



## Introduction to Chemical-terrorism Vulnerability Information (CVI)

- The information contained in this presentation is for information only and should not be construed as complete for compliance purposes.
- Most Recent information available @ [www.dhs.gov/chemicalsecurity](http://www.dhs.gov/chemicalsecurity)



# Legal Foundation

- Section 550 of the 2007 DHS Approps Act provides, in part, that: “[I]nformation developed under this section, . . . shall be given protections from public disclosure consistent with [Sensitive Security Information (SSI)] . . . *Provided*, That in any proceeding to enforce this section, . . . Information submitted or obtained under this section . . . shall be treated as if the information were classified material.”
- Subpart D (Section 27.400) of the Interim Final Rule describes in detail the rules for access, maintenance, safeguarding and disclosure of CVI.



# What is CVI?

- Top-screens
- Security Vulnerability Assessments
- Site Security Plans
- Notices of determination or deficiency
- Compliance orders
- Derivative products
- Requests for re-determination
- Sensitive correspondence between facilities and DHS
- Inspection findings, Audit records
- Extended list available in 6 CFR 27 and @ [http://www.poultryegg.org/Environment/DHS/chemsec\\_cvi\\_proceduresmanual.pdf](http://www.poultryegg.org/Environment/DHS/chemsec_cvi_proceduresmanual.pdf)



## Covered Persons

- Individuals who have a “need to know” CVI, as defined in section 27.400(e) of the rule (IFR)
- Anyone who otherwise receives or gains access to what they know or reasonably should know constitutes CVI
- Federal employees must have CVI on-line training
- All other covered persons, including chemical facility employees and their contractors must have CVI on-line training and non-disclosure agreement

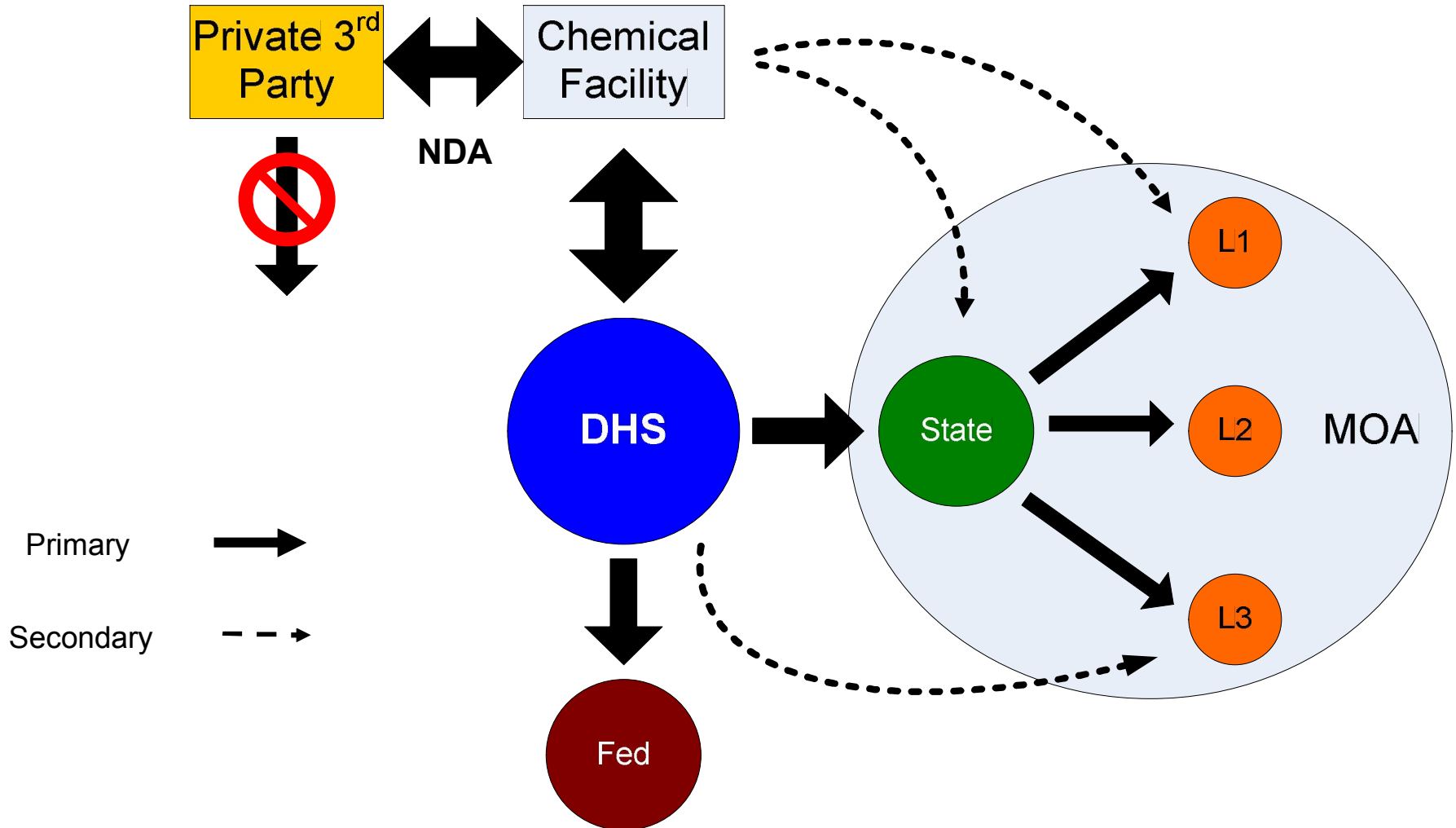


# What meets “Need to Know”

- If access is required to:
  - **Carry out** facility security activities approved, accepted, funded, recommended, or directed by the Department
  - **Receive training** to carry out security activities . . .
  - **Supervise or otherwise manage individuals** carrying out security activities . . .
  - **Provide technical or legal advice** to a covered person who has a need to know
- Federal employees, contractors and grantees if required for the performance of official duties
- If DHS determines access is required for enforcement proceedings



# Information Flow





## Disclosure to Private 3<sup>rd</sup> Parties

- Chemical facilities may disclose CVI to interested third parties (e.g., insurers) so long as facilities:
  - (1) provide notice to DHS; and
  - (2) require that the third parties sign an NDA and complete on-line CVI training.
- The NDA must prohibit further disclosures of CVI.



# Marking Information as CVI

- Authorized users are responsible
- The CVI Cover Sheet
  - must be affixed to the front and back
  - must remain with the document permanently
  - If the information is presented electronically, this information shall be displayed prior to an individual accessing the information.
- New CVI must include a tracking number.
- All pages in a document designated as CVI shall have the words -  
**Chemical-terrorism Vulnerability Information**  
placed in the header of each page.



## Storage Requirements

- Hard copies of CVI should be placed in a locked storage device when not in use.
- Users must use the screen locking and log-off features, or turn off the computer at the end of a work session.
- Anyone seeking to store CVI electronically is encouraged to contact the Chemical Security Help Desk to learn more about IT system requirements.



# Transmitting CVI

- Encryption is required when transmitting CVI over the internet, high-frequency, or other radio signals (including cellular telephones).
- Encryption is not required when CVI is discussed over wire line telecommunications networks or when transmitted via fax. When faxing CVI, ensure that an individual authorized to access CVI is standing by at the destination to receive the fax.
- Transmission by USPS or Commercial Carrier requires double protection to any document or electronic storage device. This includes an inner envelope marked as CVI and an outer envelope without CVI markings.



# Transmitting CVI

- A log of who received CVI information must be maintained, including:
  - Date CVI was shared
  - Tracking number(s) of the CVI shared
  - Who received the CVI
  - Contact information for the recipient
  - How CVI was sent to the recipient
  - Evidence of receiving prior written authorization from CSCD Director (if required)



# Sanitized Information

- CVI may be used to prepare information for public release, including advisories, alerts, and warnings issued to the public. This information product must be sanitized before its release.
- The author should consider the following points before disseminating the sanitized information:
  - Is sensitive chemical siting, security, vulnerability, etc. information included?
  - Have I provided information otherwise not customarily in the public domain?



# Sharing CVI Under Emergency Circumstances

- In the event of emergency circumstances, dissemination or access to CVI can be granted without meeting DHS requirements, provided a record is kept and immediately submitted to the CSCD CVI Security Officer (e.g., within less than 24 hours), including:
  - Name and contact information for the recipient and date shared
  - How CVI was sent to the recipient
  - Reason for emergency or exigent dissemination/access
- Within five business days of emergency dissemination/access being granted, the CSCD will contact the recipient and ensure the recipient meets all of the requirements for an authorized user.



# Using and Sharing CVI

- Authorized users are responsible for protecting the information and any CVI derivative products from unauthorized disclosure and cannot be shared with unauthorized users.
- In general, an authorized user must:
  - Have a need to know for that specific information as determined by the holder of the information
  - Complete CVI Authorized User Training
  - Have signed a Non Disclosure Agreement (NDA), if a non-Federal employee
  - Completed a background check if required by CSCD.



# Using and Sharing CVI

- If a chemical facility decides to share CVI with a private third party, a notice must be provided to the CSCD Director. The third party must complete DHS CVI training and sign a non-disclosure agreement (NDA) which must state that these third party recipients may not disseminate this information.
- CSCD will maintain a list of authorized users for verification.
- A chemical facility must receive the consent of the CSCD Director if it decides to share CVI with a state or local government authority.
- The recipient of CVI must destroy this information when no longer needed



# Other Federal Obligations

- The rule does not prohibit chemical facilities from complying with obligations they may have to provide information to federal, state, or local agencies.
- These obligations, however, do **not** require facilities to provide CVI.
- Pieces of information by themselves, or compiled for purposes other than the rule, do not constitute CVI.
  - Example: the rule does not prohibit a facility from providing an EPA or state inspector a list of chemicals on-site even though that same information may be included in a Top-Screen and the Top-Screen does constitute CVI.



# Disclosure in Administrative and Judicial Proceedings

- CVI must be treated like classified material in enforcement proceedings.
- DHS may provide CVI to covered persons and their counsel for use in administrative or judicial enforcement proceedings.
  - USG can attempt to prevent disclosure in judicial proceedings by requesting that court accept a redacted version or a summary substitute.
- CVI is not available in litigation unrelated to CFATS, except at the discretion of DHS.