GUIDE FOR THE PREPARATION OF SANITIZED AND DERIVATIVE WORK PRODUCTS USING CHEMICAL-TERRORISM VULNERABILITY INFORMATION (CVI)

June 2007

CONTENTS

Introduction 1
Categories of CVI Work Products 1
1. Sanitized Information 1
2. Derivative Information 2
Unclassified Work Products Containing CVI 2
Classified Products Derived from and Containing CVI 3
The CVI Cover Sheet 3
Dissemination of Derivative Information 4
Destruction of Derivative Information 4
CVI Sharing Requirements 4
Appendix A – Example of a CVI Derivative Product 5
Appendix B – Example of a CVI Derivative Product Containing Classified Information 6
Appendix C – CVI Cover Page 7

Introduction

A user of Chemical-terrorism Vulnerability Information (CVI) may on occasion need to create products that contain or are based upon this sensitive but unclassified information. These products may be subject to same handling and safeguarding requirements as the source material. This guide provides the instructions for marking these materials and guidance on how to sanitize the information sufficiently to allow for general public access.

Remember, if ***any*** CVI is contained in a product, that work product becomes subject to CVI handling and safeguarding requirements and may not be publicly disclosed. Any information that identifies the submitter of CVI or the infrastructure is considered CVI. Such information identifying the submitter may be either explicit (e.g., name of chemical facility, facility official name, or this person's respective contact information) or implicit (e.g., name of a product or service, or geographic location).

Categories of CVI Work Products

The two primary categories of CVI work products are:

1. Sanitized information such as advisories, alerts, and warnings; and
2. Derivative information that provides verbatim CVI or information that can infer either the identity of the submitter or a specific chemical facility.

1. Sanitized Information

When Federal, State, or local officials use CVI to prepare communications for a public audience, this information must be sanitized sufficiently to protect the identity of the submitter and the critical infrastructure in question. For the purposes of the Chemical Security Compliance program, "sanitization" means distilling the information in such a manner that the resulting product does not reveal:

- *vulnerabilities of critical infrastructure or protected systems;*
- *security procedures or practices carried out by the chemical facility;*
- *information regarding the consequences of any act of terrorism*
- *proprietary, business-sensitive, or trade secret information;*
- *pending compliance or enforcement actions; or*
- *any other company information not customarily found in the public domain.*

When appropriate and necessary, the author of any sanitized product will contact the Chemical Security Compliance Division's CVI Security Officer to

ensure that the sanitized information meets the criteria stated above. The CVI Security Officer is responsible for ensuring that advisories, alerts, and warnings have been sufficiently sanitized.

If a CVI derivative product is used as the basis for developing information for public release, the author of the information shall only be required to consider that information that is portion marked as CVI or other protection marking. If no source information is portion marked, the author may proceed forward without considering any effort to further sanitize the information.

The requirements for sanitizing apply not only to the submitter and the chemical facility described in the submission but also any third party information included in the submission or other sensitive but unclassified materials.

As with classified information, authorized users of CVI may use any information they can derive from legitimate open non-CVI sources, even if it is the same information is protected as CVI.

2. Derivative Information

Unclassified Work Products Containing CVI

All users must follow these guidelines when preparing an *unclassified* CVI derivative work product:

- Insert the text "COUNTER-TERRORISM VULNERABILITY INFORMATION" in the header and footer in a font larger than the document text.
- Insert the distribution limit statement on the bottom of each page of the document. See Appendix A for an example.
- Mark each paragraph, table, graphic, figure, etc., containing verbatim or paraphrased CVI with "(CVI)". (All other paragraphs, tables, graphics, figures, etc. are **not** portion-marked.)
- Include appropriate markings for other Sensitive but Unclassified (SBU) information in the product including Sensitive Security Information (SSI), Safeguards Information (SGI), and Protective Critical Infrastructure Information (PCII). These categories of SBU each have their respective handling requirements. Attach the appropriate cover sheets beneath the CVI one to alert the recipient of the handling and safeguarding requirements that must be followed.
- Include the document control number in the footer of each page marked with CVI. Provide each respective tracking number if more than one source document was used.
- Affix a CVI Cover Sheet to the front and back of derivative product.

Classified Products Derived from and Containing CVI

Derivative products that contain both CVI and classified materials must be handled and protected in accordance with the safeguarding and handling requirements for **both** CVI and the highest level of classified designation within the product**.**

All users must follow these guidelines when preparing a *classified* CVI derivative product in addition to the procedures required by the classified designation:

- Insert the text "COUNTER-TERRORISM VULNERABILITY INFORMATION" in the header beneath the classified marking in a font larger than the document text.
- Insert the distribution limit statement on the bottom of each page of the document above the classified marking. See Appendix B for an example.
- Mark each paragraph, table, graphic, figure, etc., containing verbatim or paraphrased CVI with "(CVI)". (All other paragraphs, tables, graphics, figures, etc. are **not** portion-marked.) Where information in a paragraph, table, graphic, figure, etc., is classified, it must be appropriately marked, e.g., (S) or (TS). This marking is necessary because subsequent declassification will not affect the information marked as CVI.
- Include the CVI document control number in the footer of each page marked with CVI. Provide each respective tracking number if more than one source document was used.
- Affix a CVI Cover Sheet to the front and back of the derivative product. The CVI Cover Sheet is placed immediately behind any classified cover sheet.

The CVI Cover Sheet

The CVI cover sheet is a shield that alerts observers that the document contains CVI. The cover sheet provides the distribution limitation statement required by 6 CFR 27.400(f)(3). The cover sheet also provides the recipient with basic handling and safeguarding instructions to remind this person of their legal obligations to protect the information from public release. An example of the cover sheet is found in Appendix C.

The person preparing a CVI work product must attach the CVI cover sheet or an equivalent alert for CVI found in electronic format, audio tapes, or other non-document information sources. CVI materials should always be protected by the CVI cover sheet, whether in storage, transit, or left unattended in a controlled-access work environment. This ensures that CVI will not be accessed by those individuals that do not have a need to know.

Dissemination of Derivative Information

Derivative products can only be disseminated to authorized users with homeland security responsibilities and a need-to-know. Follow the procedure for sharing CVI as described in Section 10.0 of the CVI Procedural Manual. Disclosure of CVI to the general public may only occur with the consent of the Assistant Secretary for Infrastructure Protection. In general, authorized users in state and local agencies must confirm a requesting person's need to know with the state CVI Security Officer.

Destruction of Derivative Information

The DHS Chemical Security Compliance Division encourages authorized users to destroy any derivative information when it is no longer needed. No approval is required from the Chemical Security Compliance Division to destroy derivative CVI. Authorize users are encouraged to keep a record of when the destruction occurred. Only the Chemical Security Compliance Division may destroy original CVI held by the Department of Homeland Security.

CVI Sharing Requirements

Authorized users must keep of a log that records the tracking number(s), date, name, organization, and contact information for anyone that receives CVI. Authorized users should also keep any records that document need to know decisions provided by the appropriate CVI Security Officer. No further tracking is required.

Appendix A – Example of a CVI Derivative Product

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

The chemical industry faces many challenges to meet the ever-changing landscape of cyber security. These challenges come from both domestic and foreign sources and are often difficult to identify.

(CVI) The E Pluribus Union Company reported that in 2006 that it received over 200 cyber attacks that included Trojan horses, net bots, and tracking cookies. The most serious incident resulted in a 72 hour shut down of facility systems.

These types of attacks caused over $3 billion in damages according to a Department of Commerce study. What does not get reported are the downstream impacts to those companies who do business with the companies directly affected by a cyber attack.

(CVI) The changing nature of the viruses and other malware require companies to invest significant resources in training systems engineers to identify threats and remedy resulting attack. Habeus Corpus LLP reported spending $300 thousand in employee development. This investment has a short return, as the company reported high turnover of qualified employees leaving to take offers from other companies. The shutdown of monitoring system blamed on staff shortages resulted in the release of 500 lbs. of ethylene oxide.

Recently, the National Association of Cyber Systems Officials posted the announcement of a symposium to discuss this issue. All interested persons are invited to attend.

CVI Control Number: 01-10000-1111, 02-00001-2222

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).

Appendix B – Example of a CVI Derivative Product Containing Classified Information

SECRET

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

The chemical industry faces many challenges to meet the ever-changing landscape of cyber security. These challenges come from both domestic and foreign sources and are often difficult to identify.

(CVI) The E Pluribus Union Company reported that in 2006 that it received over 200 cyber attacks that included Trojan horses, net bots, and tracking cookies. The most serious incident resulted in a 72 hour shut down of facility systems.

These types of attacks caused over $3 billion in damages according to a Department of Commerce study. What does not get reported are the downstream impacts to those companies who do business with the companies directly affected by a cyber attack.

(CVI) The changing nature of the viruses and other malware require companies to invest significant resources in training systems engineers to identify threats and remedy resulting attack. Habeus Corpus LLP reported spending $300 thousand in employee development. This investment has a short return, as the company reported high turnover of qualified employees leaving to take offers from other companies. The shutdown of monitoring system blamed on staff shortages resulted in the release of 500 lbs. of ethylene oxide.

(S)The Department of Defense confirmed similar attacks on their systems. On December 7, 2007, Fort Noshow reported that a virus entered the system responsible for controlling access to elemental chlorine used for the fort's water treatment system.

Recently, the National Association of Cyber Systems Officials posted the announcement of a symposium to discuss this issue. All interested persons are invited to attend.

CVI Control Numbers: 01-10000-1111, 02-00001-2222
Classified Source: 99-200-333-01

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).

SECRET

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