security Plan (ASP)	Regulated facility	CSCD
27.220(a) and (b)	Notice of Placement in a Risk Tier	Assistant Secretary or delegated authority	Regulated facility
27.240(a)	Letter of Approval for SVA	Assistant Secretary or delegated authority	Regulated facility
27.240(b)	Notice of Deficiency for SVA	Assistant Secretary or delegated authority	Regulated facility
27.245(a)	Letter of Authorization for SSP	Assistant Secretary or delegated authority	Regulated facility
27.245(a)	Letter of Approval for SSP	Assistant Secretary or delegated authority	Regulated facility
27.245(b)	Notice of Deficiency for SSP	Assistant Secretary or delegated authority	Regulated facility
27.245(a); 27.250(e)	Inspection Findings/Correspondence	DHS Inspector	CSCD
27.255(a)(1)	Training Records	Regulated facility	Regulated facility
27.255(a)(2)	Exercise and Drill Records	Regulated facility	Regulated facility
27.255(a)(3)	Incidents and breaches of security	Regulated facility	Regulated facility
27.255(a)(4)	Maintenance, calibration, and testing of security equipment	Regulated facility	Regulated facility
27.255(a)(5)	Security Threats	Regulated facility	Regulated facility
27.255(a)(6)	Audit Record	Regulated facility	Regulated facility
27.255(b)	Sensitive correspondence between regulated facility and DHS	Regulated facility and DHS	Regulated facility and DHS

Table 1 Records Designated as CVI			
Reference	**Description**	**Who Creates?**	**Who Receives?**
27.300(b)	Order of Compliance as describes actions for coming into compliance	Assistant Secretary or delegated authority	Regulated facility
27.300(d); 27.310(b)	Notice for Application for Review	Regulated facility	Assistant Secretary or delegated authority

Covered Person – Is anyone who:

- Has access to CVI pursuant to a need to know determination; or
- Otherwise receives or gains access to what they know or should reasonably know constitutes CVI.

Designate/Designation – Designate/designation refers to an original determination made by the Secretary or his/her designee that information developed for chemical facility security purposes but not otherwise categorized as CVI under the regulations (Section 27.400(b)(1) through (8)) warrants designation as CVI under Section 27.400(b)(9).

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.

Need to Know – The determination made by a CVI Security Officer 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 applicable CVI Security Officer will determine if 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.

5.0 Responsibilities

5.1 Chemical Security Compliance Division (CSCD)

CSCD will:

a. Be responsible for the practical application of all aspects of the program to protect materials containing CVI.
b. Promulgate policy guidance, as necessary, to implement a CVI protection program.
c. Develop procedures for coordinating with the Secretary to determine if specific information or types of information warrant protection as CVI under Section 27.400(b)(9).
d. Develop and implement a central DHS education and awareness program for safeguarding of materials containing CVI.
e. Develop and maintain a central authorized user database and implement a program for ensuring that only authorized users have access to materials containing CVI.
f. Maintain a Tracking Log of the receipt and subsequent dissemination of CVI held by CSCD, including:
    - Date CVI was received;
    - Date CVI was shared;
    - Who received the CVI;
    - Contact information for the recipient;
    - How CVI was sent to the recipient; and
    - Evidence of receiving consent, if required.
g. Ensure that all information is marked appropriately, and apply a unique tracking number to all information received by DHS (*e.g.*, the unique facility number plus an information-type designation). The numbering system shown in

Appendix A may be used to identify the unique facility number and the information-type designation.

h. Appoint a DHS/CSCD CVI Security Officer and Deputy CVI Security Officer.
i. Develop a program for determining when and to what extent background checks should be required for authorized users. For Federal Employees and Contractors, such procedures will be in compliance with the DHS program under Federal Information Processing Standards *(*FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

5.2 Other Federal, State, and Local Agencies

Non-DHS Federal, state, and local agencies must enter into a Memorandum of Agreement (MOA) with CSCD before receiving CVI. Generally, it is expected that the MOA with a state will cover all state and local agencies and separate MOAs will not be required for each separate agency within that state. The MOA also requires the agency to appoint a CVI Security Officer that will provide oversight and assistance to authorized users. In addition, the CVI Security Officer will arbitrate whether a person covered by a state's MOA has the need to know CVI. For employees of other Federal, state, and local agencies to become authorized users, they must accept the following responsibilities:

a. Be aware of and comply with the safeguarding requirements for CVI, as outlined in the regulations, in this Manual and in any other guidance or direction issued by CSCD.
b. Participate in DHS-approved training presented to communicate the requirements for safeguarding CVI and other SBU information.
c. Be aware that divulging information without proper authority could result in civil penalty or administrative or disciplinary action.
d. For state and local agency employees, enter into a DHS-approved NDA. (See Appendix B.)
e. Maintain a Tracking Log of the receipt and subsequent dissemination of CVI, including :

   - Date CVI was received
   - Date CVI was shared
   - Who received the CVI
   - Contact information for the recipient
   - How CVI was sent to the recipient, and
   - Approval from the CVI Security Officer that the requestor demonstrated a need to know
   - Evidence of receiving consent, if required.

f. Ensure all information is marked appropriately, and apply the unique tracking number to all derivative products.
g. Complete any required background checks or other requirements for personal identification or trustworthiness that may be required by DHS (DHS may sanction the use of equivalent non-DHS Federal, state or local background check procedures).

5.3 Regulated Chemical Facilities

Chemical facilities are required to appoint a CVI point of contact who will serve as the primary liaison with CSCD. This person will also provide oversight and assistance to individuals that are provided access to CVI within the chemical facility. Chemical facilities including their board members, employees and contractors, who require access to CVI will:

a. Be aware of and comply with the safeguarding requirements for CVI as outlined in the regulations, in this Manual and in any other guidance or direction issued by CSCD.
b. Participate in DHS-approved training presented to communicate the requirements for safeguarding CVI.
c. Be aware that divulging information without proper authority could result in civil penalty or administrative or disciplinary action.
d. Enter into an appropriate NDA similar to that shown in Appendix B.
e. Maintain a Tracking Log of the receipt and subsequent dissemination of CVI, including:

- Date CVI was received;
- Date CVI was further disseminated;
- Who received the CVI (make sure to identify private third parties that do not have the authority to further disseminate CVI);
- Contact information for the recipient;
- How CVI was sent to the recipient; and
- Evidence of receiving DHS authorization, as required.

f. Ensure that all information is marked appropriately.
g. Complete any required background checks or other requirements for personal identification or trustworthiness that may be required by DHS.

.

5.4 CVI Security Officers and CVI Points of Contact

a. The CSCD CVI Security Officer has the following responsibilities:

- Demonstrate full familiarity with the minimum requirements for protecting CVI according to Section 550(c), the implementing regulations, and the procedures established in this Manual.
- When appropriate, certify or assist the CSCD Director in certifying Federal contractors who require access to CVI. This includes confirming they have appropriate language in their contracts requiring compliance with Section 550(c), the implementing regulations, and this Manual (see Appendix D) and have an official chemical security program purpose.

- Implement operational procedures, pursuant to guidance given by the CSCD Director, to enter into and enforce compliance with the provisions of MOAs with non-DHS Federal, state and local Agencies.
- Ensure the secure dissemination of CVI to only authorized users, including:
    - Response to, or assistance with, need to know inquiries;
    - Assistance to the CSCD in developing, delivering and maintaining initial and ongoing training programs; and
    - Assistance to the CSCD in certifying Federal contractor NDAs are executed and implemented.
- Implement operational procedures, pursuant to guidance given by the CSCD Director, to ensure that CVI and 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 investigation into any suspected misuse, loss or unauthorized dissemination of CVI or any suspicious or inappropriate requests for CVI. Immediately report to the CSCD Director following such investigation if further investigation or enforcement action needs to be taken. The CSCD Director will consult with the Office on General Counsel when considering the appropriate response to the incident.
- Ensure that the National Protection and Programs Directorate Disclosure Office is aware that CVI is Federal information and that the Disclosure Officers are prepared to make an appropriate response to requests for CVI under Section 550(c) and the regulations.
- Coordinate promptly and appropriately with the CSCD Director regarding any request, challenge, or complaint arising out of the implementation of the DHS CVI protection program.
- Participate in meetings with the CSCD, CVI Officer working groups, and other coordination activities regarding CVI, as appropriate.
- 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.
- In coordination with the CSCD Director, implement operational procedures for determining when and to what extent individuals or classes of individuals must successfully complete background checks to access CVI.

b. Non-DHS Federal and state CVI Security Officers have the following responsibilities:

- Demonstrate full familiarity with the minimum requirements for protecting CVI according to Section 550(c), the implementing regulations and the procedures established in this Manual.
- Ensure the secure dissemination of CVI to only authorized users, including:

    - Determine if an authorized user request for CVI meets the need to know requirements. If the information is held by DHS, the CVI Security Officer will make the request to DHS and disseminate the information to the requesting individual;
    - For state agencies, ensure the requestor is covered by the state MOA with DHS;
    - Assure that individuals that may seek access to CVI complete the requirements to become an authorized user; and
    - Coordinate with the CSCD CVI Security Officer any requests for sharing CVI beyond the scope of an existing Memorandum of Agreement.
- Certify all contractors requiring access to CVI, including confirming they have appropriate language in their contracts requiring compliance with Section 550(c), the regulations, and this Manual. (See Appendix D) and have an official chemical security program purpose.
- Implement operational procedures to ensure that CVI and 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. Immediately report to the CSCD CVI Security Officer following such investigation if further investigation or enforcement actions need to be taken.
- 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 that qualifies for exemption from the Freedom of Information Act and similar state and local public disclosure laws. If the requestor has any further questions about the applicability of disclosure laws to CVI, state and local participating entities are encouraged to refer the requestor directly to either the CSCD CVI Security Officer or the DHS Preparedness Directorate Disclosure Office.
- 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, as appropriate.
- 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 CVI Security Officer by February 1 of each year, showing for the last calendar year:

- Tracking Log of CVI shared;
- Synopsis of ways CVI was used for homeland security purposes;
- Authorized Users certified;
- Incidents reported; and
- Implementation issues.

c. Chemical facility and federal contractor CVI Points of Contact have the following responsibilities:

- Demonstrate full familiarity with the minimum requirements for protecting CVI according to Section 550(c), the implementing regulations, and the procedures established in this Manual.
- Ensure the secure dissemination of CVI to authorized users and private third parties with a vested interest in the chemical facility, including:
  - Response to, or assistance with, need-to-know inquiries;
  - Verification that initial and ongoing training has been completed; and
  - Certification that NDAs are executed and implemented, as necessary.
- 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.

The following table provides a quick check of responsibilities for CVI protection.

Table 2 Responsibilities for CVI Protection

Requirement	Non-DHS Federal, State, and Local Agencies	Regulated Chemical Facilities	CVI Security Officers	CVI Points of Contact
Be aware of and comply with the safeguarding requirements for CVI	X	X		
Participate in DHS-approved training	X	X	X	X
Be aware of penalties for divulging CVI improperly	X	X		
Employees/ board members/contractors enter into a DHS-approved NDA, as required	X (state and local only)	X	X	X
Enter into an appropriate MOA with DHS	X			
Maintain a CVI Tracking Log	X	X		
Ensure all information is marked and has a unique tracking number	X	X		
Complete any background checks or other requirements	X	X		

Table 2 Responsibilities for CVI Protection				
Requirement	**Non-DHS Federal, State, and Local Agencies**	**Regulated Chemical Facilities**	**CVI Security Officers**	**CVI Points of Contact**
for personal identification or trustworthiness				
Appoint an agency CVI Security Officer and Deputy or CVI Point of Contact	X	X		
Be familiar with the requirements for protecting CVI			X	X
Determine a need to know for each request for CVI			X	X
Ensure Ongoing training is completed by all authorized users			X	X
Certify NDAs are executed			X (state and local only)	X
Certify all contracts requiring access to CVI have CVI language			X (Federal only)	
Implement operational procedures to ensure that CVI is used, handled, and disseminated appropriately and properly safeguarded			X	
Establish and maintain an ongoing self-inspection program			X	
Coordinate the preliminary investigation into CVI improprieties			X	
Ensure that the appropriate Disclosure Office is aware that CVI is Federal information and is not to be disclosed			X	
Coordinate any request, challenge, or complaint arising out of CVI procedures with the CSCD CVI Security Officer			X	
Participate in meetings with CVI Officer working groups and other coordination activities			X	
Foster and maintain awareness of CVI policies and procedures			X	X
Remind individuals of their post-employment CVI responsibilities			X	X

Table 2 Responsibilities for CVI Protection				
Requirement	**Non-DHS Federal, State, and Local Agencies**	**Regulated Chemical Facilities**	**CVI Security Officers**	**CVI Points of Contact**
Complete and file an Annual Report with the CSCD CVI Security Officer by February 1 of each year			X	

6.0 Policy and Procedures

6.1 General

This Manual addresses the management and handling of information and data used by DHS to identify and assess high-risk chemical facility security under Section 550 of PL 109-295. Specifically, DHS plans to collect information in several formats, including Security Vulnerability Assessments (SVAs), and Site Security Plans (SSPs). Such collection shall be performed through the completion of the Chemical Security Assessment Tool (CSAT) or a similar program by facility owner/operators, as well as through on-site inspections. DHS will utilize this information for the purposes of administering, executing and verifying compliance with the requirements of the Chemical Security Program, as well as in the generation of internal reports and analytical products.

6.2 Information Designated as CVI

Access to material containing CVI requires a valid need to know. This means an operational need for security-related information for individuals to perform official homeland security duties, and an indication of trustworthiness. The determination of trustworthiness is normally obtained based on a background check or other means to verify an individual's character. Access to material containing CVI requires the holder of the information to verify that the recipient is an authorized user and that the transfer complies with all applicable requirements for dissemination as marked on the CVI, as stipulated in this Manual or the regulations. For state and local government officials, need to know determinations will be made by the state CVI Security Officer unless otherwise noted in the Memorandum of Agreement.

With the consent of CSCD Director, regulated chemical facilities may also share CVI with private third parties, i.e. bank, insurance company, utility commission, etc. that have vested interest in the chemical facility and a need to know. These individuals are not considered authorized users since they will have the right to further disseminate CVI. These individuals must sign a chemical facility approved NDA and complete the training provided to authorized users.

If information is identified or developed that would be detrimental to chemical facility security is publicly disclosed but it is not specifically categorized as CVI under Section 27.400(b) (see Table 1 above), a request for designation as CVI can be sent to the CSCD Director. The CSCD Director will coordinate with the Secretary to determine if the information or type of information warrants protection as CVI under Section 27.400(b)(9). A record of each such original CVI designation shall be maintained, including the date, subject or title, and a detailed synopsis of the information. A copy of the record and the information to be protected will be transmitted to the CSCD CVI Security Officer within thirty (30) days following designation. Once the information has been properly designated as CVI, the designation must be communicated to appropriate parties with a need to know.

Other Federal, state, and local government agencies will not have the authority to designate information independently gained from chemical facilities as CVI. Absent emergency or exigent circumstances, state, and local government authorized users can only receive CVI with the approval of the appropriate state CVI Security Officer who will make the determination on need to know.

Only information that is specifically categorized as CVI under Section 27.400(b) (as established in Table 1 above) may be marked as CVI by regulated facilities or other covered persons. Exceptions may be made if a request has been forwarded to the CSCD CVI Security Officer for special designation under Section 27.400(b)(9) of the regulations. Such information should be marked and protected as CVI on an interim basis pending a final assessment by the Secretary or his/her designee.

Materials containing CVI must be appropriately designated and withheld from public disclosure. CVI must also be physically controlled and protected. Physical protection requirements include:

1) Secure storage
2) Document marking
3) Application of a tracking number
4) Restricted access
5) Limited reproduction
6) Secure transmission
7) Enhanced automatic data processing system controls
8) Appropriate destruction.

6.3 Education, Training, and Awareness

This section provides a high-level description of the education, training, and awareness program for all individuals seeking access to CVI. The CSCD is responsible for establishing and carrying out a program to train CSCD staff in carrying out their specific responsibilities to ensure consistent, effective and efficient handling of CVI, as well as

providing training to all covered persons seeking authorization to access CVI. The training and awareness program will help those seeking access to CVI to:

- Understand individual safeguarding and handling requirements; and
- Follow procedures for sharing CVI with other authorized users.

Before being authorized to access CVI, individuals must participate in a training and awareness program. This program must include:

- Fundamental training that prepares authorized users to comply with minimum safeguarding and handling requirements; and
- Continuing education and refresher training to ensure that authorized users are following the most recent requirements for safeguarding and handling CVI.

Where feasible, the participating entity is encouraged to remind terminating employees of:

- Their continuing responsibility not to use or disclose materials containing CVI in the future; and
- The penalties for unauthorized use of disclosure of materials containing CVI.

7.0 Marking Materials Containing CVI

CVI will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. This is a special designation for regulatory information communicated to DHS pursuant to Section 550 of PL 109-295 and shall be marked as shown in Appendix E.

Regardless of form (*e.g.*, paper, electronic, digital or sound), all CVI and any copies or materials derived there from CVI must be marked as shown in Appendix E.

If an authorized user receives a record or verbal transmission containing CVI that is not marked as specified in Appendix E, this person must:

- Mark the record as specified in this section; and
- Inform the sender of the record that the record must be marked as specified in this section.

If the CVI or material containing CVI cannot be directly marked, the cases or containers in which CVI is stored (*e.g.*, CD cases) must include the protective marking and dissemination limitation statement as shown in Appendix E.

8.0 General Handling Procedures

Original copies of CVI shall be safeguarded according to CVI requirements. Authorized users outside of the CSCD seeking access to CVI shall only be given copies of the original or derivative products.

When CVI is removed from an authorized storage location (see Section 8.1) within the workplace and persons without a need-to-know are present, or where casual observation would reveal materials containing CVI to unauthorized users, a cover sheet (see Appendix F) will be used to prevent unauthorized or inadvertent disclosure. When transmitting CVI, an appropriate cover sheet should be placed on the front and back of the transmittal letter, report, or document.

CVI may be reproduced to the extent necessary to carry out official duties. CVI copying requirements include:

a. Copies must be protected in the same manner as the original.
b. The copy must have the same marking as the original information.
c. As long as the requirements of this section are met, copy machines, scanners and printers may be used to process both CVI and non-sensitive materials.
d. Copy machine, scanners or printer malfunctions must be cleared and all paper paths checked for materials containing CVI and all unusable pages must be destroyed immediately.
e. When no longer needed, copies of CVI must be destroyed as detailed below.
f. Before allowing vendor personnel to access copy machines, scanners or printers for repair or maintenance and before disposing of such machines, an authorized person must ensure that no access to CVI is possible. This may include erasing the memory of a machine, running blank pages through, and physically inspecting the machine for residual CVI.

Computer workstations accessing or storing CVI must limit access to authorized users through a user verification process such as a login name and password. These workstations must have screen locking features when an authorized user is either inactive on the computer, must step away, or if unauthorized personnel are present. Authorized users must clear recycle bins, delete temporary files, and log off any computer holding CVI to prevent unauthorized access to it.

For further clarification about a particular submission, DHS authorized users (*e.g.*, DHS SVA reviewers or inspectors) may need to contact a regulated facility or a regulated facility may need to contact a DHS authorized user (*e.g.*, DHS Chemical Security IT Helpdesk personnel). In such cases:

a. If additional, clarifying CVI is required or offered by the regulated facility, it should be properly marked and transmitted to DHS CSCD in accordance with the requirements of this Manual.
b. If received verbally, the regulated facility must inform the authorized user that the information warrants CVI protection. Any record that may result from this

conversation that includes the affected information should be marked as CVI in accordance with the requirements of this Manual.

c. The DHS authorized user will keep a record of the verbal transaction, including the purpose of the contact and the point of contact information; however, the record should not contain CVI related to the specific facility/submitter.
d. The DHS authorized users should follow all dissemination, access and transmission precautions when discussing or communicating any CVI.

8.1 Storage

The work space where CVI is housed must have controls to limit access (*e.g.*, keys, key cards, badges, swipe cards, etc.) to those individuals who are explicitly authorized to access materials containing CVI.

When unattended, materials containing CVI will, at a minimum, be stored in a secure container, such as a safe, locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or a similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need to know. Such rooms and areas include a locked room or an area where access is controlled by a guard, cipher lock or card readers. When an individual responsible for materials containing CVI places the material in a locked container, that individual is responsible for ensuring that positive measures are in force to restrict access to the container keys or combination to only individuals with a need to know.

When CVI is managed within an area authorized for open storage of classified material, it is not necessary to store CVI in a locked container when not under the control of an authorized user, except at the end of the authorized user's workday. However, such materials must have a CVI cover sheet when not in use. When materials containing CVI are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible (*i.e.*, separate folders, separate drawers, etc.).

IT systems used to handle, store, or transmit materials containing CVI must have operational and technical controls in place to ensure that only CVI authorized personnel and processes can access electronic materials containing CVI. The computer systems will provide appropriate markings and warnings for any displayed CVI.

IT systems or AIS operated by DHS or its contractors/consultants that are used to handle, store, or transmit materials containing CVI must be certified and accredited (C&A) for operation in accordance with Federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, for more detailed information. Additional requirements may apply to IT systems or AIS that

process classified chemical security information and are operated by DHS or its contractors/consultants.

If CVI will be stored on IT systems or AIS within state or local governments, these systems must demonstrate that operational and technical controls are in place to ensure that only CVI authorized users and processes can access electronic materials containing CVI. Storage of CVI on these systems will be determined in the agency MOA.

Laptop computers and other media used to handle, store, or transmit materials containing CVI will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control of DHS or DHS contractor/consultant laptop computers and other media containing CVI will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

Laptop computers and other media used by state or local governments to handle, store, or transmit materials containing CVI must demonstrate that operational and technical controls are in place to ensure CVI will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage of CVI on these systems will be determined in the agency MOA.

Regulated chemical facilities may only store CVI on computers and networks that are accessible to individuals authorized to access CVI. These computers or systems must demonstrate operational and technical controls are in place to ensure CVI will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure.

8.2 Transmission of Hard Copy Materials

Postal Service or Commercial Carriers

The United States Postal Service or commercial carriers may be used to transport CVI, provided the material is accompanied by a CVI cover sheet. Ensure that all CVI has an appropriate inner cover or envelope before placing it in an opaque, unmarked, envelope. The CVI cover page can serve as the inner envelope. The cover page must be placed on both the front and back of the CVI. The outer envelope must bear the complete name and address of the intended recipient, who must be authorized to access CVI. The envelope must include a notation that if the intended recipient is not at this address, the package shall not be forwarded to another address and must be returned to the sender. The second/outer envelope should have no marking that identifies the contents as materials containing CVI.

Materials containing CVI may be mailed by U.S. Postal Service First Class Mail or a commercial delivery service. For U.S. Postal Service a return receipt or other tracking process must be used. Commercial delivery services must provide a tracking mechanism that documents the departure and receipt of the package.

Inter-Office Mail

Materials containing CVI may be entered into an inter-office mail system provided the CVI material is accompanied by a CVI cover sheet. The CVI must also be placed in an opaque envelope or container that is sufficiently sealed to prevent inadvertent opening and to show evidence of tampering (if any). The outer envelope must bear the complete name and address of the intended recipient, who must be authorized to access CVI. The second/outer envelope should have no marking that identifies the contents as materials containing CVI.

8.3 CVI in Transit or Use at a Temporary Duty Station

When in transit or in use at a temporary duty station, CVI must:

a. Remain under the control of an authorized person at all time while in transit (e.g., may not be placed in checked baggage).
b. 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 of have access to this information.
c. Be locked in the trunk when traveling by car and when the traveler is away from the vehicle.
d. Be locked in an available and suitable room when in a hotel. The room safe is the preferred method for protecting materials containing CVI while in temporary duty status (*e.g.*, hotel). 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).
e. Always have a cover sheet attached and must not be displayed when the materials containing CVI are not in use.

8.4 Electronic Transmission

Transmittal by Facsimile (Fax)

Unless otherwise restricted by the originator, CVI may be sent via non-secure fax. However, the use of a secure fax machine is highly encouraged. When a non-secure fax is used, the sender will:

a. Confirm that the person receiving the CVI at the other end is an authorized user with a need to know.
b. Coordinate with the recipient to ensure the facsimile number of the recipient is current and valid.
c. Contact the recipient to ensure that the materials faxed will not be left unattended.

d. 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 must immediately notify the sender for disposition instructions.
e. Ensure that the CVI is properly marked in accordance with Appendix E.
f. Verify that the holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

Transmittal via E-Mail

CVI may be transmitted by e-mail, provided that the following conditions are met:

a. 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 under a separate cover. CVI should never be included in the subject or body of an e-mail transmission.
b. In addition, if an encrypted or security communication e-mail system is not available, persons with access to CSAT can upload and download CVI through the encrypted CSCD Web site (*i.e.*, CSAT Web site).
c. Due to inherent vulnerabilities, materials containing CVI shall not be sent to personal e-mail accounts. (See DHS MD 3400, DHS Sensitive Systems Handbook.)

DHS Internet/Intranet

Materials containing CVI information will only be posted on secure sites as specifically authorized by the CSCD Director.

8.5 Telephone

When discussing CVI over a telephone:

a. The use of a Secure Telephone Unit (STU III) or Secure Telephone Equipment (STE), is encouraged, but not required.
b. The risk of interception and monitoring of conversations is greater when using cellular telephones and cordless telephones, which transmit the conversation to a base unit. Individuals needing to discuss CVI by telephone must avoid these devices unless the circumstances are exigent, or the transmissions are encoded or otherwise protected.
c. The caller must ensure that the person receiving the oral CVI is an authorized user.

9.0 Destruction

Materials containing CVI will be destroyed when no longer needed. Methods of destruction include the following:

a. "Hard Copy" materials will be destroyed by crosscut shredding, burning, pulping, and pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of along with normal waste.
b. Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.
c. All information stored in the DHS information collection database will be deleted and destroyed according to processes defined by the DHS IT Security Office.

10.0 Dissemination and Access

These procedures are provisional and will be adjusted based on input provided by a working group comprised of state Homeland Security Advisors and local officials. This document will be updated and a notice will be provided on the CVI webpage at http://www.dhs.gov/chemical security.

10.1 Dissemination and Access – General

All information designated as CVI under the regulations (*e.g.*, only those records specifically listed in Section 27.400(b)(1) through (8) or specifically designated by the Secretary as CVI under Section 27.400(b)(9)) will be originally developed and held by either DHS or regulated chemical facilities. Absent emergency or exigent circumstances, regulated chemical facilities must receive prior written authorization from DHS CSCD Director to disseminate marked CVI to third parties in the private sector. Regulated chemical facilities may share CVI with local and state governments provided these entities have signed a Memorandum of Agreement with CSCD and the recipient has a need to know. Except for non-DHS Federal agencies, any state or local agency recipient of CVI from either DHS CSCD or a regulated chemical facility may not further disseminate CVI beyond the scope of the authorities defined in the Memorandum of Agreement without prior written authorization of CSCD Director. No government official shall disclose CVI in any manner – orally, visually, or electronically – to any unauthorized users without the consent of the Secretary for Homeland Security.

Access to CVI is based upon need to know (See Definition), as determined by the appropriate CVI Security Officer or CVI Point of Contract. When discussing or transferring CVI to another individual(s), the holder of the information must ensure that the individual is an authorized user with a valid need to know. In addition, the holder of the information must ensure the recipient is an authorized user. Any request should be

provided to the CVI Security Officer who will verify the requestor's authorization and determine the requestor's need to know the CVI in question. With approval in hand, the holder of the information should also ensure that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information. The holder of the information will comply with any access and dissemination restrictions associated with any CVI record.

A security clearance is not required for access to materials containing CVI. However, the CSCD Director may require background checks or other verification activities to establish the trustworthiness of any single individual or classes of individuals seeking access to CVI.

Other Federal Law Obligations

Section 550 provides that the chemical security rule "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." Pub. L. No. 109-295, sec. 550(f) (2006). In other words, the chemical security rule does not limit or conflict with any statutory, regulatory, or other obligations a facility may have to the EPA, DOT, DOC, DOL , DOJ, or other Federal agency. We expressed this principle in the IFR at section 27.405(a)(1) and in the preamble (72 FR 17688, 17714).

For example, the Department of Commerce administers the Chemical Weapons Convention Implementation Act (22 USC 6701 et seq.) through its Chemical Weapons Convention Regulations (15 CFR 710-721). The Act and 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 United States. The chemical security rule does not prohibit chemical facilities from complying with these obligations. And these obligations do not require that facilities provide security information constituting Chemical-terrorism Vulnerability Information (CVI) to the OPCW.

To understand why this is so, it is necessary to understand the relationship between information required under statutory, regulatory, and other obligations aside from section 550 and information compiled in a form that constitutes CVI—which has special handling requirements and restrictions on public disclosure under section 27.400 of the IFR. A facility may include information, such as production, use, or trade-related data, required under statutory, regulatory, or other obligations in its Top-Screen (or other documents required under Section 550). When a facility does so, it is the Top-Screen (or other documents required under Section 550) that constitutes CVI. The separate pieces of information by themselves, or compiled for purposes other than the IFR, do not constitute CVI. Accordingly, for example, the IFR does not of its own force prohibit a chemical facility from providing a Chemical Weapons Convention inspector a list of chemicals on-

site, or any other required information, even though that same information may be included in a Top-Screen and the Top-Screen does constitute CVI. Facilities may not, however, disclose information in a form that constitutes CVI to anyone that does not meet the requirements governing CVI as set forth in the IFR.

The following diagram (Figure 1) shows how information may be shared between the Chemical Security Program's stakeholders. Additional diagrams showing how government authorities and chemical facilities will share CVI are found in Appendix G. More detailed discussions are included in each subsection below.

CVI Sharing Model

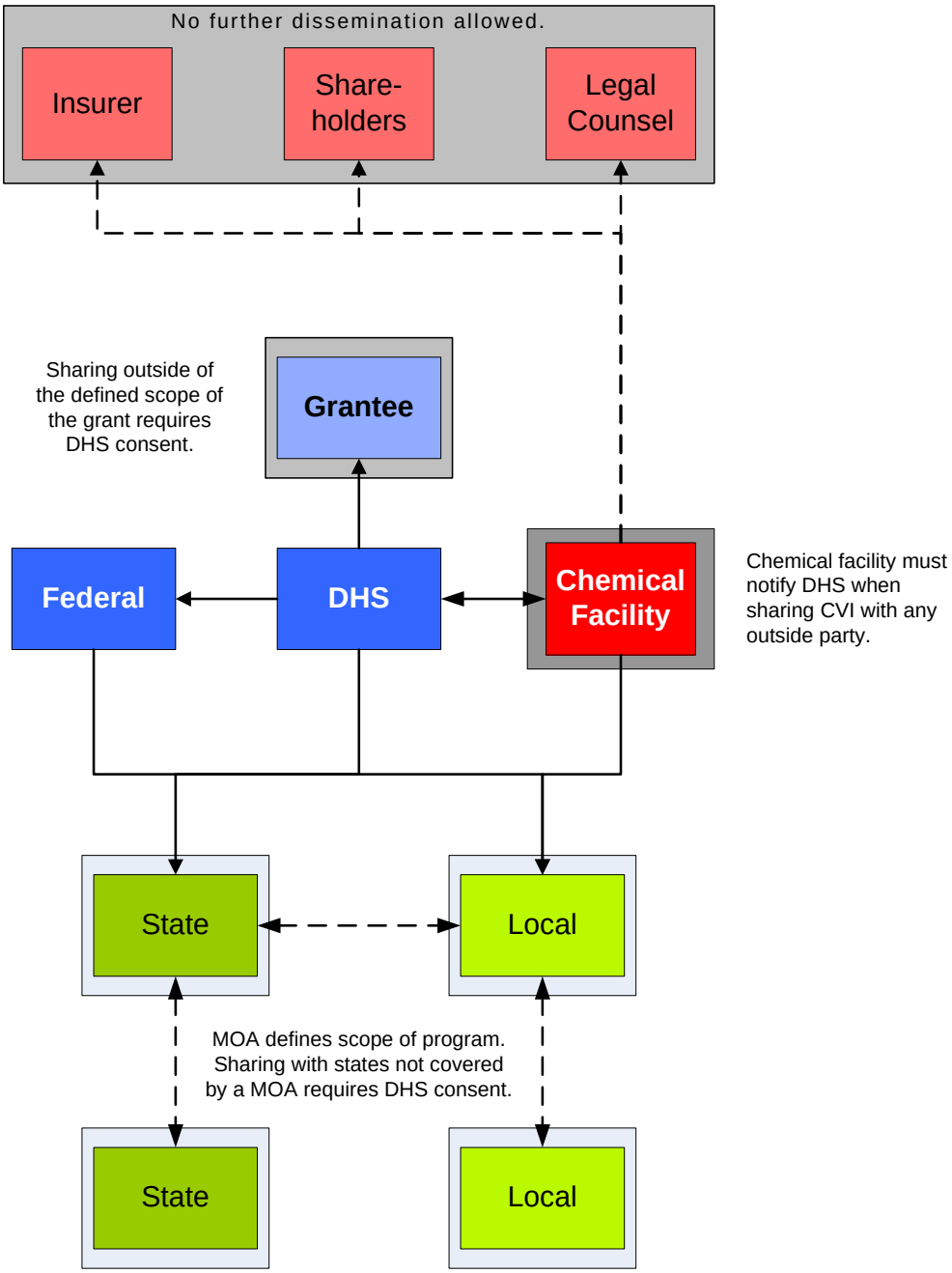


Figure 1. Sharing CVI between Chemical Security Stakeholders

The sharing model makes the following assumptions:

a. Dissemination occurs under normal circumstances—i.e., there are no emergency or exigent circumstances requiring immediate dissemination.
b. All covered persons will have completed training before accessing CVI.

c. All non-federal covered persons will have agreed to the terms of non-disclosure before accessing CVI.
d. CVI will only be shared with individuals that have demonstrated a need to know. For non-DHS employees, need to know will be determined by the appropriate agency CVI Security Officer or CVI Point of Contact.
e. Non-DHS Federal, state and local governments will have entered into a MOA with DHS before CVI access is provided to representatives within their jurisdiction.
f. The CSCD Director may require state and local governments entering into a MOA to describe their background check procedures. The CSCD Director may request additional background checks before access is granted.
g. Other Federal departments and their components may share CVI with state and local government agencies without seeking consent from DHS. However, these Federal officials may only share with other authorized users.
h. State and local governments may only share CVI outside of their jurisdiction, as established in the pertinent MOA, with the prior written authorization from the Assistant Administrator.
i. Regulated chemical facilities may only share CVI with private third parties(i.e., board members, insurers, stockholders) with the prior written authorization from the Assistant Administrator. Third parties receiving CVI from regulated facilities may not share CVI outside the provisions of the NDA executed with the regulated facility.
j. Federal grantees and contractors may only share CVI with the prior written authorization from the Assistant Secretary or the appropriate delegated authority.

Anyone who shares CVI with another person must keep a log of the following data:

- 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; and
- Evidence of receiving prior written authorization from CSCD Director.

Authorized users will be required to keep this record for no less than three years from the date CVI was shared. The CVI Security Officer may ask for this information as part of routine audits and self-inspection activities.

10.2 Dissemination and Access - Non-DHS Federal Agencies

Except in exigent or emergency circumstances, Federal employees or contractors outside DHS seeking access to CVI must complete the following tasks:

a. The person receiving CVI must have homeland security duties and demonstrate a need to know, as determined by the agency CVI Security Officer.

b. The recipient must be covered under the agency MOA.
c. The person receiving the information must complete authorized user training.
d. If the recipient is a Federal contractor, they must meet the requirements set forth in Section 10.3.

10.3 Dissemination and Access – Federal Government Contractors

Companies with Federal government contracts must complete the following tasks before being authorized to receive CVI

a. The pertinent agency CVI Security Officer will certify that the contractor is performing homeland security duties.
b. The contractor must whenever and to whatever extent possible, modify its contract to include a special condition that is substantially similar to the example shown in Appendix D.
c. Each contract employee has completed CVI training.

Each individual covered by the contract must become an authorized user. These requirements include:

a. Completing CVI authorized user training.
b. Executing a NDA and providing a copy to DHS. (See Appendix B.)
c. DHS 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.

After completion of these tasks, any authorized user must still demonstrate a need to know.

Contractors may not disseminate CVI outside the defined scope of their contract. Disclosure of CVI beyond the scope of the contract requires prior written authorization from the Assistant Secretary for Infrastructure Protection.

10.4 Dissemination and Access – State and Local Agencies

DHS intends to enter into a formal Memorandum of Agreement (MOA) with each state before CVI is shared. Appendix C provides an example MOA that lists the responsibilities DHS and states assume. These responsibilities include:

a. Defining the scope of access. DHS would prefer that each MOA cover all state and local entities that may have a need to know CVI.
b. Appointing a CVI Security Officer and a Deputy CVI Security Officer.
c. Define the authorities that a state will use to prosecute a covered person that misuses or mishandles CVI.

Each individual covered by the MOA must become an authorized user. These requirements include:

d. Completing CVI authorized user training.

e. Executing a NDA and providing a copy to DHS. (See Appendix B.)

f. Individuals must submit a written request demonstrating a need to know to the CSCD Security Officer for CVI held by DHS. The CVI Security Officer will confirm the person's need to know.

g. DHS 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.

For state and local government authorities limits on sharing CVI include:

a. The CVI Security Officer must notify CSCD if CVI is shared with another state.

b. State and local government authorities must seek consent of the CSCD Director to share CVI with states not covered by a MOA.

c. State and local government contractors are prohibited from sharing CVI with chemical facility representatives.

d. State and local government authorities and contractors may not disclose CVI to private third parties.

10.5 Dissemination and Access – Regulated Chemical Facilities

Except in exigent or emergency circumstances, regulated chemical facilities will only further disseminate and provide access to CVI to authorized users who have completed the following tasks:

a. The person receiving CVI must have homeland security duties and demonstrate a need to know.
b. The person receiving the information must complete authorized user training.
c. The person must enter into a NDA similar to that found in Appendix B, which limits further dissemination of CVI.
d. If the person is not an employee, contractor, or member of the corporate board of directors of the regulated facility (e.g., a private third party), the chemical facility is required to notify the CSCD Director. Any recipient must complete training and sign a NDA. These private third parties are prohibited from disseminating further CVI in their possession.
e. Chemical facilities must provide notice to the CSCD Director before sharing CVI with any state or local government authority.

10.6 Dissemination and Access – Derivative Products

Authorized users may develop analytical products that are derived from CVI. Derivative products include:

a. Work products containing CVI
b. Classified products containing CVI.

An authorized entity's CVI Security Officer/Point of Contact is responsible for overseeing the use of CVI in derivative products. Work products containing CVI verbatim are subject to the same handling, storage, and marking requirements as original CVI.

Wherever CVI is paraphrased in an analytical product and the paraphrased information may reveal the source of the submission (*e.g.*, naming the particular facility name or asset that would reveal the submitter's identity) or the critical infrastructure/asset, it must be handled in the same manner as CVI.

Authorized users are responsible for seeking guidance from their respective CVI Security Officers or CVI Points of Contact regarding whether a derivative product has been sufficiently marked or sanitized (if needed), and what the appropriate dissemination is for a particular product. CVI Security Officers or CVI Points of Contact may seek guidance from the CSCD CVI Security Officer.

10.6.1 Dissemination and Access – Unclassified Products

The CVI Security Officer for any entity using CVI must ensure that documents prepared under its purview are reviewed and processed in accordance with this guidance regarding derivative products. In cases where the CVI maintains its integrity and/or can be associated with the source of the information, the derivative products must be labeled and handled as CVI.

In the case of information that is both CVI and has been designated as critical infrastructure information under Section 214 of the Homeland Security Act, any covered person in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under Section 214 and any implementing regulations.

10.6.2 Dissemination and Access – 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.

CVI contained in classified documents retains its marking and does not lose its protection even if the document is subsequently declassified. As with unclassified products containing CVI, any entity generating such products is responsible for ensuring that products derived from CVI are labeled and handled appropriately.

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. (See Appendix E for details regarding marking classified products containing CVI.) The CVI markings will 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 shall be so portion marked. CVI commingled with classified information must comply with all safeguarding requirements of both:

- CVI; and
- The highest level of classified designation within the product, as prescribed in Executive Order 12958 (as amended) and its implementing directives 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.

10.7 Dissemination and Access – DHS Advisories, Alerts, and Warnings

If DHS uses CVI to prepare advisories, alerts, and warnings regarding potential threats and vulnerabilities to critical infrastructure for dissemination to the private sector, the general public, or foreign governments, the entity producing such a derivative product must sanitize it. For the purposes of the CVI Program, "sanitization" means distilling the information in a manner to render it untraceable to the submitter and that it does not reveal any information that:

- Exposes vulnerabilities of identifiable critical infrastructure or protected systems;
- Is proprietary, business-sensitive, or trade secret;
- Relates specifically to the submitting person or entity (explicitly or implicitly); or
- Is otherwise not appropriately in the public domain.

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

10.8 Dissemination and Access – 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.

Information relating to security measures is typically not considered CVI if the information is customarily found in the public domain. However, the fact that the information has appeared publicly does not render the information ineligible for designation as CVI. Therefore, any questions raised about the accuracy, designation, or technical merit of such information in the public domain should be responded to in a "no comment" manner; that is, the DHS will neither confirm nor deny the presence of CVI. Such information in the public domain should not be acknowledged by authorized persons as CVI and is covered by a "no comment" policy.

10.9 Dissemination and Access – Automated Information Systems

Much of the information designated as CVI will reside in automated information systems that allow for the safe storage of CVI and also provide facilitated access to this information. First, any system storing CVI must meet the DHS standards for storing sensitive but unclassified information as defined in the DHS Security Manual -- 4300A. Federal government agencies should follow the Federal Information Processing Standards Publication – *Minimum Security Requirements for Federal Information and Information Systems* (FIPS 200). The National Institute of Standards and Technology has also published the Guide for the Security Certification and Accreditation of Federal Information Systems. Both publications are found at http://csrc.nist.gov. State and local government agencies must demonstrate that their information security procedures are compatible and no less stringent than those defined in this publication.

Before an automated information system can receive, store, and provide access to CVI, the CSCD CVI Security Officer will determine if this system meets the stated requirements. In general, these systems must have controls that allow only CVI authorized users with an established need to know the opportunity to access CVI. The appropriate CVI Security Officer will determine an individual's need to know before access is provided. Once this action is completed, the authorized user will have on-going access to CVI stored on this automated information system until the appropriate CVI Security Officer determines that a need to know no longer exists.

Also, all automated information systems must have the ability to created audit logs. These logs must record at least the following information:

- Time of access;
- Identity of person accessing CVI;
- What information was accessed; and
- Whether the information was viewed or downloaded.

System to system transfer of CVI may only be established with the consent of the CSCD Director. Consent will depend on each system's demonstrated compliance with DHS information security requirements or an equivalent standard.

10.10 Dissemination and Access – Emergency or Exigent Circumstances

In the event of emergency or exigent circumstances (see definition above), dissemination or access to CVI can be granted without meeting the provisions of this section, provided that a record is kept and immediately submitted to the CSCD CVI Security Officer (*e.g.*, within less than 24 hours). The record must include:

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

Within five (5) business days following receipt of notice of emergency or exigent dissemination/access being granted, the CSCD CVI Security Officer will contact the recipient to ensure that the recipient meets all of the requirements for an authorized user.

10.11 Dissemination and Access – Objections, Appeals and Administrative or Civil/Criminal Judicial Proceedings

All requests for CVI for the purpose of objections, appeals, or civil/criminal judicial proceedings will be coordinated through the Assistant Secretary, Adjudicating Official or Office of the General Counsel.

10.12 Freedom of Information Act (FOIA) Requests

Under Section 550 of PL 109-295, and the implementing regulations, notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, 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.

FOIA requests for materials containing CVI are to be processed by the DHS Infrastructure Protection Disclosure Officer, with exceptions made for any decision to release materials containing CVI that must have the concurrence of the CSCD Director.

As per current law, no law, regulation, or administrative action of a state or political subdivision thereof, or any decision or order rendered by a court under state law, shall

have any effect if such law, regulation, or decision conflicts with, hinders, poses an obstacle to or frustrates the purposes of this regulation or of any approval, disapproval or order issued there under. Therefore, requests for information that are addressed to covered persons, under state and local freedom of information or open records laws, should be referred to the DHS Preparedness National Protection and Programs Directorate Disclosure Office.

All CVI is protected from disclosure, however, for other work products (*e.g.*, derivative products), DHS will work with such affected entities to determine what records or portions of records should remain undisclosed and what may be released.

If a record contains both information that may not be disclosed under Section 550 of PL 109-295 and information that may be disclosed, the latter information will be provided in response to a FOIA request, provided that the record is not otherwise exempt from disclosure under FOIA and if it is practical to redact the requested information from the record. If it is not practical to do so, the entire record will be withheld from public disclosure.

11.0 Incident Reporting

The loss, compromise, suspected compromise, or unauthorized disclosure of materials containing CVI will be reported to the CVI Security Officer or coordinator for the entity holding the CVI. Suspicious or inappropriate requests for information by any means (*e.g.*, e-mail or verbal) shall be reported to the CVI Security Officer or coordinator for the entity holding the CVI.

Any loss, compromise, suspected compromise, unauthorized disclosure or suspicious or inappropriate requests for CVI that are verified by the CVI Security Officer for the entity holding the CVI must be reported to the CSCD CVI Security Officer within one working day. CSCD will coordinate any response with the DHS Office of General Counsel. The CSCD CVI Security Officer will provide notification to the originator of the CVI for verified incidents of unauthorized disclosure.

Incidents involving materials containing CVI in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center (CSIRC) in accordance with IT incident reporting requirements.

Additional notifications to appropriate DHS management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.

At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and effect of the incident and the appropriateness of administrative or disciplinary action against the offender.

APPENDIX A: Unique CVI Record Tracking Number

X = Facility ID number created by CSAT

Unique CVI Record Tracking Numbering		
Unique Number	**Type of CVI**	**Reference**
X.001	Top Screen from Chemical Self Assessment Tool (CSAT)	27.200
X.002	Initial determination by Assistant Secretary that a chemical facility presents a high level of security risk	27.205(a)
X.003	Request for re-determination	27.205(b)
X.003	Objection to an initial determination	27.205(c)
X.004	Final determination on security risk	27.205(c)
X.005.01	Security Vulnerability Assessment (SVA) (subsequent filings will have consecutive sub-numbers)	27.210(a)
X.005.01	Alternative Security Plan (ASP) (when accepted and completed, the ASP will be the facility's SVA)	27.210(b)
X.006.01	Site Security Plan (SSP) (subsequent filings will have consecutive sub-numbers)	27.210(a)
X.007	Notice of Placement in a Risk Tier	27.220
X.005.01.01	Letter approving SVA (subsequent filings will have consecutive sub-numbers)	27.240(a)
X.005.01.02	Notice of Deficiency for SVA (subsequent filings will have consecutive sub-numbers)	27.240(b)
X.006.01.01	Letter of Authorization for SSP	27.242(a)
X.006.01.02	Letter of Approval for SSP	27.242(a)
X.006.01.03	Notice of Deficiency for SSP	27.242(b)
X.008	Inspection Findings/Correspondence	27.245(b)
X.009.01	Training Records	27.250(a)(1)
X.009.02	Exercise and Drill Records	27.250(a)(2)
X.009.03	Incidents and breaches of security	27.250(a)(3)
X.009.04	Maintenance, calibration, and testing of security equipment	27.250(a)(4)
X.009.05	Security Threats	27.250(a)(5)
X.009.06	Audit Record	27.250(a)(6)
X.010	Sensitive correspondence between regulated facility and DHS	27.250(b)
X.011	Order of Compliance as describes actions for coming into compliance	27.300(b)
X.012	Responses to Compliance Orders	27.300(c)
X.013	Objections	27.317
X.014	Appeals	27.320
X.015	Other	

APPENDIX B: Individual Non-Disclosure Agreement

This document provides the official DHS Non-Disclosure Agreement (NDA). Federal employees are covered by their terms of employment not to disclose any Sensitive But Unclassified information and will not be required to sign this document before accessing CVI. All state, and local government employees, contractors, or grantees must sign this agreement before access is provided. Chemical facilities may develop a similar NDA for their use.

Individuals required to sign the following NDA include:

- Federal contractors (including FFRDCs), subcontractors, and consultants;
- Federal government grantees:
- State and local government employees;
- State and local government contractors, subcontractors, and consultants;
- State and local government grantees;

DEPARTMENT OF HOMELAND SECRUITY
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 and 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 and 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 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.
(c) If the Authorized Entity is a state or local agency or regulated facility contractor performing services in support of the Chemical Security Compliance Program, I will not request, obtain, maintain, or use CVI unless the appropriate CVI Security Officer or CVI Point of Contract (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:

APPENDIX C: Memoranda of Agreement

Before being given access to CVI, non-DHS Federal, State, and Local government entities must sign a Memorandum of Agreement (MOA) with the CSCD. DHS intends to sign a single MOA with each state that will cover all state and local authorities that may seek access to CVI. Because requirements for Federal government entities are different than those for state and local government entities, separate MOAs are provided in this Appendix.

Please do not use the MOA provided here as an official MOA. Instead, please contact the CSCD CVI Security Officer to initiate the process for developing an MOA between the government authority and CSCD..

Department of Homeland Security Memorandum of Agreement with Insert Federal Agency Here for Access to Chemical-terrorism Vulnerability Information (CVI)

[Please do not use the MOA provided here as an official MOA. Please contact the CSCD CVI Security Officer to begin development of a MOA specific to your department or agency.]

1. **Parties.** The parties to this Memorandum of Agreement (MOA) are the Department of Homeland Security, through its Chemical Security Compliance Division (hereinafter referred to as "DHS CSCD"), and the officials, persons, parties, offices, or governmental divisions designated to access and receive CVI as listed in Attachment A (hereinafter referred to as "the Recipient").

2. **Purpose.** The purpose of this MOA is to set forth the agreed terms and conditions under which DHS will provide CVI to the Recipient.

3. **Authorities.** DHS is authorized to enter this MOA under Section 550 of PL 109-295.

4. **Background**. 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) establishes the statutory requirements for the submission and protection of information submitted pursuant to that section. Section 550 provides that:

> [I]nformation developed under this section, including vulnerability assessments, site security plans, and other security related information, records, and documents shall be given protections from public disclosure consistent with similar information developed by chemical facilities subject to regulation under section 70103 of title 46, United States Code: Provided, That this subsection does not prohibit the sharing of such information, as the Secretary deems appropriate, with state and local government officials possessing the necessary security clearances, including law enforcement officials and first responders, for the purpose of carrying out this section, provided that such information may not be disclosed pursuant to any state or local law: Provided further, That in any proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this section, and related vulnerability or security information, shall be treated as if the information were classified material.

The Procedures Manual entitled, *Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information (CVI)* provides further detailed guidance, and requires that Federal agencies that obtain CVI from the DHS CSCD enter into an MOA. This MOA fulfills that requirement.

5. Responsibilities.

A. DHS will:

(i) Provide access to CVI to the Recipient for the purposes and under the conditions outlined in this MOA;
(ii) Train the Recipient's CVI Security Officer(s) and be available for consultation and guidance.

B. The Recipient will:

(i) Warrant and agree that all employees covered by the scope of this MOA employees and contractors who will have access to CVI are familiar with, will be trained in, and will comply with, the statutes, regulations, and rules that address CVI set forth in the Procedural Manual, and other relevant guidance issued by the DHS CSCD, and will periodically check such guidance for updates and amendments;
(ii) Use any CVI provided to it only for the purposes set forth Section 550 of PL 109-295 and will not use CVI as a substitute for the exercise of its own legal authority to compel access to or submission of that same information, and further, will not use CVI for regulatory purposes beyond the scope of Section 550 PL 109-295 without the consent of the Secretary of DHS or his designee;
(iii) Designate a CVI Security Officer and Deputy CVI Security Officer), who each may be asked to submit to a background investigation. Both shall be familiar with and trained in the responsibilities overseeing the use and dissemination of CVI as set forth in Section 550 of PL 109-295 and the accompanying Procedural Manual, and any other guidance issued by DHS. The Security Officer will be responsible for determining need to know for all persons covered by this Agreement.
(iv) Upon request from DHS, immediately take such steps as may be necessary to return promptly all CVI, including copies, however made, to DHS;
(v) Consider any violations of procedures regarding CVI as matters subject to rules of conduct (including sanctions) that apply to its employees, and will refer violations of Section 550 or other applicable law to appropriate authorities for prosecution;
(vi) Immediately report all compromises of CVI and violations of applicable procedures to the DHS CSCD CVI Security Officer and cooperate with any investigation that may be initiated;
(vii) Ensure that information it receives from DHS that is marked "**CHEMICAL–TERRORISM VULNERABILITY INFORMATION**." is accessed only by those persons covered by this Agreement and have a need to know as determined by the CVI Security Officer;
(viii) Not further disclose CVI to any unauthorized person without the prior approval of the CSCD Director;
(ix) Fully comply with any requests or visits, whether scheduled or unscheduled, by the CSCD CVI Security Officer or his/her designee, to review the

Recipient's compliance with the terms of this MOA, and will take any corrective action recommended; and

(x) Notify and coordinate with DHS CSCD prior to responding to any requests for release of CVI under a court order, agency decision, the Freedom of Information Act, or any other statute or regulation.

(xi) Ensure all IT systems and media used to handle, store, or transmit materials containing CVI are in compliance with the requirements of the CVI Procedural Manual and all other requirements set forth herein.

(xii) Consider any violations of procedures regarding CVI as matters subject to rules of conduct (including sanctions) and will refer violations of law to appropriate authorities for prosecution;

6. **Amendments.** This MOA is required by the CVI Procedural Manual. Should there be a change in that manual DHS will require conforming amendments to this MOA. Otherwise, no amendments are permitted.

7. **Reimbursables.** This MOA does not provide authority for any reimbursable expenditure, or funding. In the event that such authorization is required, DHS and the Recipient will, in a separate agreement, coordinate funding reimbursement through appropriate channels and will execute appropriate Reimbursable Agreements or other funding documents in accordance with the Economy Act and DHS procedures for such agreements including an Economy Act Determination and Findings.

8. **Other Provisions.** Nothing in this MOA is intended to conflict with current law or regulation. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

9. **Effective Date and Termination Provisions.** This MOA is effective as of the date of the last required signature. It continues until terminated in writing by either party. It may be terminated effective upon the delivery by any means of written notice of termination signed by an authorized official. Unwillingness by the Recipient to agree to amendments required by DHS will constitute a basis for termination. If terminated, the Recipient agrees to promptly return all CVI that it has received to the DHS CSCD CVI Security Officer.

10. **Original Memorandum of Agreement.** The original of this document will be kept by the DHS CSCD CVI Security Officer. Copies may be made as necessary.

Agreed to and Accepted By:

Name Date	Name Date
Name of DHS Signatory	Name of Federal Agency Signatory
Title	Title
Component	Agency Component
Department of Homeland Security	Federal Agency

CVI Security Officers

Department of Homeland Security	**Recipient Agency**
Name of CSCD Security Officer	Name of Federal Agency Security Officer
Title	Title
Component	Agency Component
Department of Homeland Security	Federal Agency

Department of Homeland Security Memorandum of Agreement with Insert State Name Here for Access to Chemical-terrorism Vulnerability Information (CVI)

[Please do not use the MOA provided here as an official MOA. Please contact the CSCD CVI Security Officer to begin development of a MOA specific to your department or agency.]

1. **Parties.** The parties to this Memorandum of Agreement (MOA) are the Department of Homeland Security, through its Chemical Security Compliance Division (hereinafter referred to as "DHS CSCD"), and the officials persons, parties, offices, or governmental divisions designated to access and receive CVI as listed in Attachment A (hereinafter referred to as "the Recipient").

2. **Purpose.** The purpose of this MOA is to set forth agreed terms and conditions under which DHS will provide CVI to the Recipient.

3. **Authorities.** DHS is authorized to enter this MOA under Section 550 of PL 109-295.

4. **Background**. 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) establishes the statutory requirements for the submission and protection of information submitted pursuant to that section. Section 550 provides that:

> [I]nformation developed under this section, including vulnerability assessments, site security plans, and other security related information, records, and documents shall be given protections from public disclosure consistent with similar information developed by chemical facilities subject to regulation under section 70103 of title 46, United States Code: Provided, That this subsection does not prohibit the sharing of such information, as the Secretary deems appropriate, with state and local government officials possessing the necessary security clearances, including law enforcement officials and first responders, for the purpose of carrying out this section, provided that such information may not be disclosed pursuant to any state or local law: Provided further, That in any proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this section, and related vulnerability or security information, shall be treated as if the information were classified material.

The Procedures Manual entitled, *Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information (CVI)* provides further detailed guidance, and requires that Federal agencies that obtain CVI from the DHS CSCD enter into an MOA. This MOA fulfills that requirement.

5. Responsibilities.

A. DHS will:

(i) Provide access to CVI to the Recipient for the purposes and under the conditions outlined in this MOA; and
(ii) Train the Recipient's CVI Security Officer(s) and be available for consultation and guidance.

B. The Recipient will:

(i) Warrant and agree that each of its employees and contractors who will have access to CVI has signed an individual non-disclosure agreement approved of, or provided by, DHS, and is familiar with, will be trained in, and will comply with, the statutes, regulations, and rules that address CVI set forth in Section 550 of PL 109-295 and the accompanying Procedures Manual, and other relevant guidance issued by the CSCD, and will periodically check such guidance for updates and amendments;
(ii) Use any CVI provided to it only for the purposes set forth in Section 550 of PL 109-295 and will not use CVI as a substitute for the exercise of its own legal authority to compel access to or submission of that same information, and further, will not use CVI for regulatory purposes without first contacting the DHS CSCD;
(iii) Designate a CVI Security Officer and Deputy CVI Security Officer), who each may be asked to submit to a background investigation to determine eligibility and suitability for access to CVI, or have a current SECRET or higher security clearance. Both shall be familiar with and trained in the responsibilities overseeing the use and dissemination of CVI as set forth in Section 550 of PL 109-295 and the accompanying Procedural Manual, and any other guidance issued by DHS. The Security Officer will be responsible for determining need to know for all persons covered by this Agreement.
(iv) Upon request, immediately take such steps as may be necessary to return promptly all CVI, including copies, however made, to DHS;
(v) Consider any violations of procedures regarding CVI as matters subject to rules of conduct (including sanctions) that apply to its employees, and will refer violations of law to appropriate authorities for prosecution;
(vi) Immediately report all compromises of CVI and violations of applicable procedures to the DHS CSCD CVI Security Officer and cooperate with any investigation that may be initiated;
(vii) Ensure that information it receives from DHS that is marked "CHEMICAL–TERRORISM VULNERABILITY INFORMATION" is accessed only by those persons covered by this Agreement and have a need to know this information as determined by the Security Officer;
(viii) Not further disclose CVI to authorized persons covered by this Agreement without the consent of the CVI Director. Not further disclose CVI to other authorized users outside the scope of this Agreement without the consent of

the CSCD Security Officer. Not further disclose CVI to any unauthorized person without the prior approval of the CSCD Director;

(ix) Fully comply with any requests or visits, whether scheduled or unscheduled, by the DHS CSCD CVI Security Officer or his/her designee, to review the Recipient's compliance with the terms of this MOA, and will take any corrective action recommended; and

(x) Notify and coordinate with DHS prior to responding to any requests for release of CVI under a court order, agency decision, state or local laws requiring the disclosure of information or records, or any other statute or regulation.

(xi) Ensure all IT systems and media used to handle, store, or transmit materials containing CVI are in compliance with the requirements of the CVI Procedural Manual and all other requirements set forth herein.

(xii) Consider any violations of procedures regarding CVI as matters subject to rules of conduct (including sanctions) and will refer violations of law to appropriate authorities for prosecution;

6. Amendments. Should there be a change in either the DHS CVI Procedures Manual, DHS will require conforming amendments to this MOA. Otherwise, no amendments are permitted.

7. Reimbursables. This MOA does not provide authority for any reimbursable expenditure, or funding.

8. Other Provisions. Nothing in this MOA is intended to conflict with current law or regulation. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

9. Effective Date and Termination Provisions. This MOA is effective as of the date of the last required signature. It continues until terminated in writing by either party.

It may be terminated effective upon the delivery by any means of written notice of termination signed by an authorized official. Unwillingness by the Recipient to agree to amendments required by DHS will constitute a basis for termination. If terminated, the Recipient agrees to promptly return all CVI that it has received to the DHS CSCD CVI Security Officer.

10. Original Memorandum of Agreement. The original of this document will be kept by the DHS CSCD CVI Security Officer. Copies may be made as necessary.

Please do not use the MOA provided here as an official MOA. Instead, please contact the DHS CSCD CVI Security Officer for an individualized MOA for signature.

Agreed to and Accepted By:

Name Date	Name Date
Name of DHS Signatory	Name of State Agency Signatory
Title	Title
Component	Agency Component
Department of Homeland Security	Federal Agency

CVI Security Officers

Department of Homeland Security	**Recipient Agency**
Name of CSCD Security Officer	Name of State CVI Security Officer
Title	Title
Component	Agency Component
Department of Homeland Security	Federal Agency

Attachment A

Defined Scope of the Memorandum of Agreement (pick one)

☐ Statewide

☐ State government only

☐ Specific components of state government

☐ Regional or metropolitan authority

☐ Single local government

Identify the authority responsible for use and appropriate safeguarding of Chemical-terrorism Vulnerability Information (CVI). This authority will be represented by the signatory to the MOA. The signatory will appoint a CVI Security Officer to oversee the safeguarding of CVI including the determination of need to know for authorized users covered under the scope of this MOA.

APPENDIX D: Contract Language

Government officials must include to whatever extent possible the following special condition on all contracts that may result in the contract employees having access to CVI. Regulated Facilities should include a similar condition in all contracts that may result in the contract employees in having access to CVI. This condition is not a prerequisite for access but must be accomplished whenever and to whatever extent possible.

APPROVED CONTRACT LANGUAGE

The Contractor shall not request, obtain, maintain or use CVI without a prior written certification from the DHS CSCD CVI Security Officer.

The Contractor shall comply with all requirements of Section 550 of PL 109-295, any properly promulgated implementing regulations, and in the DHS Procedures Manual as they may be amended from time to time, and shall safeguard CVI in accordance with the procedures contained therein.

The Contractor shall ensure that each of its employees, consultants, and subcontractors who access CVI have executed NDAs in a form prescribed by the Department's CVI Security Officer. The Contractor shall ensure that each of its employees, consultants and subcontractors has executed an NDA and agrees that none of its employees, consultants or sub-contractors will be given access to CVI without having previously executed an NDA and understand the requirements for safeguarding CVI as documented in the CVI Procedural Manual.

APPENDIX E: Marking CVI

For all paper records containing CVI, mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of— (i) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover; (ii) Any title page; and (iii) 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 the case of non-paper records that contain CVI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously 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.

CVI contained on electronic and magnetic media must have protective markings and the distribution limitation statement applied at the beginning and end of the electronic and magnetic text. The protective marking and distribution limitation statement must be displayed in such a manner that both are fully visible on the screen or monitor when the text is viewed. Electronic submissions, electronic copies of information in the CSAT or other DHS-approved information collection tool, and electronic copies of CVI that are disseminated will have an electronic watermark applied to them to identify them as CVI. All electronic storage devices (*e.g.*, external hard drives or thumb drives) that contain CVI will be marked with the protective marking. The protective marking and distribution limitation statement must 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 must, if possible, be included in the introduction and at the end of this text.

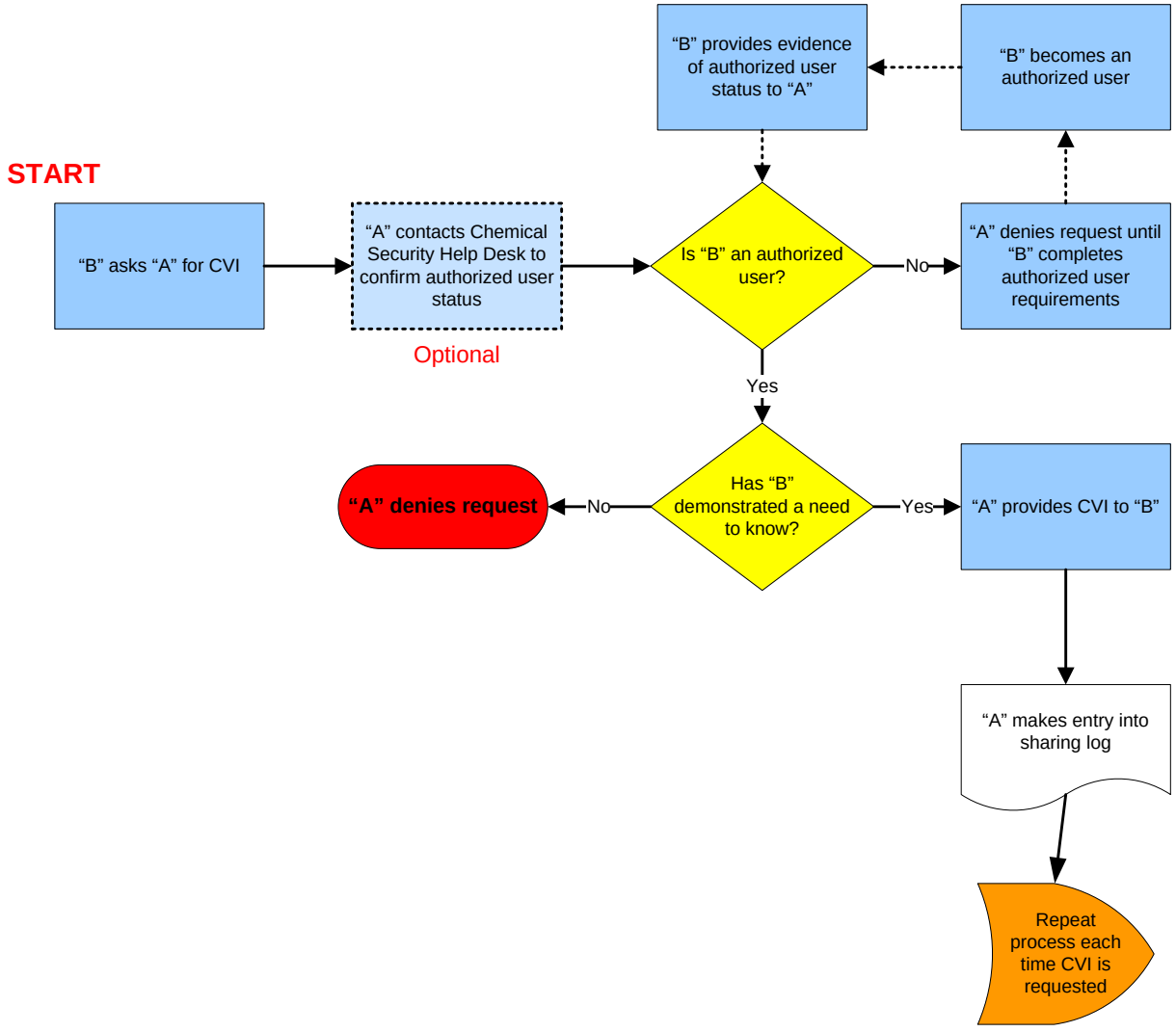
APPENDIX F: Flowcharts for Sharing CVI

Process for Sharing CVI within DHS

CSCD will not require DHS components to sign a formal agreement prior to accessing CVI. Need to know determinations will be made by the person holding the information when shared internally within DHS. Contractors may determine need to know only within the scope of their contract. Under these conditions CVI may be shared without the consent of the CVI Security Officer. These same conditions apply to grantees.

Different Sharing Conditions

DHS employee to DHS employee
DHS employee to DHS contractor
DHS contractor to DHS employee
DHS contractor to DHS contractor
DHS employee to DHS grantee

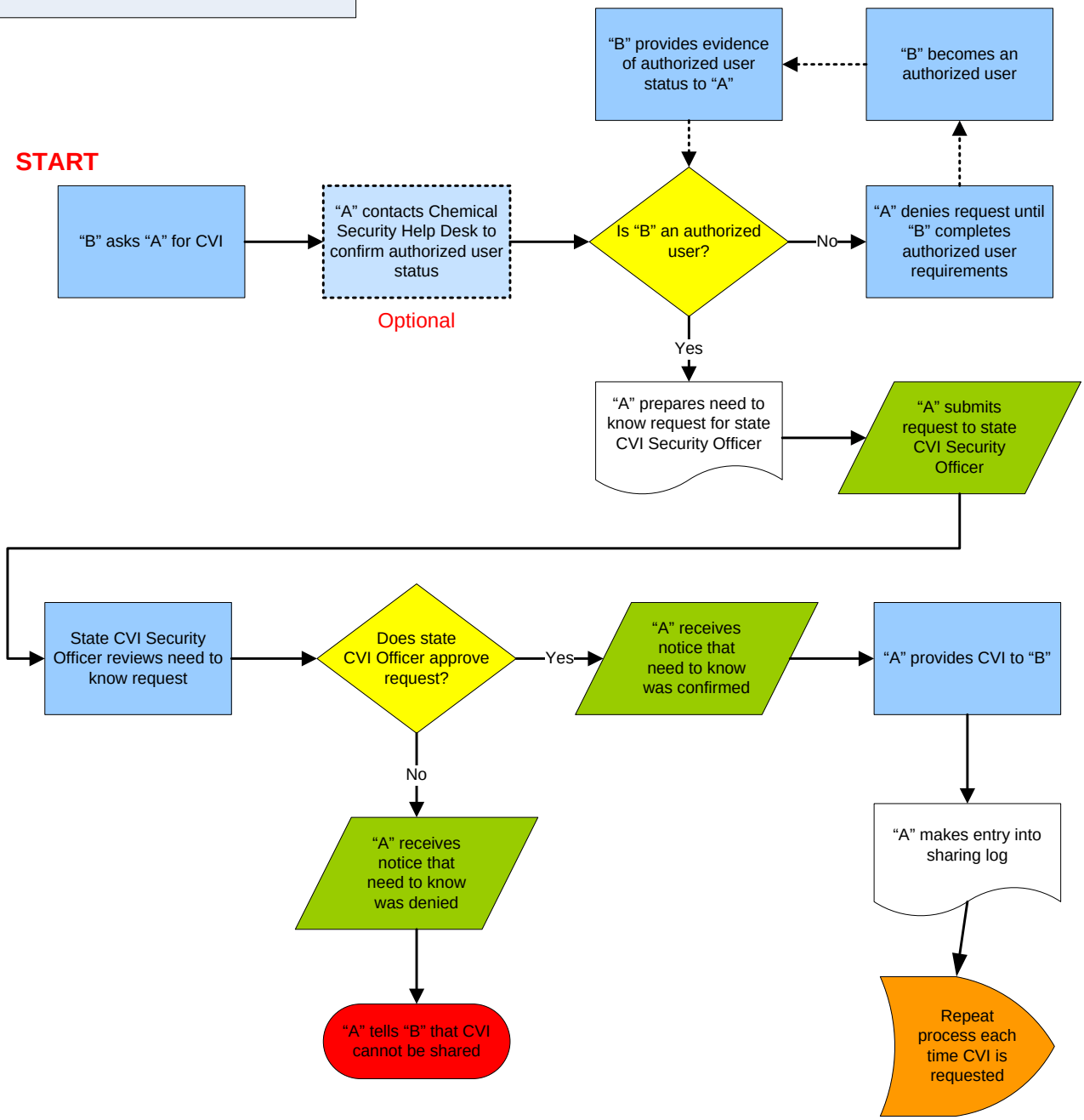


Process for Sharing CVI within the Scope of a State Memorandum of Agreement

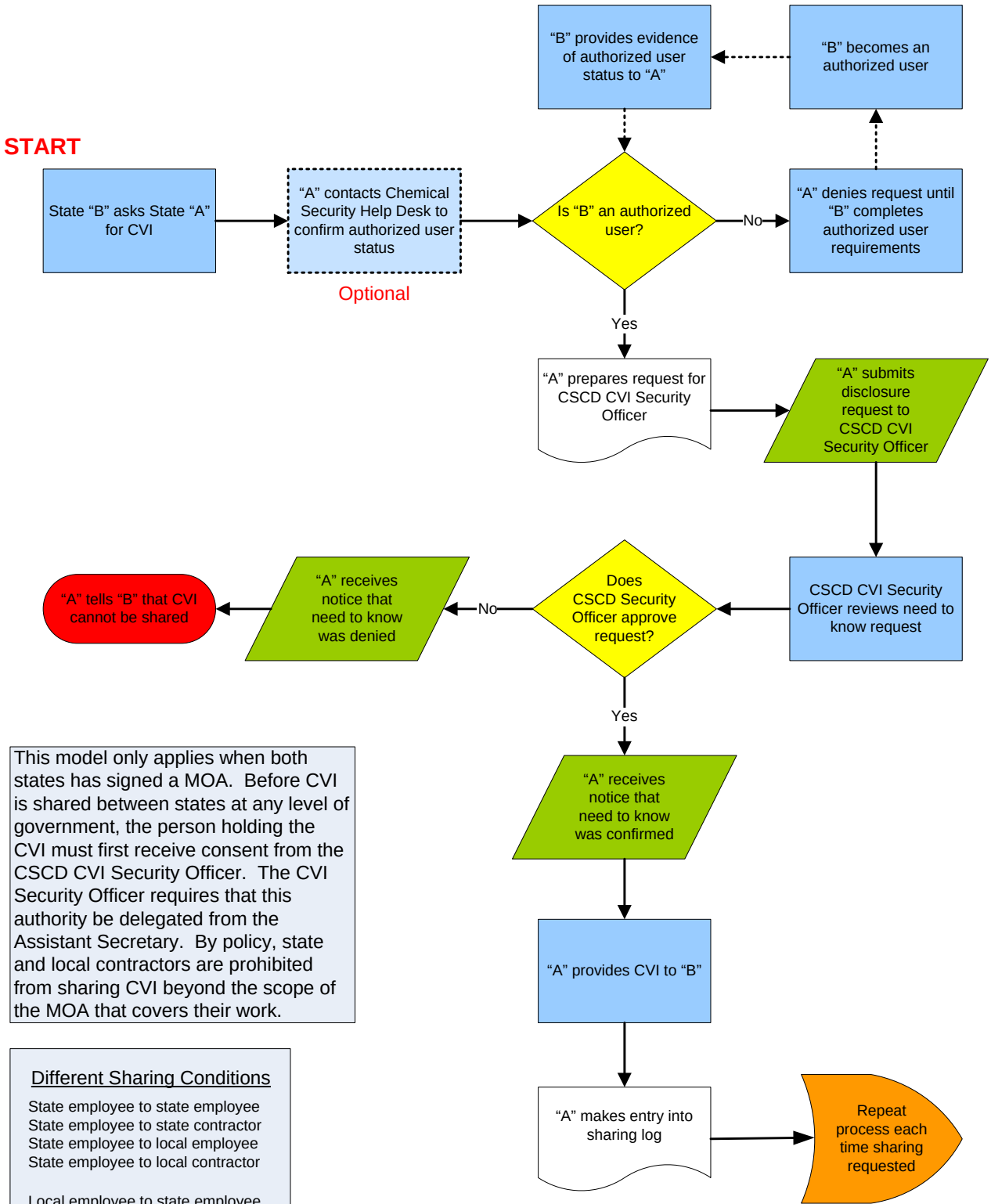
CSCD general policy is to sign MOAs with the state offices of homeland security. The proposed scope of state MOAs will include all state components and local jurisdictions. This approach allows all authorized users covered by the MOA to share CVI without seeking consent from CSCD. The state CVI Security Officer will determine need to know on all information requests.

Different Sharing Conditions

State employee to state employee	State employee to local employee
State employee to state contractor	State employee to local contractor
State contractor to state employee	State contractor to local employee
State contractor to state contractor	State contractor to local contractor
Local employee to state employee	Local employee to local employee
Local employee to state contractor	Local employee to local contractor
Local contractor to state employee	Local contractor to local employee
Local contractor to state contractor	Local contractor to local contractor



Process for Sharing CVI between States



This model only applies when both states has signed a MOA. Before CVI is shared between states at any level of government, the person holding the CVI must first receive consent from the CSCD CVI Security Officer. The CVI Security Officer requires that this authority be delegated from the Assistant Secretary. By policy, state and local contractors are prohibited from sharing CVI beyond the scope of the MOA that covers their work.

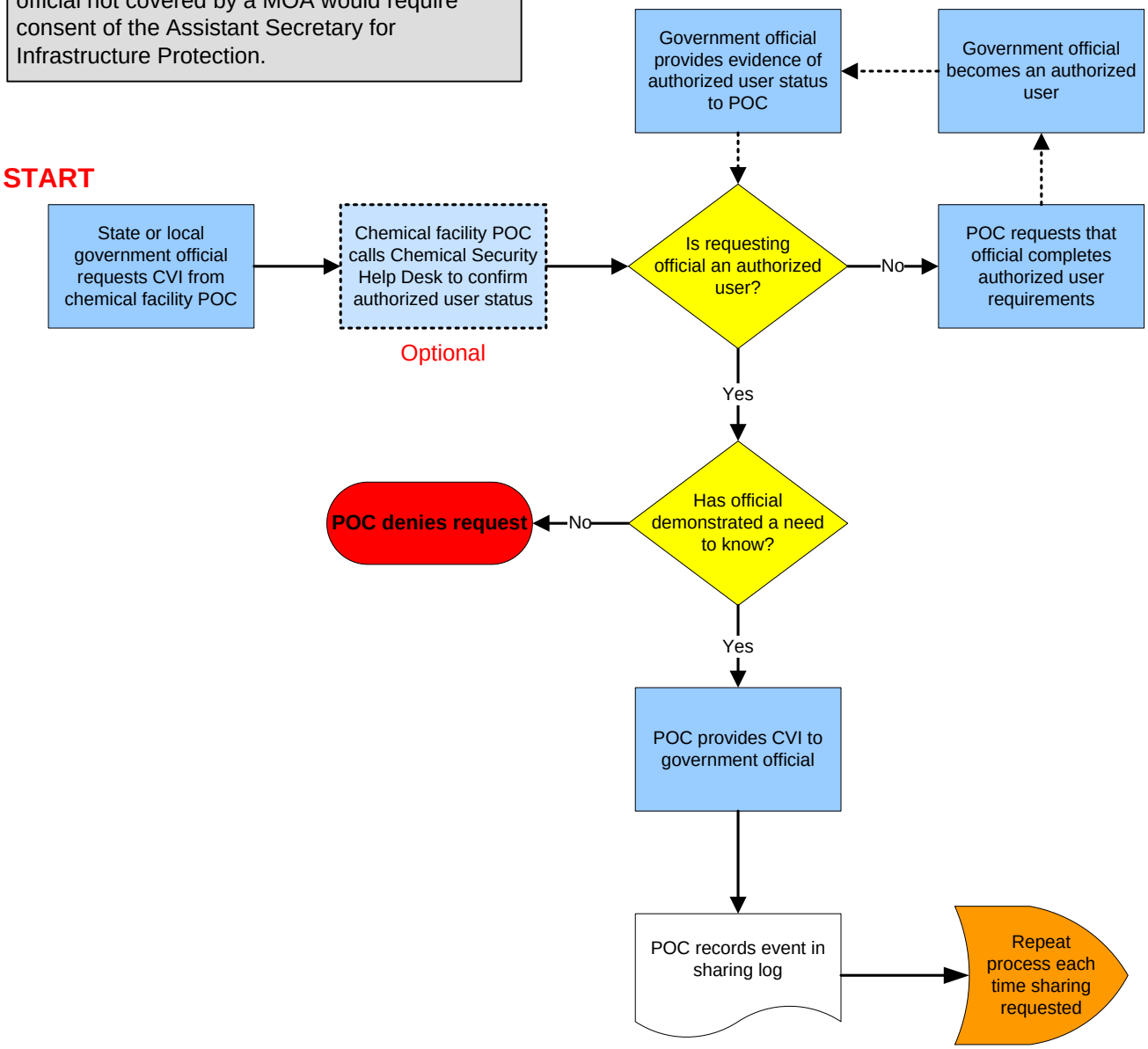
<u>Different Sharing Conditions</u>

State employee to state employee
State employee to state contractor
State employee to local employee
State employee to local contractor

Local employee to state employee
Local employee to state contractor
Local employee to local employee
Local employee to local contractor

Process for State and Local Officials Requesting CVI from Chemical Facilities

Chemical facilities may only share with state and local government officials covered by a MOA. Disclosure to any state or local government official not covered by a MOA would require consent of the Assistant Secretary for Infrastructure Protection.



APPENDIX G: Front and Back Cover for Material Containing CVI

The following page format will be used for both the front and back cover of any material containing CVI.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION
Requirements for Use

Nondisclosure

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

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

- Government officials and contractors must be covered by a Memorandum of Agreement signed with the Chemical Security Compliance Division
- All individuals must complete CVI Authorized User Training
- All individuals must demonstrate a valid need-to-know for specific CVI. For state and local officials this determination will be made by the state CVI Security Officer

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 an eligible individual who meets the access requirements listed above. In all cases, 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: 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: 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 Unit/Equipment. 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 document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized 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 appropriately found in the public domain.

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 on the bottom. 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 endnote.

Tracking Number:

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

Version 1.0 (effective 6/2007)