

# **TSCA CBI Protection Manual**

---



**United States  
Environmental Protection Agency**

**Office of Pollution Prevention and Toxics  
Washington, DC 20460 (7407 M)**

**October 20, 2003  
7700 A1**

This page intentionally left blank.

# *Table of Contents*

– Summary –

[See *Detailed Contents* below]

	Page
<b><u>PREFACE</u></b> .....	-xv-
<b><u>GUIDING PRINCIPLES</u></b> .....	-xvii-

## **CHAPTER 1**

### **References**

<b><u>1.1</u></b> ABBREVIATIONS AND ACRONYMS .....	-1-
<b><u>1.2</u></b> GLOSSARY .....	-3-
<b><u>1.3</u></b> LIST OF APPENDICES .....	-7-

## **CHAPTER 2**

### **TSCA CBI Access**

<b><u>2.0</u></b> INTRODUCTION .....	-9-
<b><u>2.1</u></b> TSCA CBI ACCESS FOR FEDERAL EMPLOYEES: CERTIFICATION, MAINTENANCE, SUSPENSION, AND TERMINATION .....	-10-
<b><u>2.2</u></b> TSCA CBI ACCESS FOR CONTRACTORS AND CONTRACTOR EMPLOYEES: CERTIFICATION, MAINTENANCE, TERMINATION AND INDUSTRY NOTICE .....	-16-
<b><u>2.3</u></b> TSCA CBI ACCESS CERTIFICATION FOR OTHER FEDERAL AGENCIES .....	-25-
<b><u>2.4</u></b> REQUESTS FROM CONGRESS OR THE GENERAL ACCOUNTING OFFICE (GAO) .....	-28-

## **CHAPTER 3**

### **TSCA CBI Responsibilities**

<b><u>3.0</u></b>	<b>INTRODUCTION .....</b>	<b>-31-</b>
<b><u>3.1</u></b>	<b>EMPLOYEE RESPONSIBILITIES .....</b>	<b>-31-</b>
<b><u>3.2</u></b>	<b>MANAGER RESPONSIBILITIES .....</b>	<b>-33-</b>
<b><u>3.3</u></b>	<b>DCO RESPONSIBILITIES .....</b>	<b>-34-</b>
<b><u>3.4</u></b>	<b>EAD AND IMD ANNUAL REVIEW .....</b>	<b>-44-</b>

## **CHAPTER 4**

### **TSCA CBI Document Management**

<b><u>4.0</u></b>	<b>INTRODUCTION .....</b>	<b>-47-</b>
<b><u>4.1</u></b>	<b>RECEIPT OF TSCA CBI. ....</b>	<b>-47-</b>
<b><u>4.2</u></b>	<b>DOCUMENT TRACKING SYSTEM (DTS) REQUIREMENTS .....</b>	<b>-50-</b>
<b><u>4.3</u></b>	<b>STORING TSCA CBI .....</b>	<b>-53-</b>
<b><u>4.4</u></b>	<b>TSCA CBI DOCUMENTS .....</b>	<b>-60-</b>
<b><u>4.5</u></b>	<b>REPRODUCING TSCA CBI .....</b>	<b>-63-</b>
<b><u>4.6</u></b>	<b>TRANSFERRING, TRANSFER RECORD- KEEPING, AND TRANSMITTING TSCA CBI .....</b>	<b>-64-</b>
<b><u>4.7</u></b>	<b>USING AND HANDLING TSCA CBI .....</b>	<b>-71-</b>
<b><u>4.8</u></b>	<b>USING COMPUTERS TO WORK WITH TSCA CBI .....</b>	<b>-73-</b>
<b><u>4.9</u></b>	<b>DESTRUCTION OF TSCA CBI .....</b>	<b>-76-</b>

# CHAPTER 5

## Procedures Violations, Missing Documents and Unauthorized Disclosures

<b><u>5.0</u></b>	<b>INTRODUCTION .....</b>	<b>-79-</b>
<b><u>5.1</u></b>	<b>EMPLOYEE REPORTING PROCEDURES .....</b>	<b>-79-</b>
<b><u>5.2</u></b>	<b>REPORT OF VIOLATIONS TO TSS .....</b>	<b>-80-</b>
<b><u>5.3</u></b>	<b>CORRECTIVE ACTION AND PENALTY GUIDELINES .....</b>	<b>-82-</b>
<b><u>5.4</u></b>	<b>OPPT DIRECTOR AS ARBITER .....</b>	<b>-85-</b>

This page intentionally left blank.

# *Table of Contents*

## **- Detailed -**

	Page
<b><u>PREFACE</u></b> .....	-xv-
<b><u>GUIDING PRINCIPLES</u></b> .....	-xvii-

## **CHAPTER 1**

### **References**

<b><u>1.1</u></b> ABBREVIATIONS AND ACRONYMS .....	-1-
<b><u>1.2</u></b> GLOSSARY .....	-3-
<b><u>1.3</u></b> LIST OF APPENDICES .....	-7-

## **CHAPTER 2**

### **TSCA CBI Access**

<b><u>2.0</u></b> INTRODUCTION .....	-9-
<b><u>2.1</u></b> TSCA CBI ACCESS FOR FEDERAL EMPLOYEES: CERTIFICATION, MAINTENANCE, SUSPENSION, AND TERMINATION .....	-10-
<b><u>2.1.1</u></b> Re-Certification For Federal Employees .....	-11-
<b><u>2.1.1.1</u></b> <i>Document Audit</i> .....	-11-
<b><u>2.1.1.2</u></b> <i>Time For Re-Certifying</i> .....	-12-
<b><u>2.1.2</u></b> Failure to Maintain Access Certification .....	-12-
<b><u>2.1.2.1</u></b> <i>Suspension and Termination</i> .....	-12-

<b><u>2.1.3</u></b>	<b>Suspension of Log-Out Privileges</b> .....	-13-
<b><u>2.1.4</u></b>	<b>EPA Employee Transfers</b> .....	-13-
<b><u>2.1.4.1</u></b>	<b><i>Supervisors' Responsibilities When Employee Transfers</i></b> ...	-13-
<b><u>2.1.5</u></b>	<b>TSCA CBI Access Termination for Federal Employees</b> .....	-13-
<b><u>2.1.5.1</u></b>	<b><i>TSCA CBI Access Termination Procedures: Federal Employees</i></b> .....	-14-
<b><u>(a)</u></b>	<b><i>DCO And Supervisor Responsibilities For Access Termination</i></b> .....	-15-
<b><u>(b)</u></b>	<b><i>OPPT DCO Responsibilities For Access Termination:</i></b> ..	-15-
<b><u>2.1.6</u></b>	<b>Unaccounted For Documents</b> .....	-15-
<b><u>2.2</u></b>	<b>TSCA CBI ACCESS FOR CONTRACTORS AND CONTRACTOR EMPLOYEES: CERTIFICATION, MAINTENANCE, TERMINATION AND INDUSTRY NOTICE</b> .....	-16-
<b><u>2.2.1</u></b>	<b>Determination of TSCA CBI Access for Contractors</b> .....	-16-
<b><u>2.2.2</u></b>	<b>Approval for TSCA CBI Access or Expedited Approval for Immediate Access.</b> .....	-17-
<b><u>2.2.3</u></b>	<b>Rules for Contractors</b> .....	-17-
<b><u>2.2.4</u></b>	<b>Notice to Affected Businesses Prior To Granting Access</b> .....	-18-
<b><u>2.2.5</u></b>	<b>Requirement for Contractor DCO</b> .....	-19-
<b><u>2.2.6</u></b>	<b>TSCA CBI Certification for Contractor Employees</b> .....	-19-
<b><u>2.2.7</u></b>	<b>Initial Certification for Contractor Employees</b> .....	-20-
<b><u>2.2.8</u></b>	<b>National Agency Check &amp; Inquiries (NACI)</b> .....	-21-
<b><u>2.2.9</u></b>	<b>TSCA CBI Re-Certification for Contractor Employees</b> .....	-21-
<b><u>2.2.9.1</u></b>	<b><i>Document Audit</i></b> .....	-21-
<b><u>2.2.9.2</u></b>	<b><i>Time for Re-Certifying</i></b> .....	-22-
<b><u>2.2.10</u></b>	<b>Failure to Maintain Access Certification for Contractor Employees</b> .....	-22-
<b><u>2.2.11</u></b>	<b>TSCA CBI Access Termination: Contractor Employees</b> .....	-23-
<b><u>2.2.11.1</u></b>	<b><i>TSCA CBI Access Termination Procedures: Contractor Employees</i></b> .....	-23-



**2.2.11.2 *Unaccounted For Documents* ..... -25-**

**2.2.12 **Change in Corporate Status** ..... -25-**

**2.3 **TSCA CBI ACCESS CERTIFICATION FOR OTHER FEDERAL AGENCIES** ..... -25-**

**2.3.1 **Procedures for Other Federal Agencies to Obtain TSCA CBI Access** ..... -26-**

**2.3.2 **Notice to Affected Businesses** ..... -27-**

**2.3.3 **Security Requirements at Other Federal Agencies** ..... -28-**

**2.4 **REQUESTS FROM CONGRESS OR THE GENERAL ACCOUNTING OFFICE (GAO)** ..... -28-**

## **CHAPTER 3**

### **TSCA CBI Responsibilities**

**3.0 **INTRODUCTION** ..... -31-**

**3.1 **EMPLOYEE RESPONSIBILITIES** ..... -31-**

**3.1.1 **Personal Accountability** ..... -31-**

**3.1.2 **Assuring Adequate TSCA CBI Protection** ..... -31-**

**3.1.3 **Reporting Procedural Violations** ..... -31-**

**3.1.4 **Document Accountability** ..... -32-**

**3.1.5 **TSCA CBI Procedure Accountability** ..... -32-**

**3.1.6 **Return TSCA CBI Document** ..... -32-**

**3.1.7 **Determination of TSCA CBI** ..... -32-**

<b><u>3.1.8</u></b>	<b>Receipt of Possible CBI</b> .....	-33-
<b><u>3.2</u></b>	<b>MANAGER RESPONSIBILITIES</b> .....	-33-
<b><u>3.2.1</u></b>	<b>Assigning DCO and ADCO</b> .....	-33-
<b><u>3.3</u></b>	<b>DCO RESPONSIBILITIES</b> .....	-34-
<b><u>3.3.1</u></b>	<b>DCOs and Alternate DCOs</b> .....	-34-
<b><u>3.3.2</u></b>	<b>Maintaining a Document Tracking System (DTS)</b> .....	-34-
<b><u>3.3.3</u></b>	<b>Transfer of TSCA CBI</b> .....	-34-
<b><u>3.3.4</u></b>	<b>Receiving TSCA CBI</b> .....	-35-
<b><u>3.3.5</u></b>	<b>Proper Storage of TSCA CBI</b> .....	-35-
<b><u>3.3.6</u></b>	<b>Records of Lock-Combinations</b> .....	-35-
<b><u>3.3.7</u></b>	<b>Conditions For Changing Lock Combinations</b> .....	-36-
<b><u>3.3.8</u></b>	<b>Updating The TSCA CBI Authorized Access List</b> .....	-36-
<b><u>3.3.9</u></b>	<b>Monitoring And Controlling Release of TSCA CBI</b> .....	-36-
<b><u>3.3.10</u></b>	<b>Overdue Materials: Monitoring And Notification</b> .....	-37-
<b><u>3.3.11</u></b>	<b>DCO Guidance In Identifying And Sanitizing CBI Documents</b> ..	-38-
<b><u>3.3.12</u></b>	<b>TSCA CBI Audits</b> .....	-38-
<b><u>3.3.12.1</u></b>	<b><i>Federal DCOs And The Confidential Business Information Center (CBIC)</i></b> .....	-38-
<b><u>(a)</u></b>	<b><i>Comprehensive Audits of Entire Collection</i></b> .....	-38-
<b><u>(b)</u></b>	<b><i>Transaction Audits</i></b> .....	-40-
<b><u>(c)</u></b>	<b><i>DCO Transition Audits</i></b> .....	-41-
<b><u>3.3.12.2</u></b>	<b><i>Contractor DCOs</i></b> .....	-42-
<b><u>(a)</u></b>	<b><i>Comprehensive Audits of Entire Collection</i></b> .....	-42-
<b><u>(b)</u></b>	<b><i>Contract close-out Audits</i></b> .....	-43-

**3.3.13 Termination Of Employment Or Status For DCO** ..... -44-

**3.4 EAD AND IMD ANNUAL REVIEW** ..... -44-

## CHAPTER 4

### TSCA CBI Document Management

**4.0 INTRODUCTION** ..... -47-

**4.1 RECEIPT OF TSCA CBI** ..... -47-

**4.1.1 Incoming TSCA CBI** ..... -47-

**4.1.2 Personal File Copies - New Chemicals Program (OPPT-CCD)** ... -48-

**4.1.3 Supplemental Filings - New Chemicals Program (OPPT-CCD)** .. -48-

**4.1.4 Processing Newly Received TSCA CBI** ..... -48-

**4.1.4.1 CBI Fax Transmission From Industry** ..... -49-

**4.1.5 TSCA CBI Claims That Appear Unwarranted** ..... -50-

**4.2 DOCUMENT TRACKING SYSTEM (DTS) REQUIREMENTS** ..... -50-

**4.2.1 Use of an Automated Document Tracking System (DTS)** ..... -50-

**4.2.2 Use of a Manual Document Tracking System (DTS)** ..... -51-

**4.2.2.1 Receipt Log** ..... -52-

**4.2.2.2 Inventory Log** ..... -52-

**4.3 STORING TSCA CBI** ..... -53-

**4.3.1 Secure Storage Areas (SSAs)** ..... -53-

**4.3.1.1 Entering An SSA With An Electronic Access Card (EAC)** ... -54-

**4.3.1.2 Entering an SSA Without An Electronic Access Card** ..... -54-

**4.3.1.3 Entering An SSA With Expired Certification** ..... -54-

**4.3.1.4 Grantees And Interns In SSAs** ..... -54-

<u>4.3.1.5</u>	<i>Visitors In SSAs</i> .....	-55-
<u>4.3.1.6</u>	<i>Custodian, Maintenance and Delivery Persons in SSAs</i> .....	-55-
<u>4.3.1.7</u>	<i>DCOs And SSAs</i> .....	-55-
<u>4.3.1.8</u>	<i>Using TSCA CBI Outside An SSA</i> .....	-56-
<b>4.3.2</b>	<b>Required Storage Containers</b> .....	-56-
<b>4.3.3</b>	<b>Storing TSCA CBI At Other Locations</b> .....	-56-
<u>4.3.3.1</u>	<i>Storing Of TSCA CBI While Traveling</i> .....	-57-
<u>4.3.3.2</u>	<i>Storing and Working with TSCA CBI in a Personal Residence</i> .....	-57-
<b>4.3.4</b>	<b>Employee Absence and Storage of TSCA CBI</b> .....	-60-
<b>4.4</b>	<b>TSCA CBI DOCUMENTS</b> .....	-60-
<b>4.4.1</b>	<b>New CBI Documents</b> .....	-60-
<b>4.4.2</b>	<b>Working Papers</b> .....	-60-
<u>4.4.2.1</u>	<i>When Working Papers Become Subject to Tracking</i> .....	-61-
<u>4.4.2.2</u>	<i>Destroying Working Papers</i> .....	-61-
<b>4.4.3</b>	<b>When CBI Documents Are No Longer CBI</b> .....	-61-
<b>4.4.4</b>	<b>Aggregating CBI</b> .....	-62-
<b>4.4.5</b>	<b>Declassifying CBI Documents</b> .....	-62-
<b>4.4.6</b>	<b>TSCA CBI Document Submitters: Dropping a Claim</b> .....	-63-
<b>4.5</b>	<b>REPRODUCING TSCA CBI</b> .....	-63-
<b>4.5.1</b>	<b>Managing TSCA CBI Copies</b> .....	-63-
<b>4.5.2</b>	<b>Copying CBI Outside SSAs</b> .....	-64-
<b>4.6</b>	<b>TRANSFERRING, TRANSFER RECORD- KEEPING, AND TRANSMITTING TSCA CBI</b> .....	-64-
<b>4.6.1</b>	<b>Transferring Hard Copy TSCA CBI</b> .....	-64-
<u>4.6.1.1</u>	<i>Procedures For Sending Or Receiving TSCA CBI</i> .....	-64-
<u>4.6.1.2</u>	<i>Preparing CBI For Mailing</i> .....	-65-
<u>4.6.1.3</u>	<i>Transferring TSCA CBI to Another Facility</i> .....	-65-

**4.6.1.4 *Transferring TSCA CBI to Industry* ..... -66-**

**4.6.2 **Hard Copy TSCA CBI Transfer Record-Keeping** ..... -66-**

**4.6.2.1 *Record-Keeping For Permanent Transfer* ..... -66-**

**4.6.2.2 *Record-Keeping For Temporary Transfers Within A Facility* -67-**

**4.6.3 **Transmitting TSCA CBI Electronically** ..... -68-**

**4.6.3.1 *Transmitting TSCA CBI By Telephone* ..... -68-**

**4.6.3.2 *Transmitting TSCA CBI by Fax* ..... -69-**

**4.6.3.3 *Transmitting TSCA CBI By E-mail* ..... -70-**

**4.6.3.4 *Transmitting TSCA CBI By Tele-Video Conference* ..... -70-**

**4.7 **USING AND HANDLING TSCA CBI** ..... -71-**

**4.8 **USING COMPUTERS TO WORK WITH TSCA CBI** ..... -73-**

**4.8.1 **Prohibition** ..... -73-**

**4.8.2 **TSCA CBI Computers Must Be Separate From Public Networks** -73-**

**4.8.3 **Registration is Required to Use CBI Computer Systems** ..... -73-**

**4.8.4 **Using Portable Computers (*Laptops and Handheld Devices*)** ..... -74-**

**4.8.5 **Disposing of Computers Formerly Used for TSCA CBI** ..... -74-**

**4.8.6 **Modems** ..... -75-**

**4.8.7 **TSCA CBI Data Processed Only Within SSAs** ..... -75-**

**4.8.8 **Printing CBI Information** ..... -75-**

**4.8.9 **Storing CBI on Magnetic Media** ..... -75-**

**4.8.10 **Disposing of TSCA CBI Computer Disks** ..... -75-**

**4.8.11 **Security for TSCA CBI Data Stored on Contractor’s Off-site Computer** ..... -76-**

**4.9 **DESTRUCTION OF TSCA CBI** ..... -76-**

**4.9.1 Procedures for Destroying TSCA CBI . . . . . -76-**

**4.9.2 Destruction Methods . . . . . -77-**

**4.9.3 Destruction Record-Keeping . . . . . -77-**

**4.9.4 Disposition of CBI Cover Sheets . . . . . -77-**

**4.9.5 Contracts Involving TSCA CBI . . . . . -77-**

**CHAPTER 5**  
**Procedures Violations, Unaccounted For Documents and**  
**Unauthorized Disclosures**

**5.0 INTRODUCTION . . . . . -79-**

**5.1 EMPLOYEE REPORTING PROCEDURES . . . . . -79-**

**5.1.1 Oral Report . . . . . -79-**

**5.1.2 Written Report . . . . . -80-**

**5.2 REPORT OF VIOLATIONS TO TSS . . . . . - 80-**

**5.2.1 TSS Investigation . . . . . -80-**

**5.2.2 Oral Notice to Submitter . . . . . -81-**

**5.2.3 Report of Investigation (ROI) . . . . . -81-**

**5.2.4 Company Notification of Improper Disclosure: EAD Director . . . -81-**

**5.2.5 Company Notification of Documents Unaccounted for: EAD Director**  
    **. . . . . -82-**

**5.2.6 Referral to the Inspector General . . . . . -82-**

**5.2.7 Annual Security Report . . . . . -82-**

<b><u>5.3</u></b>	<b>CORRECTIVE ACTION AND PENALTY GUIDELINES .....</b>	<b>- 82-</b>
<b><u>5.3.1</u></b>	<b>Responsibility for Monitoring Compliance With Protection Manual .....</b>	<b>-82-</b>
<b><u>5.3.2</u></b>	<b>Violations by Federal Employees .....</b>	<b>-83-</b>
<b><u>5.3.3</u></b>	<b>Violations by Contractor Employees .....</b>	<b>-85-</b>
<b><u>5.4</u></b>	<b>OPPT DIRECTOR AS ARBITER .....</b>	<b>-85-</b>

This page intentionally left blank



## PREFACE

This Manual applies to all federal employees, contractors, and contractor employees with access to information claimed as Toxic Substances Control Act (TSCA) Confidential Business Information (CBI) in connection with either their official duties or with a TSCA-related government contract, as stated in Section 14(a) of TSCA.

**This Manual does not apply to other persons, including submitters to the Agency of TSCA CBI, nor purport in any way to set rules regarding how information must be submitted to the Agency or otherwise handled by those persons.**

The following general subjects correspond to the chapters in this Manual:

- Steps necessary to become authorized for access to TSCA CBI.
- Relative roles and responsibilities regarding TSCA CBI.
- Steps for use and protection of TSCA CBI.
- Procedures in cases of lost or improperly disclosed TSCA CBI.

The provisions in this Manual are designed to protect the confidential information entrusted to the Federal Government, and to ensure that employees and contractors are aware of the importance of adhering to the procedures of handling TSCA CBI, their personal responsibilities in doing so, and the consequences for failing to do so. When situations and circumstances not specifically addressed in this Manual arise, the obligation to protect TSCA CBI materials entrusted to EPA continues and must be ensured. For these unspecified instances, additional protections may be recommended or required at the appropriate time.

Most TSCA CBI is stored and handled at Environmental Protection Agency (EPA) Headquarters in the TSCA Confidential Business Information Center (CBIC). When necessary, EPA approves storing and handling of CBI at other Headquarters locations as well as facilities such as EPA Regional Offices, other federal agencies, and contractor facilities. Some differences in security and control procedures may be necessary depending on local circumstances. Any such differences, however, must be approved in writing by the Director of the EPA's Office of Pollution Prevention and Toxics (OPPT) Information

Management Division (IMD).

Information coming to the Agency pursuant to the **Lead-Based Paint Real Estate Notification and Disclosure Rule** (40 C.F.R. Part 745, Subpart F) will be exempted from the requirements of this Manual once a replacement security plan has been developed and approved by the OPPT Director. This replacement security plan may be accessed by contacting the OPPT DCO. A replacement security plan approved by the OPPT Director is binding upon Federal and contractor employees handling Residential Lead Disclosure CBI. Please be aware that approval of a replacement security plan does not exempt this information from the requirements of EPA confidentiality regulations at 40 CFR Part 2, Subpart B.

The provisions of this Manual are intended to apply in all situations. From time to time, however, extraordinary circumstances may arise presenting the need for a change from a prescribed procedure. In such cases, the appropriate divisional or other regional managers may apply directly in writing to the IMD Director for an exception. In examining the justification for the requested exception, the IMD Director will, in his/her judgment, decide whether to grant the request, in full or in part, including any conditions deemed appropriate.

This Manual is a “living” document. That is, its development and interpretation is continuing in nature and will be amended as the need arises.

This Manual may not appear to fit some situations, or the provisions within it may not seem to include every scenario, contingency, or specialized case. In these situations, please call the OPPT DCO or the OPPT IMD Attorney Advisor for special guidance or clarification.

## **GUIDING PRINCIPLES**

You have a responsibility to protect the information claimed as TSCA CBI. Any document that contains TSCA CBI which you receive, retain, create, or give to another must be protected. This is integral to your work.

The Agency tracks all documents in its possession and you, as a TSCA CBI cleared individual, are required to undergo an annual audit of all TSCA CBI entrusted to you by the Agency. Working papers must be individually tracked when not in direct possession of the creator and otherwise protected until destroyed.

You can only discuss or disseminate TSCA CBI with persons you know are authorized for access to TSCA CBI.

If you think you may have a TSCA CBI issue or problem, you should talk with your manager about it immediately.

You must ensure through personal accountability that you will act consistently with all guidelines established in this manual to protect TSCA CBI.

This page intentionally left blank

# CHAPTER 1

## Reference

### 1.1 ABBREVIATIONS AND ACRONYMS

Provided below is a list of abbreviations and acronyms used in this manual:

ADCO	Alternate DCO
CBIC	Confidential Business Information Center
CBITS	Confidential Business Information Tracking System
CCD	Chemical Control Division, OPPT
CFR	Code of Federal Regulations
DCN	Document Control Number
DCO	Document Control Officer
DOPO	Delivery Order Project Officer
DTS	Document Tracking System
EAC	Electronic Access Cards
EAD	Environmental Assistance Division, OPPT
ECO	Environmental Careers Organization
EETD	Economics, Exposure and Technology Division, OPPT
EPA	Environmental Protection Agency
FMSD	Financial Management and Services Division
FOIA	Freedom of Information Act
ID	Identification
IMD	Information Management Division, OPPT
ISO	Information Security Officer
LAN	Local Area Network
NACI	National Agency Check and Inquiries
NCIC	Non-Confidential Information Center
NOWCC	National Older Worker Career Center employee
OAM	Office of Acquisition Management
OARM	Office of Administration and Resources Management
OGC	Office of General Counsel
OPPT	Office of Pollution Prevention and Toxics
OMB	Office of Management and Budget
PC	Personal Computer
PMN	Premanufacture Notification

PO	Project Officer
RDMB	Records and Dockets Management Branch, IMD
ROI	Report of Investigation
SEE	Senior Environmental Employment Program
SOW	Contractor Statement of Work
SSA	Secure Storage Area
TSCA	Toxic Substances Control Act
TSCA CBI	Information submitted in connection with TSCA and claimed as confidential business information
TSS	TSCA Security Staff
WAM	Work Assignment Manager

## 1.2 GLOSSARY

Agency DCO	The lead document control officer for the TSCA program at EPA (aka: OPPT DCO)
Alternate Document Control Officer (ADCO)	The OPPT DCO and other DCOs can nominate ADCOs to assist them in performing document control functions. ADCOs can perform all functions of a DCO.
Annual Audit Certification Report	Employees complete these reports on an annual basis to indicate the status of any TSCA CBI logged out in their name.
Authorized Access List	A list of people who are authorized for access to TSCA CBI.
Certification	The process whereby federal and contractor employees acquire administrative access to TSCA CBI.
Contractor DCO	The document control officer designated by the Project Officer for a TSCA CBI cleared contract.
Contractors and Subcontractors	Persons, including individuals or business entities, who perform work under a contract with the United States Government or a subcontract with a contractor.
Document Control Officer (DCO)	DCOs oversee the receipt, storage, transfer, use, reproduction and destruction of TSCA CBI by employees. DCOs are responsible for assisting employees in requesting and renewing TSCA CBI access authorization, as well as managing the manual or automated Document Tracking System (DTS) for TSCA CBI in their facility or office.
Document Tracking System (DTS)	A Document Tracking System is used to track receipt of and activity involving TSCA CBI within a facility. The system may be manual or automated (electronic). Automated systems are recommended for high-volume facilities.

TSCA CBI PROTECTION MANUAL

Environmental Assistance Division (EAD)	EAD is responsible for oversight of the TSCA Confidential Business Information security function. This includes enforcement of the procedures and provisions contained in the TSCA CBI Protection Manual.
EPA Office	Organizational element of EPA, at any level or location.
EPA Project Officer <i>(also known outside this Manual as “Contract Level COR”)</i>	The Contracting Officer’s primary representative on a basic contract who oversees the delivery order, task order or work assignment.
Facility	Any location where EPA, a government contractor or another federal agency stores and uses TSCA CBI. Specific procedures may vary from location to location, but the general procedures in this Manual are in force at all facilities.
Federal Employee	Generally, an employee of the federal government who has a Standard Form (SF-52) on file with the Office of Personnel Management (OPM).
Grantee	Person who performs work under a grant. [Under TSCA, grantees are not authorized to handle TSCA CBI. Contact the OPPT-DCO for more information].
Hard-Copy	Data (e.g., submissions, printouts, photographs) received or generated on paper. Also, Magnetic Media (e.g., diskette, video tapes), and other “physical” things which can hold or contain CBI.
Information Management Division (IMD) Director	Within the Office of Pollution Prevention and Toxics (OPPT) the IMD director is responsible for the day-to-day implementation of TSCA CBI and control programs, including the development of policies for the use and handling of TSCA CBI and operation of the EPA headquarters-Confidential Business Information Center (CBIC).
Office of Pollution Prevention and Toxics (OPPT) Director	The OPPT director has overall authority for managing TSCA activities, including TSCA security programs.



TSCA CBI PROTECTION MANUAL

<p>OPPT Confidential Business Information Center (CBIC)</p>	<p>The primary area for storing and using TSCA CBI is the EPA CBIC at EPA headquarters in Washington, D.C. If appropriate, EPA may authorize TSCA CBI access at other facilities including EPA regional offices, other Federal agency offices, and contractor facilities.</p>
<p>OPPT Document Control Officer (OPPT DCO)</p>	<p>The OPPT DCO provides day-to-day support to other Federal and Contractor DCOs nationwide. This includes issuing the TSCA CBI authorized access list and processing forms and records pertaining to requests for TSCA CBI access authority for organizations and individuals. The OPPT DCO manages the headquarters CBIC, oversees other DCOs at headquarters, and provides training materials and guidance to all DCOs on appropriate TSCA CBI handling procedures.</p>
<p>Originator</p>	<p>An employee who is responsible for determining if documents he/she creates contain CBI and stamping them as such.</p>
<p>Requesting Official</p>	<p>This is (1) employee's immediate supervisor or higher authority who nominates a Federal employee for TSCA CBI access or (2) the EPA project officer who nominates a contractor employee for TSCA CBI access. Requesting officials' responsibilities include ensuring that their employees renew their TSCA CBI access authority yearly, determining when their employees no longer require access authority, authorizing their employees to transfer TSCA CBI using a courier or express mail, and initiating or reviewing their employees' reports of violation of this manual's procedures.</p>
<p>Sanitize</p>	<p>To remove TSCA CBI from a document.</p>
<p>Secure Storage Area (SSA)</p>	<p>An area that is secured from persons not authorized for access to TSCA CBI. Secure storage areas house the bulk of an organization or facility's TSCA CBI records, or serve as an organization or facility's primary TSCA CBI work area, or both.</p>
<p>Temporary Transfer</p>	<p>Relinquishing custody of TSCA CBI from one person to another in the same facility on a temporary basis.</p>

TSCA CBI PROTECTION MANUAL

TSCA CBI	TSCA information claimed business-confidential under EPA's confidentiality regulations at 40 CFR Part 2, Subpart B.
TSCA CBI LAN	The physically isolated Local Area Network (LAN) located at EPA Headquarters dedicated exclusively to TSCA CBI.
TSCA CBI Materials	Documents or any other information-bearing media that contain TSCA CBI.
TSCA Security Staff	The TSCA security staff (of EAD) responsible for security-related activities, including reviewing security procedures, performing facility site inspections, and investigating violations of the procedures contained in this manual.
Unauthorized Access	Access to TSCA CBI by persons lacking administrative clearance or whose clearance has expired.
Working Papers	Temporary work product documents produced by a federal or contractor employee containing TSCA CBI, which are subject to special handling procedures.

## 1.3 LIST OF APPENDICES

<b>Appendix A</b>	Form 7740-6: TSCA CBI Access Request, Agreement, and Approval
<b>Appendix B</b>	Form 7740-25: TSCA CBI ADP User Registration
<b>Appendix C</b>	Request for EPA Identification Badge
<b>Appendix D</b>	Request for Building Pass
<b>Appendix E</b>	Form 7740-28: United States Environmental Protection Agency TSCA Confidential Business Information Document Reconciliation Certification
<b>Appendix F</b>	Form 7710-17: Confidentiality Agreement for United States Employees Upon Relinquishing TSCA CBI Access Authority
<b>Appendix G</b>	Form 3110-1: Employee Separation or Transfer Checklist
<b>Appendix H</b>	Form 7740-17: Request for Approval of Contractor Access to TSCA Confidential Business Information
<b>Appendix I</b>	EPAAR 1552.235-78: Data Security for Toxic Substances Control Act Confidential Business Information
<b>Appendix J</b>	EPAAR 1552.235-75: Access to Toxic Substances Control Act Confidential Business Information
<b>Appendix K</b>	EPAAR 1552.235-76: Treatment of Confidential Business Information (TSCA)
<b>Appendix L</b>	Form 7740-27: Contractor Information Sheet – Contractor TSCA CBI Access/Transfer
<b>Appendix M</b>	Contractor Checklist For TSCA CBI Access
<b>Appendix N</b>	Contractor Employee Checklist For TSCA CBI Access
<b>Appendix O</b>	Form 86: Questionnaire for National Security Positions
<b>Appendix P</b>	Fingerprint Card “FD258 Application”
<b>Appendix Q</b>	Procedures for Terminating Contractor Access to TSCA CBI
<b>Appendix R</b>	Form 7740-18: Confidentiality Agreement for Contractor Employees Upon Relinquishing TSCA CBI Access Authority
<b>Appendix S</b>	Form 7740-24: Federal Agency, Congress, and Federal Court Sign Out Log
<b>Appendix T</b>	Stamp to use when Material contains TSCA CBI
<b>Appendix U</b>	Form 7740-9: Confidential Business Information Cover Sheet
<b>Appendix V</b>	Form 7740-11: Inventory Log
<b>Appendix W</b>	Form 7740-10: Receipt Log
<b>Appendix X</b>	Form 7740-13: TSCA CBI Visitors Log
<b>Appendix Y</b>	Form 7740-26: Permanent Transfer Receipt for TSCA Confidential Business Information
<b>Appendix Z</b>	Form 7740-12: Memorandum of TSCA CBI Telephone Conversation

<b>Appendix AA</b>	Form 7740-14: Temporary Loan Receipt for TSCA Confidential Business Information
<b>Appendix BB</b>	Laptop Computer Agreement for the Confidential Business Information Center (CBIC)
<b>Appendix CC</b>	Amendment Through Voluntary Withdrawal
<b>Appendix DD</b>	40 CFR 2.208, TSCA CBI substantive criteria for determining confidentiality
<b>Appendix EE</b>	Taking action on TSCA CBI claims that appear unwarranted

# CHAPTER 2

## TSCA CBI Access

### 2.0 INTRODUCTION

This section identifies persons entitled to TSCA CBI access and addresses requirements that must be met in order to obtain, maintain, or terminate certification to work with TSCA CBI.

**Legal access** to TSCA CBI is dependent on meeting the conditions found in Section 14 of TSCA. For federal employees, qualification for access is contingent on having federal employment and a job-related need for access to TSCA CBI. For contractor employees, qualification for access is contingent on employment with a TSCA-related federal contractor, a job-related need for access to TSCA CBI, and maintaining up-to-date administrative certification.

Federal and contractor employees who have an official job-related need for TSCA CBI access are, however, required to complete an initial administrative certification when receiving their new job assignment, prior to working with TSCA CBI. Moreover, these employees are required to complete an annual re-certification process for each year thereafter for as long as their jobs require access to TSCA CBI.

**Administrative TSCA CBI access, in every case, is granted solely to further the needs and the mission of the Government.**

Members of the following groups are not federal employees and, consequently, are not eligible for TSCA CBI access:

- Volunteers (unpaid staff)
- Students (except those in the Student Temporary Employment Program (STEP) – popularly known as Stay-In-Schools, who are federal employees)
- Student Interns who are placed in EPA facilities by the Environmental Careers Organization (ECO) and other recipients of EPA grants and cooperative agreements
- Senior Environmental Employment (SEE) program enrollees
- National Older Worker Career Center (NOWCC) staff
- Grantees

## 2.1 TSCA CBI ACCESS FOR FEDERAL EMPLOYEES: CERTIFICATION, MAINTENANCE, SUSPENSION, AND TERMINATION

The following administrative procedures, which are necessary for access, apply to federal employees who will work with TSCA CBI for the first time, or who have let their certification lapse:

- View the Security briefing: A federal employee's immediate supervisor is responsible for ensuring that the employee has read this manual and viewed the security briefing on procedures for handling TSCA CBI. The briefing, either automated or on videotape, is arranged by the OPPT Document Control Officer (DCO) or the employee's DCO.
- Complete one or both of the following forms (depending on the extent of access needed) and submit them to the DCO:

1. **Form 7740-6:** TSCA CBI Access Request, Agreement, and Approval. [See **APPENDIX A.**]

*[Note: Notwithstanding the Privacy Act statement which appears in the 9-92 version of **Form 7740-6**, providing a Social Security Number is not required under Section 14 of TSCA, and is not mandatory to obtain access to TSCA CBI. Upon request at the time of initial access, an alternate generic number may be assigned].*

2. **Form 7740-25:** TSCA CBI Automated Data Processing (ADP) User Registration Form (if online access to a TSCA CBI system or database is required). [See **APPENDIX B.**]

- Employee's immediate supervisor ensures that the employee has read this *TSCA CBI Protection Manual* and viewed the security briefing.
- Employee's immediate supervisor signs line 20 of **Form 7740-6** (general access request form) to signify approval of TSCA CBI access and forwards it to the DCO, or disapproves access.

- DCO reviews forms for completeness and forwards them to the OPPT DCO. *[In general, the DCO assists employees with obtaining and maintaining TSCA CBI certification.]*
- Subject to the oversight of the IMD Director, the OPPT DCO reviews and approves access and adds the employee's name to the TSCA CBI Authorized Access List.

*[The OPPT DCO provides monthly updated lists to DCOs and can verify which employees are on the latest list. The CBIC uses the list in conjunction with the Confidential Business Information Tracking System (CBITS) to verify access.]*

## 2.1.1 Re-Certification For Federal Employees

The OPPT DCO notifies DCOs of persons whose certifications are about to expire. Federal employees who need TSCA CBI access in connection with their official duties must renew their certification every year by:

1. Viewing the security briefing videos and
2. Completing the document audit procedure.

### 2.1.1.1 Document Audit

The following steps must be taken:

1. Employee's DCO provides list of all documents logged out to the employee. The federal employee's immediate supervisor ensures the Document Audit is completed.
2. Employee reconciles the document list by following the steps below:
  - Verify that he/she has the listed documents in his or her possession, OR
  - Return logged-out documents **which are overdue** to the DCO, AND
  - Notify the DCO of any unaccounted for documents, and report them on the Document Reconciliation Certificate (see **APPENDIX E**), OR
  - Indicate on the Document Reconciliation Certificate that no documents are logged out, AND

- Sign the Document Reconciliation Certificate, to be placed in the employee's access file for future audit.
3. If the employee fails to locate any unaccounted for documents, he or she must follow the procedures in **CHAPTER 5** concerning unaccounted-for documents.

All returned documents must be re-entered into the collection of records.

### **2.1.1.2**                      *Time For Re-Certifying*

The time for re-certifying access to TSCA CBI is no more than 30 days prior to an employee's anniversary date. Employees who re-certify within this period will retain their anniversary dates. Re-certifying prior to the 30 day window or after the anniversary date will result in a new corresponding anniversary date.

## **2.1.2 Failure to Maintain Access Certification**

Federal employees who miss their annual deadline to re-certify under the TSCA CBI protection program and who continue to have access to TSCA CBI as part of their official responsibilities are in violation of these procedures and are subject to the corrective actions and administrative penalties outlined in **CHAPTER 5**. [This violation of administrative procedure is not, however, reportable to the information submitter as an unauthorized disclosure under Section 14 of TSCA].

### **2.1.2.1**                      *Suspension and Termination*

Employees who are 29 or fewer days late in renewing their certification are suspended from receiving access to TSCA CBI. Employees who are 30 days or more late in renewing their certification are terminated from receiving access to TSCA CBI as part of their official duties.

Employees who have had their access terminated must repeat initial certification, not simply re-certification, in order to once again receive official access.



## 2.1.3 Suspension of Log-Out Privileges

If logged-out documents are overdue or are not returned or accounted for as required during the annual Document Audit procedure (see **Section 2.1.1**), an employee's privilege to log out CBI documents from secured reference areas such as the CBIC may be suspended. Once the documents at issue are returned or accounted for, borrowing privileges will be restored.

## 2.1.4 EPA Employee Transfers

The OPPT DCO must be notified when an EPA employee officially transfers to another branch, division, or office, if the new position requires TSCA CBI access. The employee will be required to perform a document reconciliation and return all CBI documents to the CBIC prior to receiving access for the new position. Upon completion of these two requirements, complete access to CBI materials will be available.

### 2.1.4.1 Supervisors' Responsibilities When Employee Transfers

It is the responsibility of the employee's former supervisor or DCO to notify the OPPT DCO of the transfer. In addition, the new supervisor or DCO must submit a new Form 7740-6 (**Appendix A**) for the employee.

## 2.1.5 TSCA CBI Access Termination for Federal Employees

TSCA CBI access terminates when the official need for access terminates, as in the following examples:

- When a federal employee leaves federal service
- When a federal employee transfers to a new federal position
- When a federal employee receives an administrative penalty, suspending employment or reassigning the employee to another federal position that does not require official need for TSCA CBI
- When a federal employee's duties change, and no longer require TSCA CBI access

- When a federal employee fails within 30 days from the anniversary date to reconcile the document audit report and attend the annual security briefing

### ***2.1.5.1 TSCA CBI Access Termination Procedures: Federal Employees***

To terminate TSCA CBI access, an employee must follow the Document Audit procedure described in the steps below. The employee receives a list of all their logged out documents from the DCO. From that list, the terminating employee must reconcile all documents in his/her possession by doing the following:

***(Both the employee's supervisor and DCO are responsible for ensuring that these steps are taken)***

- ***Either:***
  1. Return logged-out documents and magnetic media to the DCO (see **APPENDIX E**), notify the DCO of any unaccounted for documents, and report them on the Document Reconciliation Certificate, **OR**
  2. Indicate on the Document Reconciliation Certificate that no documents are logged out.
- ***In addition***, sign the Document Reconciliation Certificate, to be placed in the employee's access file for future audit.

*(If the employee fails to locate unaccounted for documents within 5 business days of the issuance to the employee of the list of items logged out to him/her, he/she must follow the procedures in **CHAPTER 5** concerning unaccounted-for documents.)*

- Receive from the DCO a copy of the Confidentiality Agreement the employee signed when first assigned or hired to work with TSCA CBI. Sign and receive a copy of a receipt for the form entitled, "*Confidentiality Agreement for United States Employees Upon Relinquishing TSCA CBI Access Authority.*" [See **APPENDIX F**],
- Complete EPA Form 7710-17: "*Confidentiality Agreement for United States Employees upon Relinquishing TSCA CBI Access Authority.*" [See **APPENDIX F**].

### **2.1.5.1(a) DCO And Supervisor Responsibilities For Access Termination**

The DCO will take action on unaccounted for documents. In the case of a dispute between the employee and DCO about whether a document is logged out, the document will be considered possibly unaccounted for, and will be reported as such in accordance with the Manual Procedures in CHAPTER 5.

The DCO must change the lock combinations for storage containers to which the employee had access and remove any CBI from the employee's desk area before any new staff arrive.

### **2.1.5.1(b) OPPT DCO Responsibilities For Access Termination:**

- Upon notice from the employee's DCO, remove the employee's name from the TSCA CBI Authorized Access List.
- Arrange with IMD to invalidate the employee's TSCA CBI computer user IDs and passwords for all TSCA CBI-related computer systems. IMD is responsible for notifying the OPPT DCO in writing when the employee's passwords are invalidated.
- Make immediate arrangements to invalidate the employee's electronic entry ID card for TSCA CBI Secure Storage Areas (SSA's).

## **2.1.6 Unaccounted For Documents**

The Facility DCO must assume that a TSCA CBI document is unaccounted for if it is not received within 5 business days of issuing the employee the list of items logged out to him/her and report the document as unaccounted for according to the procedures in CHAPTER 5.

## **2.2 TSCA CBI ACCESS FOR CONTRACTORS AND CONTRACTOR EMPLOYEES: CERTIFICATION, MAINTENANCE, TERMINATION AND INDUSTRY NOTICE**

The EPA Project Officer (PO) determines if, under TSCA Section 14(a), a contractor requires access to TSCA CBI.

### **2.2.1 Determination of TSCA CBI Access for Contractors**

To establish access for a contractor the PO submits Form 7740-17: *Request for Approval of Contractor Access to TSCA CBI* (**APPENDIX H**) to the appropriate division director (or equivalent supervisor) for signature, then forwards it to the IMD Director who issues final approval in the form of a notice (as described in **Section 2.2.4.**).

For new contracts (or to modify an existing contract) Form 7740-17 must be submitted to the IMD Director 20 business days before access is to begin. Form 7740-17 is submitted to the IMD Director prior to the modification request.

The PO also must complete the following:

- Notify EPA's Office of Acquisition Management (OAM) contracting officer of required TSCA CBI language, including the following contract clauses from the EPA Acquisition Regulation 1901 (9/12/2000):
  - Data Security for TSCA CBI (EPAAR 1552.235-78) (see **APPENDIX I**)
  - Access to TSCA CBI (EPAAR 1552.235-75) (see **APPENDIX J**)
  - Treatment of CBI (EPAAR 1552.235-76) (see **APPENDIX K**);
- Forward Form 7740-17 to OAM after the IMD Director has signed it; and
- At least 60 days prior to the date access is to begin complete a Contractor Information Sheet, Form 7740-27 (see **APPENDIX L**) and forward it to the OPPT DCO.

## 2.2.2 Approval for TSCA CBI Access or Expedited Approval for Immediate Access.

The OPPT DCO will add a contractor's name to the TSCA CBI Authorized Access List when the contractor is approved for CBI access. For contractor employees, the OPPT DCO will notify the contractor DCO of the approval of an employee by sending the contractor DCO the TSCA CBI Authorized Access List.

When a programmatic need can be demonstrated, **expedited approval** may be granted by the IMD Director which will allow a contractor and/or contractor employee access to TSCA CBI without having to wait 60 days after Form 7740-27 is submitted to the OPPT DCO. Expedited approval does not waive the requirement for the advance notice provided in Section 2.2.4.

See **APPENDIX M** for a Contractor Checklist for TSCA CBI Access.

## 2.2.3 Rules for Contractors

Contractors who receive TSCA CBI must:

- Adhere to the terms of their contracts regarding site requirements for receiving and maintaining TSCA CBI.
- Maintain TSCA CBI in a secure environment that meets or exceeds the requirements in **CHAPTER 4**.
- Maintain the “two-barrier” system described below for establishing any TSCA CBI storage site not located at a federal agency facility:

### **Barrier 1:**

- Perimeter walls must be constructed “slab to slab,” and must not have false ceilings that would permit entry into the contractor's workspace from over a corridor wall.
- Entry and exit doors must have pin-tumbler deadbolt locks or equivalents installed (unless the door is for emergency exit in which case it must have a crash bar with an audible alarm).

- Entry and exit doors must have exposed hinge pins that are pinned or otherwise constructed to prevent removal of the pins.

**Barrier 2:**

- Must have approved storage containers as described in **Section 4.3.3.**
- Arrange for a site inspection by TSS. TSCA CBI access will not be authorized at the contractor's site without TSS approval. TSS will communicate its approval to the OPPT DCO. (Contractors should contact TSS if they have any questions about establishing or maintaining TSCA CBI security.)

## **2.2.4 Notice to Affected Businesses Prior To Granting Access**

### 1) *HOW*

IMD will notify affected businesses in one of the following ways prior to granting TSCA CBI access to contractors:

- Publishing a notice in the Federal Register
- Sending an individual Notice by certified mail-return receipt requested
- Sending an individual Notice by telegram
- Using any other means to give actual notice, and documenting the fact that such notice was received.

#### ***The Notice process:***

- OPPT DCO uses the Contractor Information Sheet from the PO to prepare the Notice
- IMD Director signs the Notice, authorizing access for the contractor.

### 2) *WHEN*

IMD must wait at least 5 business days following receipt or publication of the Notice before granting access in order to allow the affected business an opportunity to comment.

### 3) *WHAT*

The Notice must include the following:

- Contractor company's identity
- Contract number
- Explanation of why TSCA CBI access is necessary for the performance of the contract
- Where access is authorized (on EPA premises and/or at the contractor's facility)
- Types of information to be disclosed
- Period of time for which TSCA CBI access is authorized

## **2.2.5 Requirement for Contractor DCO**

Each contractor with TSCA CBI access at either the contractor's facility or an EPA facility must have a contractor DCO who must be designated before the contractor is allowed access to TSCA CBI.

The contractor must nominate one DCO and one Alternate DCO, and notify the EPA PO of their names. The EPA PO nominates the employees and forwards their names, telephone and fax numbers and e-mail and mailing addresses to the OPPT DCO. [See [3.2.1](#)]

## **2.2.6 TSCA CBI Certification for Contractor Employees**

Following certification of TSCA CBI access for contractor companies, contractor employees must obtain individual access certification. All certification forms are available through the OPPT DCO. See **APPENDIX N** for a Contractor Employee Checklist for TSCA CBI Access.

After completing the above requirements (sections [2.2.1](#), [2.2.2](#), [2.2.3](#), [2.2.4](#), [2.2.5](#)), the EPA PO, EPA Delivery Order Project Officer (DOPO), or the EPA WAM confers with contractor officials to determine which contractor employees require TSCA CBI access certification. The EPA PO will request access certification for these individuals.

After contractor employees are certified for TSCA CBI access, they are listed on the TSCA

CBI Authorized Access List. The list provides the names of people cleared for TSCA CBI access, including TSCA CBI computer access, and the date on which their access expires. The OPPT DCO provides monthly copies of the updated list to DCOs. If after consulting the list questions remain about a person's TSCA CBI certification, consult the OPPT DCO.

## 2.2.7 Initial Certification for Contractor Employees

Contractor employees acquire initial certification according to the process described below:

- The employee views the security briefing on procedures for handling TSCA CBI. The contractor DCO is responsible for ensuring that contractor employees read this Manual and view the security briefing. The briefing is arranged by the OPPT DCO or any DCO.
- The employee completes the following forms and submits them to the contractor DCO:
  - **Form 7740-6:** TSCA CBI Access Request, Agreement, and Approval [see **APPENDIX A**].  
  
*[Note: Notwithstanding the Privacy Act statement which appears in the 9-92 version of **Form 7740-6**, providing a Social Security Number is not required under Section 14 of TSCA, and is not mandatory to obtain access to TSCA CBI. Upon request at the time of initial access, an alternate generic number may be assigned].*
  - **Form 86:** Questionnaire for National Security Positions (see **APPENDIX O**).
  - **FD-258:** Fingerprint card (two originals) (see **APPENDIX P**).
  - **Form 7740-25:** TSCA CBI ADP User Registration Form (for online access to a TSCA CBI system or database) (see **APPENDIX B**).
- The contractor DCO reviews forms for completeness and forwards them to the EPA PO.
- The EPA PO either signs line 20 of the general access request form, indicating approval, or disapproves access.
- The EPA PO submits the approved forms to the OPPT DCO for review and approval on that level.

[See **APPENDIX N** for a Contractor Employee Checklist for TSCA CBI Access.]



## 2.2.8 National Agency Check & Inquiries (NACI)

All contractor employees who are granted access to TSCA CBI must successfully pass a NACI background check to maintain TSCA CBI clearance. NACI investigations are conducted by the U.S. Office of Personnel Management at the request of the EPA Office of Administration and Resource Management, usually several weeks following the contractor employee's grant of access. The EPA PO or WAM must ensure the NACI investigation requirement is placed in the official Statement Of Work (SOW).

## 2.2.9 TSCA CBI Re-Certification for Contractor Employees

The OPPT DCO notifies DCOs of persons whose certifications are about to expire. Contractor employees who continue to require TSCA CBI access in connection with their job-related duties must renew their certification every year by:

1. Viewing the security briefing videos, and
2. Completing the document audit procedure below.

### 2.2.9.1 Document Audit

The following steps must be taken:

1. The Contractor DCO provides a list of all documents logged out to the contractor employee.
2. The Contractor employee reconciles the DCO document list by following the procedures below:
  - Return logged-out documents listed on the Document Reconciliation Certificate to the Facility DCO (see **APPENDIX E**), AND
  - Notify the DCO of any unaccounted for documents, and report them on the Document Reconciliation Certificate, OR
  - Indicate on the Document Reconciliation Certificate that no documents are logged out.
  - Sign the Document Reconciliation Certificate, to be placed in the contractor employee's access file for future audit.

3. If the employee fails to locate the documents, he/she must follow the procedures in **CHAPTER 5** concerning unaccounted for documents.

All returned documents must be re-entered into the collection of records.

### **2.2.9.2** *Time for Re-Certifying*

The time for re-certifying TSCA CBI is no more than 30 days prior to an employee's anniversary date. If an employee re-certifies within this period, the employee will retain the same anniversary date. Re-certifying either prior to the 30 day window or following the anniversary date will result in a new corresponding anniversary date.

## **2.2.10 Failure to Maintain Access Certification for Contractor Employees**

Contractor employees who miss their annual deadlines to re-certify under the TSCA CBI security program and who continue to have access to TSCA CBI are in violation of these procedures, and subject themselves to disciplinary or corrective action by their contractor employer.

Contractor employees who have not re-certified for TSCA CBI access within the past year must pass initial certification, not re-certification. EPA may suspend the access of any contractor employee if in the Agency's judgment doing so is necessary to protect TSCA CBI against some credible threat of loss or wrongful disclosure. For contractor employees a lapse in certification access may result in an unauthorized disclosure reportable to the submitter as described in **CHAPTER 5**.

There is no need, however, to obtain a new NACI or to be re-fingerprinted, if the employee never left the contractor's employment. This provision applies when both of the following conditions are true:

- The contractor continues to hold a TSCA-related contract.
- The contractor employee's job requires access to TSCA CBI.

## 2.2.11 TSCA CBI Access Termination: Contractor Employees

TSCA CBI access terminates for a contractor employee under various conditions. For example:

- When the contract ends.
- When a contractor employee leaves the contractor's employ.
- When a contractor employee transfers to a new position which does not require TSCA CBI access.
- When a contractor employee receives an administrative penalty from the contractor suspending employment or the contractor employee is reassigned within the company to another position which does not require TSCA CBI access.
- When a contractor employee's job duties change and he/she no longer requires TSCA CBI access.
- When EPA suspends TSCA CBI access for a contractor employee under **CHAPTER 5** of this Manual.
- When a contractor no longer needs access for the successful completion of an Agency Task.

### ***2.2.11.1 TSCA CBI Access Termination Procedures: Contractor Employees***

To terminate access to TSCA CBI, the contractor employee must follow the Document Audit procedure described in the steps below. See **APPENDIX Q** for a Checklist of Procedures for Terminating Contractor Access to TSCA CBI.

- The contractor DCO provides a list of all documents logged out to the contractor employee. From that list, the contractor employee must reconcile all documents in his/her possession by doing the following:
  - ***Either*** return logged-out documents listed on the Document Reconciliation Certificate to the contractor DCO (see **APPENDIX E**), notifying the contractor DCO of any unaccounted for documents, and report them on the Document

Reconciliation Certificate, OR

- Indicate on the Document Reconciliation Certificate that no documents are logged out.
- ***In addition***, sign the Document Reconciliation Certificate, to be placed in the contractor employee's access file for future audit.

*If the contractor employee fails to locate any of the listed documents within 5 business days of the issuance to the employee of the list of items logged out to him/her, he/she must follow procedures for reporting lost documents in **CHAPTER 5**. Both the contractor employer and the contractor DCO are responsible under the terms of the contract for assuring this procedure is completed. In addition, Prior to termination of the TSCA contract, contractor DCOs are responsible for reconciling TSCA CBI 14 calendar days before the termination date.*

***The Contractor DCO must also:***

- Request that the OPPT DCO remove the contractor employee's name from the TSCA CBI Authorized Access List.
- Make immediate arrangements to invalidate the contractor employee's electronic entry ID card for TSCA CBI.
- Change the combinations to locks for any TSCA CBI storage containers to which the contractor employee had access.
- Provide contractor employee with copy of Confidentiality Agreement (Form 7740-6) signed at the inception of assignment and obtain the contractor employee's signature on the "Confidentiality Agreement for Contractor Employees Upon Relinquishing TSCA CBI Access Authority" Form 7740-18. (See **APPENDIX R**.)
- Remove any CBI from the contractor employee's desk area before new staff occupies the desk.

The OPPT DCO must arrange with IMD to invalidate the contractor employee's TSCA CBI computer user ID code and passwords for all TSCA CBI-related computer systems to which the contractor employee had access. IMD is responsible for notifying the OPPT DCO in writing when the contractor employee's passwords are invalidated.

### ***2.2.11.2 Unaccounted For Documents***

The contractor DCO must assume that a TSCA CBI document is unaccounted for when it is not received within 5 business days of issuing the contractor employee the list of items logged out to him/her, and report this fact under the procedures in **CHAPTER 5**.

## **2.2.12 Change In Corporate Status**

When a contractor or subcontractor with access to TSCA CBI is acquired by or merged into another company (or otherwise alters its corporate status by associating in some way with another company) it shall provide notice to EPA prior to the transaction. EPA will allow the contractor or subcontractor 30 days from the time of notice to complete the corporate and employee TSCA CBI clearance procedures discussed in this section **2.2** above. If the required notice is not given within 90 days of the transaction, then access during that time will be considered unauthorized, and the Agency will follow the unauthorized disclosure procedures in Chapter 5.

## **2.3 TSCA CBI ACCESS CERTIFICATION FOR OTHER FEDERAL AGENCIES**

Access to TSCA CBI data may be granted to other federal agencies under the following circumstances:

- When TSCA CBI data is required to perform work for EPA.
- When TSCA CBI data is required to perform the other agency's legal duties to protect health or the environment.
- When TSCA CBI data is required for specific law enforcement purposes.

All persons contemplating disclosure of TSCA CBI to other federal agencies should review the regulations at 40 CFR Sections 2.209(c) and 2.306.

### **2.3.1 Procedures for Other Federal Agencies to obtain TSCA CBI Access**

Other federal agencies may obtain access to TSCA CBI by following the applicable requirements outlined in 40 CFR 2.209(c), and including taking the following steps:

An authorized agency representative must submit a written request to the IMD Director preferably at least one month before access is to begin. The request must specify the following:

- Information to which access is requested.
- Reason(s) why access is necessary (including the official purpose).
- Supporting details.

The request must be signed by an agency official whose authority is at least equivalent to that of an EPA division director.

The IMD Director reviews the TSCA CBI access request and notifies the agency's requesting official of his/her decision. If access is approved, the IMD Director informs the agency of the following stipulations:

- TSCA CBI is being disclosed under TSCA authority
- Unauthorized disclosure of the information may subject the agency's employees to criminal penalties in Section 14(d) of TSCA (see **CHAPTER 5**)
- The agency seeking TSCA CBI access must provide written agreement that it will not disclose TSCA CBI, except in any one of the following situations:
  - (i) The agency has statutory authority both to compel production of the information and to make the proposed disclosure, and it has furnished affected businesses with at least the same notice that EPA would provide under EPA regulations.
  - (ii) The agency has obtained the consent of each affected business prior to the proposed disclosure.

- (iii) The agency has obtained a written statement from the EPA general counsel, or an EPA regional counsel, that disclosure of the information is authorized under EPA regulations.

[**Note:** If the other federal agency is obtaining access to TSCA CBI for purposes not on behalf of EPA, notice must first be provided to affected businesses as provided in Section **2.3.2** just below].

Once access has been granted, designated employees of the other federal agency can obtain access to specified TSCA CBI on EPA premises. The procedures for individual employees to obtain certification for TSCA CBI access are explained in **Section 2.1** of this Manual. Employees of other federal agencies are not allowed to remove from EPA premises any documents, notes, or correspondence containing TSCA CBI and must not discuss TSCA CBI with unauthorized individuals. Only a DCO may remove TSCA CBI from EPA premises. TSCA CBI must therefore be transferred from an EPA DCO to a Facility Agency DCO.

When a programmatic need can be demonstrated (and when the other federal agency needs TSCA CBI access to perform a function on behalf of EPA) **expedited approval** may be granted by the IMD Director which will allow a federal agency access to TSCA CBI before receiving final approval from the OPPT DCO.

## 2.3.2 Notice to Affected Businesses

Before granting TSCA CBI access to another agency, in order to do work **not** on behalf of EPA, IMD provides written Notice to affected businesses. The Notice must be given at least 10 calendar days before access can be granted via publication in the *Federal Register*, telegram, or certified mail (return receipt requested). No Notice to affected businesses is required however, when EPA discloses TSCA CBI to another agency to perform work for EPA (as described in 40 CFR Sections 2.209(c) and 2.306(h)).

IMD will prepare the Notice, which must include the following:

- Identity of the agency to which TSCA CBI access is granted.
- Official purpose for the access.
- If access is authorized on EPA premises or at the other agency's facilities (see **Section 2.3.3**).
- Types of information to be disclosed.
- Period of time for which access to TSCA CBI is authorized.

### 2.3.3 Security Requirements at Other Federal Agencies

In order for the other agency to obtain access to TSCA CBI on its own premises, the requesting official to whom TSCA CBI is to be transferred, must nominate at least two people as a DCO and an Alternate DCO (ADCO). The nomination, submitted in writing to the OPPT DCO for approval, must include the names, telephone and fax numbers, and e-mail and mailing addresses of the nominees. The requesting official or the DCO can also nominate ADCOs to assist the DCO in day-to-day operations. ADCOs can perform the same duties as DCOs (including signing EPA Form 7740-28).

The following are required for TSCA CBI access on the other agency's premises:

- Agency security procedures and standards that equal or surpass those set forth in this manual. The requesting official must provide to TSS a written statement of the agency's security procedures for handling TSCA CBI. The statement should state that the security procedures in this Manual have been adopted, or how the security procedures used by the agency differ from those in this Manual.
- EPA TSS inspection and approval of the agency's TSCA CBI storage facilities. The inspection is to be arranged by the requesting official.

[NOTE: TSS will not be required to inspect facilities in other federal agencies where CBI is stored in approved storage containers as referenced in **Section 4.3.3.**]

## 2.4 REQUESTS FROM CONGRESS OR THE GENERAL ACCOUNTING OFFICE (GAO)

EPA, federal, and contractor employees must notify the IMD Director immediately when they receive a request from Congress or the GAO for information that requires access to TSCA CBI. Pursuant to 40 CFR 2.209, TSCA CBI access is allowed only when the request is made by the Speaker of the House of Representatives, the President of the Senate, a chairman of a Congressional committee or subcommittee, or the Comptroller General. All document access will be provided by the OPPT DCO, who will record all transactions on the Federal Agency, Congress, and Federal Court Sign-Out Log, Form 7740-24 (see **APPENDIX S**).

- When EPA allows access to TSCA CBI by Congress or the GAO, EPA must provide written notice to affected businesses at least 10 calendar days prior to disclosure unless Congress or GAO directs otherwise or does not give



sufficient time. In the latter case, notice shall be given as promptly as possible [see 40 CFR 2.209(b)(2)]. Such notice may be given via publication of a Notice in the *Federal Register*, or via telegram or certified mail (return receipt requested). IMD will prepare the Notice, which must include:

- Whether access is authorized on EPA premises or at the other agency's facilities
- Type of information to be disclosed
- Period of time for which need for access to TSCA CBI is expected.

This page intentionally left blank

# CHAPTER 3

## TSCA CBI Responsibilities

### 3.0 INTRODUCTION

Proper protective controls must be followed by employees of EPA, other federal agencies, and contractors with access to TSCA CBI who handle, store, or transfer any TSCA CBI.

### 3.1 EMPLOYEE RESPONSIBILITIES

#### 3.1.1 Personal Accountability

EPA holds every employee with access to TSCA CBI access personally responsible for adhering to the handling and security procedures in this Manual.

#### 3.1.2 Assuring Adequate TSCA CBI Protection

Each employee with TSCA CBI access is required to inform management immediately if he/she discovers that any procedure in this manual does not provide adequate protection for TSCA CBI. In addition, those employees are encouraged to suggest changes to improve protection.

#### 3.1.3 Reporting Procedural Violations

Each employee who has access to TSCA CBI is required to report immediately in writing any potential violations of these procedures to his/her immediate supervisor, and if applicable, the Contractor PO (see **Section 5.1**).

### **3.1.4 Document Accountability**

Employees are accountable for all TSCA CBI received from a DCO or other TSCA CBI-authorized employee, printed from the TSCA CBI LAN, or recorded on magnetic, optical, or other storage medium.

### **3.1.5 TSCA CBI Procedure Accountability**

Employees are required to adhere to the procedures established by management and their DCO for protecting and handling TSCA CBI to prevent disclosure to anyone not authorized under TSCA Section 14 for access to CBI.

### **3.1.6 Return TSCA CBI Document**

Employees are permitted to log out TSCA CBI documents from their DCO and to keep the documents in an approved storage container as defined in **Section 4.3.3**, or approved SSA as defined in **Section 4.3.1**, for up to a year. Employees must return TSCA CBI to the DCO as soon as the material is no longer needed.

Any material kept longer than a year is considered overdue; the DCO will notify the employee responsible. Materials that are not returned to the DCO within 14 days of notification are presumed to be unaccounted for. The DCO must notify his/her division director of unaccounted for materials, pursuant to the procedures in **CHAPTER 5**. If the employee does not return overdue materials to the DCO within 14 days of notification, the employee's access to TSCA CBI may be suspended. Once the documents at issue are returned or accounted for, CBI access will be restored.

### **3.1.7 Determination of TSCA CBI**

It is an employee's responsibility to decide if an existing document submitted to the Agency, or a document newly created by the employee, contains TSCA CBI. An employee who is unable to determine if a document is CBI should consult with his/her supervisor or DCO. If the issue remains unresolved, the employee should consult the chief of the IMD Records and Dockets Management Branch (RDMB), or equivalent.

### **3.1.8 Receipt of Possible CBI**

If an employee receives materials (labeled or unlabeled CBI) via mail or other means which appear to be TSCA CBI, he/she must immediately take those materials to the DCO for assessment and, if warranted, entry into the Document Tracking System (DTS). [See **Section 4.1.1**].

## **3.2 MANAGER RESPONSIBILITIES**

Program and office managers must continually ensure the following:

- Adequate personnel are available to carry out the DCO and ADCO responsibilities under the manager's supervision
- Proper physical control measures are implemented in areas where TSCA CBI is maintained and tracked
- Subordinate POs, DOPOs, and WAMs follow TSCA CBI security procedures while administering contracts
- Quarterly meetings are held with contractor POs to ensure that contractor employees are following TSCA CBI security procedures
- Employees under their supervision who require TSCA CBI access maintain current certification.

### **3.2.1 Assigning a DCO and ADCO**

The EPA manager (or Project Officer for the contractor DCO – see **2.2.5**), is responsible for nominating two employees to act as the DCO and alternate DCO, respectively. The manager (or Project Officer) must submit this nomination to the OPPT DCO. The nomination, submitted in writing, must include each nominee's name, telephone number, e-mail address, fax number, and mailing address. The contractor DCO must be in place before the contractor is allowed access to TSCA CBI.

## **3.3 DCO RESPONSIBILITIES**

DCOs manage their facilities' Document Tracking Systems (DTS) and oversee the receipt, storage, transfer, and use of TSCA CBI by employees in their facilities.

### **3.3.1 DCOs and Alternate DCOs**

All facilities authorized for TSCA CBI access must have at least one DCO and an ADCO; other ADCOs may be assigned.

DCOs and Alternate DCOs must be approved by the OPPT DCO before transfer of CBI to any facility. In addition, the OPPT DCO is responsible for providing guidance to all DCOs and ADCOs on appropriate document handling procedures.

### **3.3.2 Maintaining a Document Tracking System (DTS)**

The DCO is responsible for implementing and maintaining a Document Tracking System for his/her respective facility, to track the receipt, use, and transfer of TSCA CBI. All TSCA CBI submitted to EPA, and any produced by federal and contractor employees (except as described in **Section 4.4**), are monitored through a facility DTS (See **Section 4.2** on the requirements for a DTS).

### **3.3.3 Transfer of TSCA CBI**

A DCO must approve the transfer of TSCA CBI to a federal or contractor facility according to procedures in **CHAPTER 4**. In order to transfer a copy of a TSCA CBI submission to a requesting submitter, the submitter must provide to EPA a letter on corporate stationery which is signed by a designated corporate official indicating the person authorized to receive the copy (unless a designated representative is already on file). This letter should be submitted to the OPPT DCO.

The DCO may send TSCA CBI by courier or certified mail (with return receipt) in accordance with procedures in **CHAPTER 4** of this manual. The DCO must notify the receiving DCO before sending the TSCA CBI.

### 3.3.4 Receiving TSCA CBI

The receiving DCO must review incoming TSCA CBI for completeness. If the documents appear incomplete, the DCO must immediately contact the submitter to determine if there was an omission. If the materials appear to be complete, the DCO will do the following:

1. Stamp the document as TSCA CBI (see **APPENDIX T**). The stamp is applied to the front page, and the blank back page (if not blank, the blank back cover).
2. Assign a DCN, if one has not already been assigned.
3. Attach a TSCA CBI cover sheet (see **APPENDIX U**) to the front of the document. The DCO must write the DCN on the cover sheet and first page of the document unless the document is transferred to the CBIC.

### 3.3.5 Proper Storage of TSCA CBI

DCOs are responsible for ensuring that employees at their facilities are storing documents properly. [Procedures on storing TSCA CBI can be found in **Section 4.3**].

If an employee who works in an SSA will be out of the office for more than 7 calendar days, all TSCA CBI in his/her possession must be locked away in an approved TSCA CBI storage container. If the employee is unable to do this due to illness or other reason, the employee's supervisor or DCO will ensure the materials are stored in accordance with procedure. [See, specifically, **Section 4.3.4, Employee Absence and Storage of TSCA CBI** and **Section 4.3.1.8, Using TSCA CBI outside an SSA**].

The DCO supervises the storage of TSCA CBI in secure storage containers or in a centralized secure TSCA CBI storage area (**Section 4.3**). The responsibilities of the DCO and employee apply to CBI stored on paper or in digital form on magnetic disks, optical disks, or other medium. One exception to this requirement is when an employee's duties require that he/she be assigned individual responsibility for a specific secure storage container within an office (such as a Mosler safe or bar lock cabinet).

### 3.3.6 Records of Lock-Combinations

DCOs and other designated persons have the following responsibilities in maintaining records of lock combinations for rooms and containers in which TSCA CBI is stored:

- DCOs must maintain a list of combinations for TSCA CBI storage containers and rooms controlled by a particular division, facility, program, or office

- The OPPT DCO must maintain a list of combinations for containers and rooms assigned to IMD, and for all containers and rooms in OPPT not under any specific division's control
- Facilities Management Services Division must maintain a master list of combinations for all TSCA CBI locks at EPA Headquarters.

### **3.3.7 Conditions For Changing Lock Combinations**

The DCO is required to change lock combinations annually or if any of the following occurs:

- Each time a person who knows a combination relinquishes his/her TSCA CBI access authority
- When a storage container is put into, or taken out of operation
- If there is a known or possible compromise of TSCA CBI data in the storage container.

If any of the above three events occur, DCOs at EPA Headquarters must notify FMSD, which is responsible for changing the lock combinations.

### **3.3.8 Updating The TSCA CBI Authorized Access List**

Each DCO bears responsibility for keeping the TSCA CBI Authorized Access List current. By the 15th of each month DCOs must notify the OPPT DCO of any for whom they are responsible who should be added to or deleted from the list.

### **3.3.9 Monitoring And Controlling Release of TSCA CBI**

DCO steps for providing TSCA CBI are described below:

- The DCO receives a request from an employee for a specific TSCA CBI document.
- The DCO locates the document and notifies the requesting employee.



- When the employee is ready to receive the document, the DCO verifies the requesting employee's TSCA CBI certification by checking the TSCA CBI Authorized Access List.
- The DCO logs the document out to the employee using an automated or manual document Inventory Log. See **APPENDIX V**.

### **3.3.10 Overdue Materials: Monitoring And Notification**

The DCO monitors TSCA CBI, and notifies employees and supervisors when it becomes overdue. DCOs must monitor the Inventory Log for TSCA CBI materials which have not been returned within the **required** one-year period. The DCO will notify employees and their supervisors of overdue materials by distributing to each a list of all TSCA CBI documents logged out to the employee before the annual security briefing and TSCA CBI re-certification are accomplished. Any material kept longer than a year is considered overdue; the DCO will notify the employee responsible. Materials that are not returned to the DCO within 5 days of notification are presumed unaccounted for. The DCO must notify his/her division director of unaccounted-for materials pursuant to the procedures in **CHAPTER 5**. If the employee does not return overdue materials to the DCO within 14 days of notification, the employee's access to TSCA CBI may be suspended. Once the documents at issue are returned or accounted for, CBI access will be restored. [See also sections **3.1.6 Return TSCA CBI Documents**, and **2.1.3 Suspension of Log-out Privileges**].

In general, TSCA CBI may not be logged out from a centralized TSCA CBI storage facility for more than one year without renewal. Exceptions to this rule include the following:

- Regional DCOs may receive documents as permanent log-outs
- Contractor DCOs may receive documents as permanent logouts through the end of their contract
- The OPPT DCO in certain circumstances may grant permanent log-out status to other DCO collections on an as-needed basis.

### **3.3.11 DCO Guidance In Identifying And Sanitizing CBI Documents**

The DCO assists employees in determining whether documents contain TSCA CBI and in sanitizing documents for public disclosure.

The responsibility for determining whether documents contain TSCA CBI rests with the document's originator (see **Section 4.1**). Employees who are unable to determine if something is confidential should consult with their supervisor or DCO. If the issue remains unresolved, the employee should consult the chief of IMD RDMB. The DCO also instructs document originators on how to sanitize a TSCA CBI document if the document is going to be released to the public.

The DCO controls and documents the reproduction and destruction of TSCA CBI. TSCA CBI (except for working papers as discussed in **CHAPTER 4**) are reproduced or destroyed only by a DCO or ADCO. Specific procedures for reproduction and destruction are set forth in **CHAPTER 4**.

### **3.3.12 TSCA CBI Audits**

The following section describes the requirements to audit TSCA CBI for federal and contractor entities:

#### ***3.3.12.1 Federal DCOs And The Confidential Business Information Center (CBIC)***

[NOTE: This section applies to all Federal TSCA CBI collections and the CBIC, which is managed under contract by the OPPT DCO.]

##### ***3.3.12.1(a) Comprehensive Audits of Entire Collection***

By **April 1, 2004**, each DCO must conduct an audit of all TSCA CBI in the DCO's collection as of December 31, 2003. This step must be performed every *fourth year* subsequent to the completion of the first comprehensive audit. For the intervening years, an annual transaction audit shall be conducted as outlined in **Section 3.3.12.1(b)**. As an example, the next comprehensive audit would be conducted by **April 1, 2007** for all TSCA CBI in the DCO's

collection as of **December 31, 2006**.

Each DCO must take the following steps in performing the comprehensive CBI audit:

- 1) Audit all CBI documents in the Receipt Log or equivalent automated tracking system, comparing the physical document collection with the information in the log or tracking system.
- 2) Reconcile the TSCA CBI documents in the Receipt Log with the transactions listed in the Inventory Log (e.g., shred, transferred, logged out, declassified) .
- 3) Locate any documents logged out for more than 1 year.
- 4) Verify the status of documents indicated in the Inventory Log or tracking system as having been shredded. The TSCA CBI cover sheet must be used to verify that CBI documents have been destroyed. **[NOTE: TSCA CBI cover sheets must be retained until the next comprehensive audit cycle is complete.]**
- 5) Certify that the tracking system has been updated to reflect the results of the audit.

Prior to **April 1, 2004**, and for every *fourth year* thereafter, the DCO must submit a final report to his/her supervisor or contract manager. This report must contain, at a minimum:

- Description of the audit methodology
- Total number of documents audited
- Description of any documents not located
- The tracking number (document control number) of any documents not located

The final audit report will be forwarded by the supervisor or contract manager to the OPPT DCO and TSS. If any TSCA CBI documents cannot be located during the audit, the DCO must follow the procedures outlined in **CHAPTER 5** for reporting potential violations.

### **3.3.12.1(b) Transaction Audits**

Before **April 1** of each year for which a comprehensive audit (as described in **3.3.12.1(a)**) is not required, each DCO must conduct an annual audit of TSCA CBI in the DCO's collection that consists of:

- 1) All documents initially received by the DCO between **January 1** and **December 31** of the **previous calendar year**.
- 2) All documents that were logged out and then returned to the DCO between **January 1** and **December 31** of the **previous calendar year**.

Each DCO must also:

- 3) Locate any documents logged out for more than 1 year
- 4) Verify the status of documents indicated in the tracking system or Inventory Log as shredded. The TSCA CBI cover sheet must be used to verify that CBI documents have been destroyed. [**NOTE:** TSCA CBI cover sheets must be retained until the next comprehensive audit cycle is complete.]
- 5) Certify that the tracking system has been updated to reflect the results of the audit.

Prior to **April 1**, the DCO must submit a final report to his/her supervisor or contract manager. This report must contain, at minimum:

- Description of the audit methodology
- Total number of documents audited
- Description of any documents not located
- The tracking number (document control number) of any documents not located

The final audit report will be forwarded by the supervisor or contract manager to the OPPT DCO and TSS. If any TSCA CBI documents cannot be located during the audit, the DCO must follow the procedures outlined in **CHAPTER 5** for reporting potential violations.

### **3.3.12.1(c) DCO Transition Audits**

This procedure must be followed when DCOs terminate their employment or relinquish DCO responsibilities. The outgoing DCO must perform the following steps prior to transferring any TSCA CBI to a new DCO:

- 1) Audit all CBI documents in the Receipt Log or equivalent automated tracking system, comparing the physical document collection with the information in the log or tracking system.
- 2) Reconcile the TSCA CBI documents in the Receipt Log with the transactions listed in the Inventory Log (e.g., shredded, transferred, logged out, declassified).
- 3) Locate any documents logged out for more than 1 year.
- 4) Verify the status of documents indicated in the Inventory Log or tracking system as shredded. The TSCA CBI cover sheet must be used to verify that CBI records have been destroyed. [NOTE: TSCA CBI cover sheets must be retained until the next comprehensive audit cycle is complete.]
- 5) Certify that the tracking system has been updated to reflect the results of the audit.

Prior to **transferring the collection to the incoming DCO**, the outgoing DCO must submit a final report to his/her supervisor or contract manager. This report must contain, at a minimum:

- Description of the audit methodology
- Total number of documents audited
- Description of any documents not located
- The tracking number (document control number) of any documents not located

The final audit report will be forwarded by the supervisor or contract manager to the OPPT DCO and TSS. If any TSCA CBI documents cannot be located during the audit, the incoming DCO must follow the procedures outlined in **CHAPTER 5** for reporting potential violations.

### **3.3.12.2 Contractor DCOs**

[NOTE: This section applies to all contractor TSCA CBI collections.]

#### **3.3.12.2(a) *Comprehensive Audits of Entire Collection***

By **April 1, 2004**, each contractor DCO must conduct an audit of all TSCA CBI in the DCO's collection as of **December 31, 2003**. This comprehensive audit shall be conducted for each year thereafter for all TSCA CBI in the DCO's collection as of **December 31** of the previous year.

The DCO must take the following steps in performing the CBI audit:

- 1) Audit all CBI documents in the Receipt Log or equivalent tracking system, comparing the physical document collection with the information in the log or tracking system.
- 2) Reconcile the TSCA CBI documents in the Receipt Log with the transactions listed in the Inventory Log (e.g., shredded, transferred, logged out, declassified).
- 3) Locate any documents logged out for more than 1 year.
- 4) Verify the status of documents indicated in the Inventory Log or tracking system as shred. The TSCA CBI cover sheet must be used to verify that CBI documents have been destroyed. [NOTE: TSCA CBI cover sheets must be retained until the next comprehensive audit cycle is complete.]
- 5) Certify that the tracking system has been updated to reflect the results of the audit.

Prior to **April 1**, the DCO must submit a final report to his/her supervisor or contract manager. This report must contain, at a minimum:

- Description of the audit methodology
- Total number of documents audited
- Description of any documents not located

- The tracking number (document control number) of any documents not located

The final audit report will be forwarded by the supervisor or contract manager to the OPPT DCO and TSS. If any TSCA CBI documents cannot be located during the audit, the incoming DCO must follow the procedures outlined in **CHAPTER 5** for reporting potential violations.

### **3.3.12.2(b)      *Contract closeout Audits***

Prior to contract closeout, the contractor DCO must perform a comprehensive audit of all TSCA CBI in the DCO's collection. The contractor DCO must take the following steps in performing the CBI Audit:

- 1) Audit all CBI documents in the Receipt Log or equivalent tracking system, comparing the physical document collection with the information in the log or tracking system.
2. Reconcile the TSCA CBI documents in the Receipt Log with the transactions listed in the Inventory Log (e.g., shredded, transferred, logged out, declassified).
- 3) Locate any documents logged out for more than 1 year.
- 4) Verify the status of documents indicated in the Inventory Log or tracking system as '**shredded**'. The TSCA CBI cover sheet must be used to verify that CBI documents have been destroyed.

[**NOTE:** TSCA CBI cover sheets must be retained until the next comprehensive audit cycle is complete.]

- 5) Certify that the tracking system has been updated to reflect the results of the audit.

**Two weeks prior to contract closeout**, the DCO must submit a final report to his/her supervisor or contract manager. This report must contain, at a minimum:

- Description of the audit methodology
- Total number of documents audited
- Description of any documents not located
- The tracking number (document control number) of any documents not located

The final audit report will be forwarded by the supervisor or contract manager to the OPPT DCO and TSS. If any TSCA CBI documents cannot be located during the audit, the DCO must follow the procedures outlined in **CHAPTER 5** for reporting potential violations.

### **3.3.13 Termination Of Employment Or Status For DCO**

The following procedures must be followed when a DCO terminates his/her employment, or relinquishes DCO responsibilities. They are the same for those of a DCO at EPA Headquarters, regional offices, other federal agencies, and contractor facilities.

At termination of employment or DCO status, TSCA CBI under a DCO's authority must be inventoried. The outgoing DCO and the incoming DCO must jointly perform an inventory of TSCA CBI in the outgoing DCO's collection of records. Both parties must confirm the inventory before the outgoing DCO departs. The incoming DCO should retain a copy of the inventory for audit purposes and forward a copy to the OPPT DCO.

***NOTE:** The CBIC DCO is not required to perform a collection audit if the contractor operating the Center does not change.*

## **3.4 EAD AND IMD ANNUAL REVIEW**

On an annual basis, the Office of Pollution Prevention and Toxics Information Management Division (IMD) and the Environmental Assistance Division (EAD) will report on state of the security of TSCA CBI.

The report will summarize security activities, training, and issues that may have arisen over the preceding twelve months, including violations and vulnerabilities.

Consistent with EAD's TSCA Security Staff (TSS) charge, the EAD portion will summarize



violations, the overall state of security procedures and practices, vulnerabilities, and security activities. IMD will describe policy issues, training, future needs and other related matters.

This report will be sent to the director of OPPT by January 31st of each calendar year. To create this report, in addition to reviewing reports and other generated materials, IMD and EAD will interview representatives of the major users of TSCA CBI for information on the state of TSCA security, policy and procedural issues (including opportunities for security improvements).

This page intentionally left blank

# CHAPTER 4

## TSCA CBI Document Management

### 4.0 INTRODUCTION

DCOs are vital to the effective management of TSCA CBI documents. DCOs manage their facilities' DTSS (Document Tracking Systems) and oversee the receipt, storage, transfer, and use of TSCA CBI by employees in their facilities.

### 4.1 RECEIPT OF TSCA CBI

TSCA CBI submitters should be directed to send incoming TSCA CBI to a DCO only. TSCA CBI sent between organizations must be sent from one DCO to another DCO.

#### 4.1.1 Incoming TSCA CBI

While TSCA CBI sent to OPPT (e.g., by U.S. mail, courier, or fax transmission) may be addressed to either an EPA or contractor DCO, preferably it would be addressed to the Confidential Business Information Center (CBIC). In either case, TSCA CBI must be received in accordance with the requirements of this Manual. TSCA CBI sent or otherwise misdirected to other Agency personnel should be taken immediately, to the extent practicable, to a DCO for tracking. Practical reasons may extend the time for delivering the misdirected item to the CBIC for up to 3 business days. However, the documents must be provided to the CBIC as soon as possible for incorporation into the Agency's official file.

In the case of TSCA CBI mailed from one DCO to another, a receipt must be sent back to the sending DCO identifying the contents of the package. The recipient DCO must sign the receipt of contents and return the original to the sender within 5 business days and maintain a copy of the receipt for his/her files. The receipt of contents must include the following information:

- DCN
- Description of the CBI
- Name and signature of the sending DCO and the date sent.
- Name and signature of the receiving DCO and the date received.

### **4.1.2 Personal File Copies – New Chemicals Program (OPPT-CCD)**

New Chemicals Program (NCP) staff in the OPPT Chemical Control Division (CCD) may make and keep personal file copies of documents sent by submitters to the CCD DCO before the documents go to the CBIC. The CCD DCO will maintain a log which will track all copies made and distributed with an assigned number for each copy. When each copy is no longer needed, the document will be shredded under the supervision of the CCD DCO, who will ensure proper logging of the shredded data.

### **4.1.3 Supplemental Filings – New Chemicals Program (OPPT-CCD)**

NCP staff in OPPT CCD may scan supplemental documents sent by submitters to the CCD DCO, and place them on the TSCA CBI LAN for distribution in ‘read-only’ format before the documents go to the CBIC within the timeframe specified in section **4.1.1** above. When review is complete, the CCD DCO will ensure the scanned documents are deleted from the TSCA CBI LAN.

*{NOTE: As indicated, the paragraph above refers only to supplemental information submissions. Initial filings are not to be directed to the CCD DCO, but rather processed through the CBIC.}*

### **4.1.4 Processing Newly Received TSCA CBI (applies to all DCOs and the CBIC)**

The procedure below must be followed when receiving TSCA CBI [see also, generally, **Section 4.6.1** on transferring TSCA CBI]:

- The receiving DCO should be notified in advance of what CBI is being sent.
- Review and Acceptance:

Upon receipt of a document, the receiving DCO must complete the following steps:

- (i) Review any Transfer Slip to ensure that all listed information is included.
- (ii) Log the document into the Receipt Log. See **APPENDIX W**.

- **Stamp:**

A federal or contractor employee who creates a document is responsible for stamping the document as TSCA CBI (when the document contains information claimed as TSCA CBI) or non-CBI (as appropriate) (see **APPENDIX T** for examples of each type of stamp). The stamp is applied to the front page and the blank back page (if there is no blank page, then a blank back cover). If a document appears as though it may contain CBI, treat it as CBI until its status can be verified with the author.
  
- **Cover Sheets:**

All TSCA CBI documents must have a cover sheet, Form 7740-9 (see **APPENDIX U**), that adheres to the following guidelines:

  - (i) The cover sheet must be green, clearly signifying that the attached document contains TSCA CBI, and be attached to the front of the document.
  - (ii) The DCN (written or bar code) and the date must appear on both the cover sheet and the first page of the document.
  - (iii) The originator's DCO must complete the cover sheet.
  
- **DCN Assignment:**

The Headquarters DCN should be used (or cross-referenced to any regional DCN assigned).
  
- **Notification:**

Notify the OPPT DCO, or other TSCA CBI cleared addressee(s), of the TSCA CBI submission's availability for review and/or pickup.

#### **4.1.4.1**            *CBI Fax Transmission From Industry*

When an external submitter wants to send TSCA CBI via fax transmission, he/she must be notified that EPA cannot guarantee the confidentiality of the transmission.

The recipient of the transmission must:

- Notify the sender that EPA's transmission lines are not secure and that no encryption equipment will be used to scramble the transmission.

- Remain by the fax machine until the transmission is complete, if the receiving fax machine is outside an SSA.
- Notify the sender of a successful fax transmission.
- Provide the fax to the DCO for entry into the tracking system immediately upon receipt.

### **4.1.5 TSCA CBI Claims That Appear Unwarranted**

Any employee who discovers a TSCA CBI claim which appears unwarranted may exercise independent discretion in choosing whether to refer the matter to IMD, or take any action at all (including contacting the submitter directly). Employees should follow the guidance in **Appendix EE**.

## **4.2 DOCUMENT TRACKING SYSTEM (DTS) REQUIREMENTS**

DCOs must ensure the following regarding use of a Document Tracking System (DTS):

- All manual or automated document logs are properly maintained, updated, and stored securely
- DCNs or unique alphanumeric identifiers are assigned to documents
- Proper procedures are followed when accessing TSCA CBI.

### **4.2.1 Use of an Automated Document Tracking System (DTS)**

Use of a DTS is mandatory. The IMD Director has approved several automated DTSs. Contact the OPPT DCO for additional information about these DTSs.

EPA strongly recommends an automated DTS for a DCO who oversees a high volume of documents and transactions. An automated DTS allows the DCO to track a document's movement from the time it is assigned a DCN, or is received at EPA, until the time it is destroyed or transferred to another TSCA CBI-cleared facility.

At EPA Headquarters, the OPPT DCO uses CBITS, an automated DTS, to track TSCA CBI documents. An automated DTS has the following required and optional characteristics:

***Required:***

- **Backup of automated DTSs:** When an automated DTS is used, the DCO must back up the TSCA CBI on the DTS at the end of each day, if data are added or deleted. The backup media contain TSCA CBI data and must be protected as such.
- **Record maintenance:** Any manual document logs that are converted by an automated DTS must be retained until an audit by TSS verifies the accuracy of the conversion.

***Optional:***

- **Machine-readable bar codes:** CBITS uses machine-readable barcodes to track TSCA CBI documents. The bar code is affixed to each TSCA CBI document controlled through the CBIC. Bar codes are also affixed to the electronic entry ID cards of employees using TSCA CBI. The OPPT DCO uses these bar codes to verify, through CBITS, that employees are on the TSCA CBI Authorized Access List. The OPPT DCO also uses these bar codes to produce Annual Audit Certification Reports for employees' completion.
- **Secure off-site duplicate records:** EPA also recommends securing a duplicate set of media DTS off-site to allow for recovery of documents logged out, in the event that a natural disaster such as a flood or fire occurs. Contact the OPPT DCO and TSS for assistance in establishing a disaster recovery program for your records.

## **4.2.2 Use of a Manual Document Tracking System (DTS)**

Manual systems may be used to record CBI transactions for small CBI collections. However, automated databases allow a greater degree of flexibility and search capabilities. The following forms establish the tracking and control requirements for TSCA CBI:

- EPA Form 7740-10: Receipt Log for TSCA Confidential Business Information.
- EPA Form 7740-11: Inventory Log for TSCA Confidential Business Information.

- EPA Form 7740.24: Federal Agency, Congress, and Federal Court Sign-Out Log.

[See **APPENDIX W, V, and S**, respectively for copies of these forms.]

#### **4.2.2.1**      *Receipt Log*

A Receipt Log is used to record the receipt of all incoming CBI documents into the DCO's domain.

Each document received by a DCO must be recorded in an automated or manual receipt log (**APPENDIX W**). The DCO must record the following information in the Receipt Log:

- DCN; if a DCN has not been assigned, the copy number assigned by the DCO should be recorded.
- Date on which the document was received by the DCO.
- Submitter's name (if the document was received directly from the submitter), the author's name (if the document was generated by a federal or contractor employee), or the facility DCO's name (if the document was received from another facility authorized for TSCA CBI access).
- Number of pages contained in the document.
- Brief description of the document. For example, "an engineering report on PMN-Y," or "letter from company X on PMN-W").

#### **4.2.2.2**      *Inventory Log*

An Inventory Log is used to log documents in or out to employees or contractors of EPA. It is the official record of all **in/out** transactions of CBI documents in the DCO's jurisdiction and is used to record the final disposition of these documents (e.g., permanent transfer, shredding).

DCOs may develop their own tracking and logging forms as long as they contain, at a minimum, the information outlined in **Section 4.2.2** above.

Each DCO must maintain an inventory log, Form 7740-11 (see **APPENDIX V**), for



TSCA CBI transactions at his/her facility. The inventory log must contain the following information:

- DCN.
- Dates on which a document is logged out from, and returned to, the DCO.
- Identity of the individual logging out the document.
- If the document is to be destroyed, the entry in the disposition block of the log must include the date of destruction and the identity of the person who will destroy it.
- If the requesting employee plans to transfer the document outside the DCO's jurisdiction, the disposition block of the log must include the date and destination of the transfer.

## 4.3 STORING TSCA CBI

### 4.3.1 Secure Storage Areas (SSAs)

Secure Storage Areas (SSAs) are spaces that meet the security requirements identified below and are used as TSCA CBI work and storage areas. Division directors can request that SSAs be designated; the SSAs must be approved by the IMD Director. After approval, the IMD Director will request that TSS inspect the SSAs for adherence to the following **security requirements**:

- Pin-tumbler door lock **or equivalent**
- A monitored intrusion alarm, OR
- Either an electronic entry ID card system or a changeable push-button door lock.

#### **4.3.1.1**            *Entering An SSA With An Electronic Access Card (EAC)*

Electronic ID card holders are required to present their cards to the reader the first time they enter a specific SSA each day, even if entering with a group of card holders. Thereafter, they would not need to use their card (for example, when leaving and re-entering the SSA to use the restroom, go to lunch, etc.) if they should re-enter the SSA with another person who opens the door.

Employees are not permitted to loan their entry cards to other employees.

#### **4.3.1.2**            *Entering an SSA Without An Electronic Access Card*

Federal and contractor employees entering an SSA who do not have their entry cards are required to sign a Visitor's Log, Form 7740-13(see **APPENDIX X**), upon initial entry. Employees may obtain a temporary card from their DCO. If the card has been lost, the loss must be reported to the OPPT DCO who will provide paperwork for the re-issuance of a new card and the deactivation of the lost card.

#### **4.3.1.3**            *Entering An SSA With Suspended or Terminated Certification*

A federal employee whose certification has been suspended, yet who still has an official need for access to TSCA CBI, may continue to enter SSAs and view TSCA CBI but will be prohibited from logging out documents until certification has been renewed. A federal employee whose certification has been terminated may not enter an SSA, and must again pass initial certification, not recertification, in order to again enter an SSA and view TSCA CBI. [See 2.1.2.1]

#### **4.3.1.4**            *Grantees And Interns In SSAs*

At EPA Headquarters, certain persons, such as grantees (e.g., NOWCC employees) and some interns, may work within SSAs but are prohibited from having access to TSCA CBI. They must, nevertheless, complete the certification process.

Grantees and approved interns must be "supervised" or "monitored" within an SSA by following these guidelines:

A grantee or intern:

- Cannot deliver, locate, file, copy, type or otherwise handle or view TSCA CBI.
- Cannot be the first employee to arrive or the last employee to leave an SSA and must never be the only person in an SSA.
- Cannot have any conversations with company representatives about information that has been claimed, or may be claimed, TSCA CBI.

#### **4.3.1.5**            *Visitors In SSAs*

Visitors to SSAs who do not have TSCA CBI certification must sign the Visitor's Log the first time each day they enter and re-enter the SSA and must be escorted while they are within the area.

#### **4.3.1.6**            *Custodian, Maintenance and Delivery Persons in SSAs*

Custodial, maintenance, mail, and other delivery personnel who routinely and frequently enter an SSA, and who are known generally to EPA staff, may be supervised while conducting their regular business. Such persons who are not known to EPA staff, however, must be escorted.

#### **4.3.1.7**            *DCOs And SSAs*

In general, DCOs are responsible for monitoring activities within SSAs and ensuring adherence of requirements set forth in this manual. DCOs have the following responsibilities:

- Maintain Visitor's Log entries for one year
- Safeguard lock combinations and disclose combinations only to authorized individuals
- Ensure that lock combinations are changed annually, or whenever anyone possessing a combination terminates her/his access, or the combination is otherwise compromised. At EPA Headquarters, DCOs should request a combination change from the FMSD in the Office of Administration and Resources Management (OARM).

### **4.3.1.8**      *Using TSCA CBI outside an SSA*

Employees who are using TSCA CBI documents outside SSAs must retain possession of them, and never leave the documents anywhere that unauthorized persons may gain access to them. When a TSCA CBI document is not in use it must be locked up by the employee in an approved storage container.

## **4.3.2**      **Required Storage Containers**

The following are approved storage containers for TSCA CBI:

- Metal file cabinets with locking bars and three-way changeable combination locks
- GSA-approved Class 6 security containers (safes), or
- Other secure storage containers, as approved by the IMD Director in consultation with TSS, on a case-by-case basis.

A storage container may be used by more than one person to store TSCA CBI, provided each person is certified for access to TSCA CBI and has separately labeled his/her respective space within the container. The employee must affix a magnetic “Open”/“Close” sign to each container so that the status of the security container is visible at all times.

## **4.3.3**      **Storing TSCA CBI At Other Locations**

TSCA CBI may be stored at locations other than an SSA with certain restrictions:

- Contractor sites must be inspected and approved by TSS before TSCA CBI may be transferred to the site (see **Section 2.2.1**).
- If traveling with TSCA CBI, it must be kept in the employee’s possession, in a hotel safe, or with the host DCO. TSCA CBI may be stored at home, if TSS has approved the employee’s plan for using TSCA CBI at his/her personal residence.

### **4.3.3.1**                    *Storing TSCA CBI While Traveling*

It is sometimes necessary for a federal or contractor employee authorized for TSCA CBI access to carry TSCA CBI while traveling on official business. If it is impractical to return to work to pick up the materials before departure or to drop them off after returning, the employee may obtain permission from his/her supervisor to take the materials home for a defined, limited period and protect them in a reasonable manner under the circumstances. This permission is related only to the storage of CBI at home when traveling - not for permission to use CBI at home under such circumstances as flexiplace, etc.

While traveling by plane or other public conveyance, employees must keep TSCA CBI in their possession and may not check it with their luggage. The following security measures apply:

- Car trunk storage. If the employee is traveling by car, he/she should store TSCA CBI locked in the trunk while en route. **TSCA CBI must never be left in a car overnight.**
- Hotel safe storage. TSCA CBI may be stored overnight in hotel safes, if a receipt is obtained from the hotel management. If no receipt is available, the employee must keep the TSCA CBI in his/her possession.
- Host DCO storage. Even if the traveler does not intend to transfer possession of the TSCA CBI, he/she may temporarily store the materials with the DCO at the location he/she is visiting.

### **4.3.3.2**                    *Storing and Working with TSCA CBI in a Personal Residence*

Normally, employees are not permitted to take TSCA CBI to their homes. Under special circumstances, such as recuperation from a long-term illness or under an approved flexiplace work arrangement, the IMD Director may grant permission for an EPA employee to use TSCA CBI at home.

Exceptional Circumstances: Home use of TSCA CBI is an exception and should be permitted only on a case-by-case basis when circumstances warrant, and when doing so serves the best interests of the Agency and promotes its mission. These criteria are developed as interim requirements to be adhered to in those exceptional situations when TSCA CBI may be brought to, worked on and kept at the private residence of an EPA employee.

IMD Director Approval: In every case where home use is requested, the IMD Director or designee must first review the circumstances and the employee's plan for home use of TSCA CBI before approving the arrangement.

Adherence to all Requirements: The procedures and requirements listed in this TSCA CBI Protection Manual must be followed prior to the transfer of any TSCA CBI to an employee's residence.

These procedures and requirements include:

- a. Review and approval of a plan for keeping and protecting TSCA CBI;
- b. Provision of an approved TSCA CBI container (see below); and
- c. Completion of a satisfactory site inspection by the TSCA Security Staff (TSS).

Use Of TSCA CBI at Home Only When Necessary: An employee being granted permission to use and maintain TSCA CBI at home may only do so when it is absolutely necessary for the satisfactory performance of his/her job. Stay at home or flexiplace employees granted this permission are strongly encouraged to the greatest extent feasible to make maximum use of sanitized, or non-TSCA CBI, documents. In addition, employees should refrain from unnecessary long term home storage of large volumes of TSCA CBI documents; and instead should work with smaller manageable amounts of TSCA CBI on a revolving basis where possible.

TSCA CBI Protection Manual: Any employee with permission to use and maintain TSCA CBI at home must continue to adhere to all applicable portions of the TSCA CBI Protection Manual.

Questions Regarding Home Use: Any question relating to home use and maintenance of TSCA CBI should be addressed to the OPPT DCO.

## **MANDATORY CRITERIA FOR HOME USE:**

The following are criteria for assessing the adequacy of any plan for home use of TSCA CBI. In addition, the TSS site inspection will use these criteria in evaluating the adequacy of the employee's home for the use and maintenance of TSCA CBI.

1. Employees who are using TSCA CBI in a personal residence must never leave the documents where unauthorized persons might gain access to or view TSCA CBI. When a TSCA CBI document in a personal residence is not in use, the employee must place the document in an **approved storage container**.

- a. The following **storage containers** are approved for TSCA CBI storage:
    - Metal file cabinets with locking bars and three-way changeable combination locks
    - GSA-approved Class 6 security containers (safes), or
    - Other secure storage containers, as approved by the IMD Director in consultation with TSS, on a case by case basis.
  - b. Home use employees must affix a magnetic open/close sign to each container so the status of the security container is visible at all times.

If the container has multiple drawers with separate combinations, each drawer must have an open/close sign affixed to it to show the individual condition of each drawer.
  - c. For each type of approved container which may be used at an employee's residence the combination or a spare key must be kept by each of the employees's Document Control Officers (DCOs).
  - d. The approved container used for storing TSCA CBI must be kept in a room in the house or apartment which has a locking door and locking windows.
2. TSCA CBI may never be processed, created, or stored on computers connected to – or capable of being connected to – the Internet, nor to any LAN not cleared for CBI, nor on portable computers of any kind except as approved by the IMD Director.
  3. If persons not authorized for access to TSCA CBI must enter the approved room in an employee's house for any reason while TSCA CBI is out while being worked on, they must be accompanied at all times by the TSCA CBI approved employee.

#### **OPTIONAL CRITERIA:**

1. Maintaining an alarm system in the house and/or designated TSCA CBI workroom.
2. Keeping the approved container in a locked closet within the locked room designated for use and storage of TSCA CBI.
3. All work on TSCA CBI performed in a room in the house or apartment which has a locked door and locking windows.

### 4.3.4 Employee Absence and Storage of TSCA CBI

If an employee who works in a Secure Storage Area will be out of the workplace for more than one week (seven calendar days), all TSCA CBI materials in his/her possession must be locked away in an approved TSCA CBI storage container. If the employee is unable to do this due to illness or other reason, the employee's supervisor or DCO will ensure the materials are stored according to procedure. Division Directors may waive this requirement in exceptional circumstances where not practical.

## 4.4 TSCA CBI DOCUMENTS

Federal employees using TSCA CBI documents and other materials frequently produce new TSCA CBI from these sources (in the form of such documents as notes, outlines, and drafts) or from documents printed from the TSCA CBI LAN. These works-in-progress are internal documents that exist in paper or electronic form.

### 4.4.1 New CBI Documents

Except as provided in **Section 4.4.2** below, newly created hardcopy CBI must be logged and tracked by the originator, by following these steps:

- Stamp the document as "TSCA CBI". (See **APPENDIX T**)
- Cover the document with a TSCA CBI **Green** Cover Sheet, and include the originator's name, phone number, and the date. (See **APPENDIX U**)
- Submit the document to the DCO for tracking.

### 4.4.2 Working Papers

New TSCA CBI documents which are "working papers" are exempt from logging procedures as long as they remain in the possession and/or control of the originator, or in the possession of a TSCA CBI-certified federal or contractor employee who works in an SSA or has an approved storage container for storing the TSCA CBI when not in use.

Federal and contractor employees may make multiple copies of a working paper (the copies themselves then being "working papers") to distribute simultaneously to the members of a review group, who will then comment and return the copies to the issuer. Staff must track any transfers of these multiple copies of working papers using their own personal tracking system.



Working papers or other such works-in-progress must be protected from unauthorized disclosure and handled like any other TSCA CBI document. Though working papers generated by federal employees and contractors are exempt from logging, an employee who generates them is responsible and accountable for safeguarding those copies, and is subject to the administrative and civil penalties described in **CHAPTER 5**. A green cover sheet must be applied to every working paper if the working paper is one sheet or multiple sheets that are clipped or stapled. (Green cover sheets may be obtained from the DCO or photocopied or printed on blank green paper.)

#### **4.4.2.1**                      *When Working Papers Become Subject to Tracking*

When a working paper becomes a final document (i.e. work on the document has been completed or stopped) it must be taken to the DCO. The DCO must log it into the DTS and assign it a DCN. At Headquarters, this final document must be taken to the CBIC for incorporation into the official record.

When a working paper is sent to another facility, it must be tracked, assigned a DCN, and transferred in accordance with the procedures for transferring TSCA CBI.

#### **4.4.2.2**                      *Destroying Working Papers*

The originator of a working paper or the individual who prints the document from the CBI LAN may destroy that working paper and any copies made, preferably by shredding. (See also **Section 4.9** on *DESTRUCTION OF TSCA CBI*).

### **4.4.3 When TSCA CBI Documents Are No Longer TSCA CBI**

TSCA CBI documents are no longer TSCA CBI under any of the following circumstances:

- TSCA CBI is not included in a new document
- TSCA CBI is deleted (sanitized) from an existing document
- The TSCA CBI that is used is masked or aggregated
- The data are derived from TSCA CBI data but are not themselves TSCA CBI
- The TSCA CBI claim is dropped by the submitter
- EPA formally determines that the claim is not valid in accordance with procedures in 40 CFR part 2 subpart B.

#### 4.4.4 Aggregating TSCA CBI

IMD must be consulted in advance by any program office or enforcement staff who wish to produce a non-confidential document by aggregating CBI in a new manner. IMD must review and approve all new applications of aggregating techniques to ensure that appropriate TSCA CBI protection has been maintained.

#### 4.4.5 Declassifying CBI Documents

Employees may determine that materials are no longer confidential, but the declassification may only be performed by a DCO. To declassify a TSCA CBI document:

- The employee must take the document to a DCO. If the document has been assigned a DCN by CBITS, it must be taken to the OPPT DCO. Documents tracked using other systems may be taken to the Facility DCO for declassification.
- Evidence must be presented to the DCO proving that the material no longer contains any CBI. (See **Section 4.1**)
- The DCO must cross out all CBI markings on the document and remove the cover sheet.
- The DCO must inscribe both the document and cover sheet with the statement "Contains no TSCA CBI," and sign and date both the document and cover sheet.
- The OPPT DCO must change the document's status in the tracking system.

***NOTE: A DOCUMENT MAY ONLY BE DECLASSIFIED IF ALL TSCA CBI CLAIMS ASSOCIATED WITH THE RECORD ARE EITHER WITHDRAWN BY THE SUBMITTER OR FINALLY DETERMINED BY THE OFFICE OF GENERAL COUNSEL TO NOT CONSTITUTE TSCA CBI.***

## 4.4.6 TSCA CBI Document Submitters: Dropping a Claim

A submitter can drop one or more claims of confidentiality for a document. To do so, **an authorized representative of the submitter** must send a letter on company letterhead to the OPPT DCO to drop the CBI claim. There may be other means of securing clear notice of a submitter's withdrawal of a CBI claim as well. For further information contact the branch chief of the TSCA Records and Dockets Management Branch, IMD. The steps outlined above for declassification must then be followed.

## 4.5 REPRODUCING TSCA CBI

This section applies to all TSCA CBI except working papers.

Reproducing TSCA CBI should be limited to as few copies as possible. TSCA CBI **must** be reproduced only at copying machines located in SSAs unless otherwise approved by the OPPT DCO. With the exception of working papers, only DCOs and ADCOs are permitted to photocopy TSCA CBI documents or print multiple copies from the CBI LAN.

### 4.5.1 Managing TSCA CBI Copies

The following rules apply to management of TSCA CBI copies:

- The cover sheet on the original document must not be copied. A new cover sheet must be used for each document copy.
- Copies must be logged into the DTS and must be assigned unique DCNs/copy numbers by the DCO.
- The originator may loan the copies to other employees and obtain signed transfer receipts indicating that the transfers were completed. These transfer receipts must be retained until the documents are returned. If a document is transferred and no transfer receipt is obtained, the originator of the document will be held accountable for the document.

## 4.5.2 Copying CBI Outside SSAs

Copying machines outside SSAs may be used if all other machines in locations approved for copying CBI are inoperable or unavailable, and as long as alternate machines or their use are approved by the OPPT DCO. A non-secured machine must be dedicated to the task and located in a manner that makes copying activity secure from observation to the extent practicable. After copying is finished, at least three blank copies must be passed through the machine to ensure that any impressions on the image surfaces of the machine have been erased.

In case of equipment failure, the operator must ensure that all CBI is removed from the photocopying equipment before leaving the area.

## 4.6 TRANSFERRING, TRANSFER RECORD-KEEPING, AND TRANSMITTING TSCA CBI

### 4.6.1 Transferring Hard Copy TSCA CBI

Except for working papers (**Section 4.4.2**), TSCA CBI can only be transferred from one employee to another through their respective DCOs (as long as the receiving employee has been approved for TSCA CBI access). Transfers of TSCA CBI must be conducted through DCOs in accordance with the procedures set forth in this manual. [See **3.3.3** and **3.3.4**]

[In addition, see **Section 4.1.4** on processing newly received TSCA CBI]

#### 4.6.1.1 *Procedures For Sending Or Receiving TSCA CBI*

An employee who requires TSCA CBI material to be mailed to a federal employee, a contractor cleared for CBI access, or to a TSCA submitter must provide the material to his/her DCO. **All TSCA CBI which is being sent by OPPT to locations outside the building must be mailed or shipped by the OPPT DCO, who has the option to delegate mailouts to the CCD and EETD DCOs.**

### **4.6.1.2**            *Preparing CBI For Mailing*

The DCO must double wrap TSCA CBI. The DCO must label the inner wrapping with the recipient DCO's name and the statement, "TSCA Confidential Business Information -- To Be Opened by Addressee Only."

The DCO must label the outer wrapper with the name and address of the recipient and a return address. The outer wrapper must be free of any indications that the package contains TSCA CBI. (The materials may be prepared for mailing by the originator, but the package must be left open for the DCOs review.)

### **4.6.1.3**            *Transferring TSCA CBI to Another Facility*

Before any TSCA CBI may be transferred to another facility, the sending DCO should notify the receiving DCO by email and by telephone that the materials will be sent. (See also Section 4.6.2 below relating to CBI Transfer Record-keeping, and Section 4.1.4 on processing newly received TSCA CBI.)

TSCA CBI may be transferred to an individual at another federal or contractor facility in one of the following ways:

- DCO can send the materials certified mail through the U.S. Postal Service – “return receipt requested”, or by Federal Express or other commercial and approved overnight delivery services which maintain routine tracking and receipt signature services. The DCO may also use a private messenger or courier service provided they are pre-approved by the IMD Director. Regular first class mail must never be used to transfer TSCA CBI.
  - DCO can appoint a cleared employee to deliver the materials directly to another DCO.
  - DCO can transfer the materials via fax. (See Section 4.6.3.2)
- 1) When sending TSCA CBI to another facility, the DCO must include a receipt identifying the contents of the package inside the inner envelope. (See APPENDIX Y, Form 7740-26 “*Permanent Transfer Receipt for TSCA CBI.*”) When used properly, the transfer receipt will not contain TSCA CBI information; therefore, the DCO has the option of either placing the form on the outside of the inner envelope or in it. (This form can also be used as a temporary transfer receipt for multiple documents; line out the word “permanent” and write “temporary” in its place.) The receiving DCO must sign the receipt of contents and return it to the sender within 5 business days. This form is not used when sending CBI to a TSCA submitter (see Section 4.6.1.4).

#### **4.6.1.4**                      **Transferring TSCA CBI to Industry**

There may be occasions when a submitter will request a copy of its submission to the Agency that contains TSCA CBI. Such a request must be in writing. However, in order to receive a copy, the company must provide a letter on corporate stationery which is signed by a designated corporate official indicating the person is authorized to receive the copy (unless a designated representative is already on file). This letter should be submitted to the OPPT DCO or in the case of a Region to the Regional DCO.

The TSCA CBI must be double-wrapped as described above and sent certified mail via the U.S. Postal Service, (indicating the person to receive the information) return receipt required. Couriers and private mail delivery systems may also be used. The tracking numbers used by these private mail delivery system must be recorded in the appropriate log.

The Agency may also initiate correspondence with industry which includes TSCA CBI. In this case the same procedures are followed except for the requirement of a notarized letter.

### **4.6.2 Hard Copy TSCA CBI Transfer Record-Keeping**

All permanent transfers must be made through a DCO. The following rules also apply:

#### **4.6.2.1**                      **Record-Keeping For Permanent Transfer**

- *Keep records on transfer.* If the transfer was made through a DCO, the DCO will record the transfer in the Document Tracking System (DTS)
- *Document Transfers.* Transfers between DCOs can be documented on a TSCA CBI Transfer Receipt, Form 7740-26 (see APPENDIX Y). Both the sending and receiving DCO should retain receipts for audit purposes. Contractor DCOs should maintain transfer receipts until the contract ends and all TSCA CBI is accounted for.
- *Obtain a receipt for returned documents.* When returning TSCA CBI documents, an employee should prepare a receipt for the DCO to sign and return to the employee or the employee's designee.

#### 4.6.2.2 *Record-Keeping For Temporary Transfers Within A Facility*

The following standards apply:

- Transferring Custody - Custody of CBI may be transferred from one employee approved for TSCA CBI access to another within the same facility.
- Recording the Transaction - There must be a record indicating that the transfer was completed.
- Obtaining Record Of Transfer - Transferors may use the Temporary Loan Receipt for TSCA CBI, Form 7740-14 (see APPENDIX AA), or any other form that records the transfer.
- Using Receipt Form - Hand delivery with a TSCA CBI Receipt form may be used only for short-term TSCA CBI transfers.
- Delivering By Hand - If hand delivery is used, the TSCA CBI must be given directly to the recipient or a TSCA CBI cleared employee.
- Monitoring Overdue TSCA CBI - TSCA CBI may not be logged out from a centralized TSCA CBI storage facility for more than one year. DCOs must monitor the DTS for TSCA CBI that have not been returned within one-year. The DCO is responsible for notifying employees and their supervisor of overdue materials.

*If a transfer is made by hand delivery to another person within the same facility, the owner or originator of the transferred document may choose to obtain a signed loan receipt indicating that the document has been loaned. If a document is transferred and no loan receipt is obtained, the owner or originator of the document will be held responsible for any loss or unauthorized disclosure of the document.*

## 4.6.3 Transmitting TSCA CBI Electronically

### 4.6.3.1 *Transmitting TSCA CBI By Telephone*

CBI may be transmitted orally during telephone conversations.

**NOTE: VOICEMAIL IS NOT SECURE. TSCA CBI MUST NEVER BE LEFT IN A PERSON'S VOICEMAIL.** [However, Case Numbers and PMN numbers may be left on a submitter's voicemail if they have not first raised an objection to EPA following receipt of an acknowledgment letter informing them of this practice and their right to object.]

Authorized employees are allowed to discuss TSCA CBI on the telephone with other authorized federal or contractor employees with TSCA CBI access. Both parties to a telephone call are responsible for verifying that the other is authorized for TSCA CBI access. To do so, the employees should consult the TSCA CBI Approved Access List upon **initial** contact.

The individual who initiates a discussion that includes TSCA CBI must indicate that the conversation involves TSCA CBI.

Authorized employees are allowed to discuss TSCA CBI on the telephone with an authorized representative of the submitter when all of the following conditions are met:

- The employee must verify that the person to whom he/she is speaking has been previously identified by the company as an authorized contact to discuss TSCA CBI. The authorized individual is normally the technical contact for the subject submission. (In cases where the technical contact or other authorized representative cannot be obtained from the document submitted to the Agency, the employee should consult the OPPT DCO.)
- The employee must verify that all federal and contractor employees on the line are cleared for TSCA CBI access and relay that information to the submitter.
- The employee must inform the submitter that any further information provided in the telephone conversation can be claimed as confidential.

Authorized contractors may also discuss TSCA CBI on the telephone with submitters. The contractor must begin the conversation by identifying that they are an EPA contractor. The same procedures identified above for employees must be followed. EPA



recommends that employees keep telephone logs of all calls with individuals located outside their organization during which TSCA CBI is discussed.

A telephone log should contain the following:

- Date and time of the call.
- Employee name and office.
- Name, number, and organization of the other party.
- Who initiated the call.
- Content of the conversation.

Telephone logs of conversations with TSCA CBI submitters should be kept when the call results in changing the status of information in an industry submission: for example, when information is requested from the submitter, when clarifications are provided to the submitter of a substantive nature, etc. Telephone logs must be provided to the DCO for incorporation into the DTS and to the CBIC if relevant to a TSCA submission, Form 7740-12 (See **APPENDIX Z**.)

#### **4.6.3.2**                      *Transmitting TSCA CBI by Fax*

EPA and contractor DCOs may transfer and receive TSCA CBI materials via facsimile. Faxing of TSCA CBI should be limited to situations where timely delivery would be compromised by using other means (e.g., mail delivery, courier service).

The following security provisions must be followed when transmitting any TSCA CBI by fax:

- Verify receiver. Before sending a fax containing TSCA CBI to an authorized government or contractor recipient, the sender must verify that the recipient has been certified for access to TSCA CBI by consulting the TSCA CBI Authorized Access List. In addition, prior to sending a fax containing TSCA CBI to a submitter of the information, the sender must verify that the recipient has been identified as the company's authorized representative on the original submission to EPA. Alternatively, the Agency must be in possession of a letter on corporate stationery signed by a designated company official authorizing the transmission to this recipient. Similarly, when a submitter requests that EPA fax its TSCA CBI to a third party (e.g., lab director or attorney), the Agency must be in possession of a letter on corporate stationery signed by a designated company official authorizing the transmission to the specified third party.

- Control the fax equipment. During transmission of TSCA CBI by employees and Agency contractors, the DCOs sending and receiving the document must completely control the fax machines. They must ensure that anyone not cleared for TSCA CBI does not view the document being sent.
- Select the fax machine. Fax machines located inside SSAs are recommended. Fax machines used outside SSAs may be used, but only with the utmost care.
- Verify the phone number. The employee sending the fax is responsible for ensuring that the number dialed is correct by verifying the number on the fax transmission confirmation receipt. Use extreme caution when dialing the number to ensure that the correct number is entered. (If TSCA CBI is accidentally transferred to a wrong number, TSS must be immediately notified.)
- Retain the receipt. The DCO must attach the fax transmission confirmation receipt to the document that was faxed and place the document in the official document file if applicable.

Authorization from the submitter to fax documents to third parties (e.g., lab directors) must be obtained in writing and maintained in the DCO's files.

#### **4.6.3.3**            *Transmitting TSCA CBI By E-mail*

TSCA CBI cannot be transmitted via e-mail except on approved Local Area Networks (LANs). (See **Section 4.8** on using computers to work with TSCA CBI.) In the event TSCA CBI is released on any other LAN or the internet, you must immediately report this to your Office Information Security Officer (ISO) and immediate supervisor. For further information, contact your ISO.

#### **4.6.3.4**            *Transmitting TSCA CBI By Tele-Video Conference*

TSCA CBI may be displayed and discussed during tele-video conferences conducted between EPA Headquarters and EPA regional offices. Employees who arrange or schedule a tele-video conference are responsible for ensuring that all TSCA CBI security procedures are followed. These procedures include the following:

- Verify that everyone who attends the tele-video conference is cleared for TSCA CBI.

- Ensure that both conference rooms are secured to prevent unauthorized persons from entering the conference rooms during the tele-video conference.
- Arrange for use of compressed video encryption during transmission, if available. For information about tele-video encryption, contact the EPA Security Officer in Research Triangle Park, at (919) 541-4013.

## 4.7 USING AND HANDLING TSCA CBI

Use TSCA CBI according to the following guidelines:

### 1) Employee Responsibilities

Employees using TSCA CBI are responsible for ensuring that no unauthorized disclosure of that information occurs. If employees take TSCA CBI outside the SSAs, they must do one or more of the following:

- Maintain constant control over the TSCA CBI documents in their possession
- Return the TSCA CBI documents to the DCO.
- Store the documents in a TSCA CBI-approved storage container.

### 2) Obtaining TSCA CBI

Except as provided in **Section 4.4.2** (*Working papers*) and in **Section 4.6.2.2** (*Record-Keeping For Temporary Transfers Within a Facility*), to obtain TSCA CBI documents follow the steps below:

- The employee requests a specific TSCA CBI document from his or her DCO.
- The DCO verifies that the employee is approved for access to the document.
- The DCO logs the document out to the employee.

### 3) Using or discussing TSCA CBI in meetings

To discuss TSCA CBI at meetings (scheduled gatherings), follow the steps below:

- a. *An employee may circulate **personal working papers** or other materials logged out to that employee at a meeting if the following conditions are met:*

- The employee to whom the document belongs attends the meeting and is present when the document is discussed.
  - The owner employee collects all copies of the document at the end of the meeting.
  - The owner employee numbers the copies ("1 of 6", "2 of 6", and so forth) before distributing them and checks to make sure that all copies are returned at the end of the meeting.
  - The owner employee destroys all copies of the document after the meeting.
- b. *To discuss TSCA CBI during meetings, a chairperson must be identified beforehand.*
1. The chairperson is responsible for ensuring that only people approved for TSCA CBI access are in the room during discussion involving TSCA CBI. The chairperson must also secure the room at the end of the meeting (by cleaning all chalkboards, removing all TSCA CBI, etc.).
- c. *The chairperson must remind meeting attendees that they must treat as confidential any notes taken at the meeting.*
- Notes taken at the meeting that contain TSCA CBI are considered to be personal working papers. To tape record a meeting, permission from the chairperson must be obtained. Such recordings may contain TSCA CBI and must be treated as TSCA CBI.

#### **4) Developing TSCA CBI photographic materials**

When photographs are claimed as TSCA CBI material, the Facility DCO must ship the film to the Regional or OPPT DCO (as appropriate) for processing and development. Processing or development by a private or commercial laboratory is prohibited **unless expressly approved by the IMD Director in consultation with TSS.**

#### **5) Claiming a videotape as TSCA CBI**

If an EPA employee utilizes video equipment during an inspection or plant visit, and the company wishes to claim the tape as TSCA CBI, the tape must be handled and controlled like any other TSCA CBI material.

## **4.8 USING COMPUTERS TO WORK WITH TSCA CBI**

### **4.8.1 Prohibition**

*TSCA CBI may not be processed, created, or stored on computers connected to the Internet or to any LAN not approved for TSCA CBI, nor on portable computers of any kind, except as approved by IMD after consultation with the TSCA Security Staff (TSS). In the event TSCA CBI is released on any other LAN or the Internet, you must immediately report this to your Office Information Security Officer (ISO) and immediate supervisor. For further information, contact your ISO.*

### **4.8.2 TSCA CBI Computers Must Be Separate From Public Networks**

TSCA CBI may be created, processed, and stored ONLY:

- on computers which are permanently connected to a self-contained Local Area Network (LAN) approved for TSCA CBI and not connected to the Internet

*OR,*

- on computers which are permanently disconnected from any network, Internet access, or other technology which can pass data to another computer.

### **4.8.3 Registration is Required to Use CBI Computer Systems**

Employees who require access to TSCA CBI computer systems must complete the “TSCA CBI ADP User Registration Form” and submit it to the OPPT DCO. IMD will provide the employee with a user ID and password to access the TSCA CBI network. (See **APPENDIX B**, EPA Form Number 7740-25).

#### **4.8.4 Using Portable Computers (*Laptops and Handheld Devices*)**

*Laptop computers* may not be used to process TSCA CBI data unless they are approved by IMD in consultation with TSS. To obtain approval, the DCO must prepare a security plan. TSCA CBI use of laptops will be approved on a case-by-case basis by IMD to ensure that proper procedures will be followed regarding their use. (See **APPENDIX BB** for an example of the Laptop Computer User Agreement for the CBIC form.)

*Handheld devices* (such as Personal Digital Assistants) may not be used to process, create, or store TSCA CBI.

Once a portable computer has been approved for TSCA CBI use,

- It must be conspicuously labeled as a TSCA CBI computer with distinctive markings that are not visible when the computer is not in use. This can include operating system and application software backgrounds, login screens, and other reminders that the user is using a TSCA CBI-cleared computer.
- Any modem, network card, wireless port, or other computer-to-computer communications device must be removed.
- The user is responsible for preventing the data from being disclosed to any unauthorized person while traveling outside the Secure Storage Area in which the portable computer is normally stored while not in use.

#### **4.8.5 Disposing of Computers Formerly Used for TSCA CBI**

If a computer which has been used to store or process TSCA CBI data is to be connected to the administrative LAN and/or the Internet, or is to be discarded, its hard drive must be destroyed or thoroughly erased by appropriate software. IMD must certify a computer as having been cleaned of TSCA CBI immediately after the computer has been disconnected from the TSCA CBI LAN or after its retirement from use as a TSCA CBI standalone computer.

## **4.8.6 Modems**

OPPT prohibits both internal and external modems on all computers used for TSCA CBI. Any exception to this general prohibition must be approved by IMD.

## **4.8.7 TSCA CBI Data Processed Only Within SSAs**

TSCA CBI may be processed only on computers located within TSCA CBI approved Secure Storage Areas, unless other arrangements are approved by TSS in consultation with the OPPT ISO.

## **4.8.8 Printing TSCA CBI Information**

Authorized employees are permitted to print out one copy of their working papers from the TSCA CBI LAN for individual use. Multiple copies may be made only by the DCO/DCA.

*[See Section 4.4.2 of this Manual for special requirements concerning personal working papers].*

All printouts from the TSCA CBI LAN are assumed to contain TSCA CBI unless the user indicates otherwise in writing on the first page of the printout, with signature and date.

Printouts from the TSCA CBI LAN must be treated like any other TSCA CBI document and protected accordingly.

The employee should promptly remove copies from the printer to reduce the likelihood that the TSCA CBI information will be viewed by visitors. Once a session ends, the computer must be re-booted or turned off.

## **4.8.9 Storing TSCA CBI on Magnetic Media**

The procedures for storing TSCA CBI hard-copy materials apply equally to magnetic media (diskettes, hard disks, magnetic tapes and data cartridges), optical disks, memory cards, and to any other storage devices.

## **4.8.10 Disposing of TSCA CBI Computer Disks**

When disks are no longer needed or are damaged, they should be destroyed in a manner approved by IMD, in consultation with TSS, or sent to IMD for destruction. At EPA headquarters they may be given to IMD for destruction.

### **4.8.11 Security for TSCA CBI Data Stored on Contractor's Off-site Computers**

A contractor's site must be inspected and approved before any TSCA CBI may be transferred, processed, or stored there (See **Section 2.2.2**). EPA contractors may not place TSCA CBI on any computer system without written authorization from EPA.

Authorized EPA contractors who use TSCA CBI must follow all computer security requirements established for EPA Contractors. Contractors are permitted to use standalone PCs and laptops for processing TSCA CBI by adhering to the procedures contained in this manual.

## **4.9 DESTRUCTION OF TSCA CBI**

Only DCOs are permitted to destroy TSCA CBI (except working papers, as discussed in **Section 4.4.2.2**). Federal employees wishing to have TSCA CBI destroyed must take these materials to their DCO. Contractor DCOs must obtain written permission from the OPPT DCO before destroying TSCA CBI. CBITS-tracked documents may only be destroyed with the approval of the OPPT DCO; however permanently logged-out documents may be destroyed by a DCO.

Contractor DCOs may not destroy CBITS-tracked documents. These documents must be returned to the Project Officer at the end of the contract. The PO must ensure the return of the documents to the CBIC for proper destruction.

### **4.9.1 Procedures for Destroying TSCA CBI**

The procedures for destroying TSCA CBI apply to all media containing TSCA CBI except working papers. (See **Section 4.4.2** on working papers.)

**[NOTE: This section, as written, does not apply in the special case of the CBIC because of its unique function.]**



## 4.9.2 Destruction Methods

TSCA CBI such as papers, documents, or printouts must be shredded. Materials such as microfiche, typewriter ribbons, and magnetic media must be burned, degaussed, or chemically destroyed.

## 4.9.3 Destruction Record-Keeping

The destruction of a TSCA CBI document that has been entered into the DTS must be recorded. The DCO must enter information about the destruction of the document into both the Receipt Log, Form 7740-10 (see **APPENDIX W**), and the Inventory Log, Form 7740-11 (see **APPENDIX V**).

## 4.9.4 Disposition of CBI Cover Sheets

CBI cover sheets (see **APPENDIX U**) must be completed by the DCO with destruction date, location where the document was destroyed, and DCO's name.

The TSCA CBI cover sheets must then be placed in the appropriate file for storage (e.g., at EPA Headquarters, a cover sheet would be placed in the CBIC file for that document).

Green cover sheets must be maintained **for at least one complete audit cycle** (see **Section 3.3.12.1(a)**).

## 4.9.5 Contracts Involving TSCA CBI

The PO and DCO for the contract are responsible for ensuring that all TSCA CBI is properly disposed of and accounted for at contract close-out. All logs and records used to track and dispose of TSCA CBI must be submitted as part of the contract close-out. Any unaccounted-for documents must be reported as required in **CHAPTER 5**.

This page intentionally left blank

# CHAPTER 5

## Procedures Violations, Unaccounted For Documents, And Unauthorized Disclosures

### 5.0 INTRODUCTION

This Chapter details the reporting and investigative actions to be followed by TSCA CBI authorized persons in the event of any possible violation of the requirements outlined in this manual. Examples of such violations include cases of unaccounted for TSCA CBI documents, as well as any disclosure of TSCA CBI to a person not authorized to receive it under Section 14 of TSCA.

The protection procedures detailed in this Manual are enforceable by both the administrative penalties and corrective actions set forth below. On policy issues, the IMD Director should be consulted.

### 5.1 EMPLOYEE REPORTING PROCEDURES

#### 5.1.1 Oral Report

Any TSCA CBI-cleared employee of EPA or another Federal agency must provide oral notice to his or her immediate supervisor within one working day if he or she thinks it is possible that

- A TSCA CBI protection procedure has been violated.
- TSCA CBI is unaccounted for.
- TSCA CBI may have been disclosed to a person not authorized to receive it under Section 14 of TSCA.

Contractor employees on the TSCA CBI Authorized Access List must provide oral notice to their EPA Project Officer or PO designee within 1 business day if any of the above situations occur. The EPA PO or PO designee must then report to the Division Director (or equivalent manager in their organization).

## 5.1.2 Written Report

Federal and contractor employees must file a written report within 2 business days in any of the same situations identified in **Section 5.1.1** above (unless otherwise relieved of the requirement by their management representative who is authorized to receive the report). EPA and other federal employees must provide this written report to their Division Director (or equivalent manager in their organization). Contractor employees must provide the written report to their PO or PO designee.

The written report must include any relevant circumstances or facts known by the employee, and describe any of the following:

- Possible violation of procedures.
- Possible unauthorized disclosure of TSCA CBI.
- Materials possibly unaccounted for.

To investigate what occurred, the employee and/or the employee's supervisor should examine files and discuss the matter with other individuals who may have first-hand knowledge of the facts.

The employee's division director (or equivalent) must review the employee's report and provide any additional comments or information. Within 2 business days of receiving the report, the Division Director must refer the report to TSS. If the Division Director reviews the employee's report and determines there was no violation of procedures, loss of TSCA CBI, or unauthorized disclosure, the report need not be referred.

## 5.2 REPORT OF VIOLATIONS TO TSS

This section applies in the case of a report referred to TSS by an employee's supervisor alleging a possible violation of the procedures contained in this manual, possible unaccounted for TSCA CBI documents, or possible disclosure of TSCA CBI to a person not authorized to receive it under Section 14 of TSCA.

### 5.2.1 TSS Investigation

Following review of the written report referred to TSS in the situations identified above, TSS will conduct an investigation if it determines one is necessary. If, after reviewing the written report, TSS determines that the facts do not warrant an investigation, TSS will notify the employee's Division Director in writing of this finding.

## **5.2.2 Oral Notice to Submitter**

If TSS conducts an investigation and determines the likelihood of either an improper disclosure of TSCA CBI under Section 14 of TSCA or the loss of a submitter's TSCA CBI, with the approval of the EAD Director TSS will notify the submitter by telephone within 2 working days.

## **5.2.3 Report of Investigation (ROI)**

Once the investigation is complete, TSS will provide the EAD Director with an ROI, which will contain the following:

- A recitation of the factual circumstances of the violation.
- Conclusions, including :
  - Probability that an improper violation occurred.
  - Nature and degree of any violation.
  - Recommendations for remedial action or mitigation, including a report forwarded to the affected employee and supervisor identifying procedures for handling, using, and storing TSCA CBI.

The length and detail of this report is determined by the nature, degree and circumstances of the alleged violation.

## **5.2.4 Company Notification of Improper Disclosure: EAD Director**

After receiving an ROI, the EAD Director will authorize issuance of a written notice to the affected company within 4 business days unless the EAD Director believes that the reported disclosure did not occur. If it is determined that an improper disclosure probably did occur, the written notice must identify the improperly disclosed document and the date upon which such disclosure was deemed to have occurred. The EAD Director will ensure that the submitter is contacted in writing and advised of the fact that it is unlikely that the reported disclosure occurred, and take no further action.

### **5.2.5 Company Notification of Documents Unaccounted for: EAD Director**

Following receipt of an ROI notifying the EAD Director of an unaccounted for CBI document, the EAD Director will issue a written notice to the affected company within 4 business days if the document is not accounted for in that time. The written notice must identify the lost or misplaced document and state the date on which it was deemed lost or misplaced. If the EAD Director believes that the document in question is not unaccounted for, she/he will ensure that the submitter is contacted in writing and advised of this fact and take no further action.

### **5.2.6 Referral to the Inspector General**

Upon consideration of the ROI, if there is any substantial evidence of a knowing or willful disclosure of TSCA CBI, the EAD Director will immediately refer the matter to the EPA Office of Inspector General.

### **5.2.7 Annual Security Report**

On a fiscal year basis, TSS will provide a report to be distributed to the OPPT Director, the EAD Director, the OPPT DCO, and others upon request, identifying the previous year's security violations by type and discussing trends, recognized vulnerabilities, and other matters that may be of interest.

## **5.3 CORRECTIVE ACTION AND PENALTY GUIDELINES**

The corrective actions and penalties described in the Chapter are intended to prevent or discourage violations of this manual, and thereby better protect TSCA CBI. Penalties imposed or actions taken must be fair, consistent, and well-reasoned.

### **5.3.1 Responsibility for Monitoring Compliance With Protection Manual**

The responsibility for monitoring compliance with the procedures in this manual belongs to the EAD Director. The Director will review the facts in a given case and, where appropriate, recommend specific action, including the imposition of corrective actions, administrative penalties or referral for criminal charges. Responsibility for implementing

the EAD Director's recommended action, or devising and implementing an alternative action, rests with the Division Director (or equivalent) of the EPA or federal employee involved.

Nothing in this section should be construed to limit the Agency's ability to end an individual's access to TSCA CBI any time it is viewed as necessary to protect confidential data entrusted to the Agency or TSCA CBI access is viewed as no longer necessary for the satisfactory performance of the person's assigned duties.

### **5.3.2 Violations by Federal Employees**

After a finding of a likely violation of the rules in this manual, the EAD Director will notify the EPA or federal employee's Division Director (or equivalent) and discuss the structure of any administrative penalties and corrective actions. The EAD Director may recommend that the employee's Division Director select and impose an appropriate penalty chosen from the ones identified in this section after weighing the totality of circumstances in each case (see **Figure 5-1**). In consultation with the EAD Director, the employee's Division Director must consider the following:

- Seriousness of the violation.
- Potential for unauthorized disclosure of TSCA CBI because of the violation.
- Nature of the employee's error (e.g., accidental, willful, or grossly negligent).
- If the employee has previously committed any other TSCA CBI violation.
- How often the employee uses or handles TSCA CBI while performing his/her official duties.

Corrective actions may be procedural, or instructional, and may include training, revision of work procedures, removal of the individual's name from the TSCA CBI Authorized Access List, and other options.

The employee's Division Director (or other appropriate authority in the employee's organization) should select, upon the EAD Director's recommendation, an administrative penalty when the employee was grossly negligent or previously incurred a prior violation, even if the violation were not serious. A table of suggested administrative penalties appears below.

**NOTE: The Terms “SUSPENSION” and “REMOVAL” in the table below relate only to TSCA CBI access, and not to federal employment.**

**Nothing in this Section prevents the employee’s supervisor from imposing other penalties in addition to those discussed in the table below.**

**Figure 5-1. ADMINISTRATIVE PENALTIES**

Nature of Offense	1st Offense	2nd Offense (in same calendar year as 1st offense)	3rd Offense (in same calendar year as 2nd offense)
<b>CBI is not compromised and breach is unintentional.</b>	Counseling by supervisor to oral reprimand.	Oral reprimand to written suspension.	1-day suspension to removal.
<b>CBI is compromised, but breach is unintentional.</b>	Oral or written reprimand to 5-day suspension.	1-day to 5-day suspension.	7-day suspension to removal.
<b>Deliberate procedure violation.</b>	<b>Reprimand to Removal.</b>	Removal.	

- These penalties cover only deliberate procedural violations that do not result in the unauthorized disclosure of TSCA CBI. If EAD's investigation reveals any evidence of the knowing and willful unauthorized disclosure of TSCA CBI, the matter will be immediately referred to the EPA Office of Inspector General. The suggested penalties in the above table do not replace or supersede the existing authority of the IMD Director to suspend the TSCA CBI access of any employee for the purpose of protecting TSCA CBI.

A federal employee who has been found to have willfully disclosed TSCA CBI to a person not authorized under Section 14 of TSCA may be liable under Section 14(d) of the Act, 15 U.S.C. 2613(d), for a fine of up to \$5,000 and/or imprisonment for up to one year.

The EAD Director has the option of recommending that no action, **or a different action,**



be taken if, for example,

- fault cannot be ascribed to any individual or
- a modification of TSCA CBI handling procedures would yield no greater level of protection to TSCA CBI.

### **5.3.3 Violations by Contractor Employees**

A contractor imposes corrective or disciplinary measures on its employees. Although the particular disciplinary action a contractor chooses to impose is a matter for the contractor to decide, a failure on the part of a contractor employee to follow the procedures in this manual may be considered a material breach of the contract if the contractor does not take adequate and appropriate disciplinary and corrective actions.

The IMD Director may suspend the TSCA CBI access of a contractor employee to protect against imminent threat to TSCA CBI security. The IMD Director maintains the right to suspend the TSCA CBI access of any contractor employee without consultation with the contractor or going through the contract administrative process if there is imminent cause for doing so which relates directly to the government's mandate of protecting TSCA CBI.

A contractor employee who is found to have willfully disclosed TSCA CBI to a person not authorized under Section 14 of TSCA may be liable under Section 14(d) of the Act, 15 U.S.C. 2613(d), for a fine of up to \$5,000 and/or imprisonment for up to one year.

## **5.4 OPPT DIRECTOR AS ARBITER**

Where disagreements arise between Headquarters divisions, or between Headquarters divisions and Regional offices, regarding objective assessments of violations, the OPPT Director will arbitrate all time-sensitive matters within 24 hours of referral. Other matters not facing legal time limits will be arbitrated within a reasonable time.



### Paperwork Reduction Act Notice

The public reporting burden for the collection of information is estimated to average .84 hours per response. This estimate includes time for reviewing instructions, gathering and maintaining the needed data, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information to the Director, Collection Strategies Division, US Environmental Protection Agency (2822T), 1200 Pennsylvania Ave., NW, Washington DC 20460, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503, marked ATTENTION: Desk Officer for EPA. Include the OMB No. identified on page 1 in any correspondence. Do not send the completed form to this address. Submit the form in accordance with the instructions in the CBI Manual.

### Privacy Act Statement

Furnishing your Social Security Number is voluntary, but encouraged. The information on this form is used by EPA to maintain a record of those persons cleared for access to TSCA Confidential Business Information (CBI) and to maintain the security of TSCA CBI.

Disclosure of information from this form may be made to the Office of Pollution Prevention and Toxics (OPPT) contractors in order to carry out functions for EPA compatible with the purpose for which this information is collected; to other Federal agencies when they possess TSCA CBI and need to verify clearance to EPA and EPA contractor employees for access; to the Department of Justice when related to litigation or anticipated litigation involving the records or the subject matter of the records; to the appropriate Federal, State or local agency charged with enforcing a statute or regulation, violation of which is indicated by a record in this system; where necessary, to a State, Federal or local agency maintaining information pertinent to hiring, retention, or clearance of an employee, letting of a contract, or issuance of a grant or other magistrate or administrative tribunal; in the course of litigation under TSCA; and to a member of Congress acting on behalf of an individual to whom records in this system pertain.

### Instructions for Form Completion

<p><b>Section I – To be completed by all</b></p> <ol style="list-style-type: none"> <li>1. List Full Name</li> <li>2. List 9-Digit ID (e.g., SSN)</li> <li>3. List Telephone number of person in item 1</li> <li>4. List Full Acronym of Requesting Office (i.e. EPA Office in which the individual works or for contractor employees, the EPA Office with whom the contract is with)</li> <li>5. List the immediate Document Control Officer for the office in which the individual works</li> <li>6. List the telephone number of the Document Control Officer</li> <li>7. Check the TSCA Sections for which access is requested or check ALL if applicable</li> <li>8. Circle the appropriate Access Justification Code                     <ul style="list-style-type: none"> <li><b>A.</b> Employee is an EPA employee or EPA contractor employee whose work assignments involve the New and/or Existing Chemical Programs of TSCA. Hence access to the TSCA sections listed in item 7 of this form is required in performance of his/her duties.</li> <li><b>B.</b> Employee is an EPA employee or EPA contractor employee whose work entails the administration of computer systems housing TSCA CBI. Hence access to the TSCA sections listed in item 7 of this form is required.</li> <li><b>C.</b> Employee is an EPA employee or EPA contractor employee whose work entails physical security or maintenance for TSCA CBI secure storage areas. Although employee will not actually work with any TSCA CBI materials, access to the TSCA sections listed in item 7 of this form is required.</li> <li><b>D.</b> List Justification here _____</li> </ul> </li> </ol>	<p><b>Section III – To be completed by HQ Federal and HQ Contractor employees only</b></p> <p>NOTE: These procedures apply only to employees requiring access to OPPT Secure Storage areas. All others follow standard Agency procedures.</p> <ol style="list-style-type: none"> <li>14. Check either box a, b, c or (c&amp;d) for EPA ID badge or Contractor Building Pass. If box c is checked, write in badge number.                     <ul style="list-style-type: none"> <li><b>a. Yes</b> - Check if new employee getting first EPA ID Badge. (New programmed badge and barcode)</li> <li><b>b. Need Replacement</b> - Check if replacement ID Badge is needed (replacement badge and barcode)</li> <li><b>c. No</b> - Existing badge needs programming. List ID Badge no.</li> </ul> </li> <li>15. Check and list OPPT secured areas for which access (via "RUSCO" electronic door control system) is required. List Division acronyms for the requested areas.                     <ul style="list-style-type: none"> <li><b>Home Division</b> - List Division in which employee works</li> <li><b>Other Divisions</b> - List other OPPT Divisions for which unrestricted daytime access is requested</li> <li><b>CBIC Only</b> - To be checked for those who only need to access the Confidential Business Information Center.</li> <li><b>IMD Areas</b> - Employees who need to regularly access the IMD Document Control Office Suite should circle <b>DC0</b> in the fourth block. Only IMD staff and contractors who work in IMD computer rooms should circle <b>IMD Computer Rooms</b>.</li> </ul> </li> <li>16. List OPPT areas by Division and Room numbers for which Alarm Activation/Deactivation authority is requested. Generally, this is employees home Division only.</li> </ol>
<p><b>Section II – To be completed by Contractor Employees only</b></p> <ol style="list-style-type: none"> <li>9. List Employer's name</li> <li>10a-d. List Employer's address</li> <li>11. List Contract number</li> <li>12. List EPA Project Officer's name</li> <li>13. List EPA Project Officer's telephone number</li> </ol>	<p><b>Section IV – To be completed by all</b></p> <ol style="list-style-type: none"> <li>17. Employee Signature (must be original)</li> <li>18. Signature Date</li> </ol> <p><b>Section V – To be completed by all</b></p> <ol style="list-style-type: none"> <li>19. Enter date employee attended TSCA CBI Security Briefing</li> <li>20. Immediate Supervisor/EPA Project Officers name and sign.</li> <li>21. Date of signature</li> </ol> <p><b>Section VI – To be completed by OPPT Security</b></p>

**PLEASE READ THE INSTRUCTIONS ON THE REVERSE SIDE BEFORE COMPLETING THIS FORM.**  
**(Please Print or Type - Do not mark in shaded areas)**



United States Environmental Protection Agency  
 Washington, D.C. 20460

# TSCA CBI ADP USER REGISTRATION

## Section I - Action - Check all appropriate boxes

- |   |   |
|---|---|
| <input type="checkbox"/> Assign new userid and password     | (Complete all items in Section II, except 2 and 15. Complete Section IV.)                   |
| <input type="checkbox"/> Add User to Systems                | (Complete all items in Section II, except 15. Complete Sections III and IV.)                |
| <input type="checkbox"/> Update User Information            | (Complete all applicable information in Section II, including item 2. Complete Section IV.) |
| <input type="checkbox"/> Delete User from Specific Accounts | (Complete items 1, 2, and 3 in Section II only. Complete Sections III and IV.)              |
| <input type="checkbox"/> Delete Users from All Systems      | (Complete items 1, 2, and 15 in Section II. Complete Section IV.)                           |

## Section II - Users Assigned to System (see instructions on reverse side)

1. User Name (Last, First, MI)		2. Userid	3. Company or Employer
4. Office/Division/Branch/Section (For EPA employees only)		5. Address (Street or P.O. Box)	
6. Telephone Number (include area code)		7. City	
8. EPA Region	9. EPA Mail Code	10. State	11. Zip Code
12. User Status - Check one: <input type="checkbox"/> EPA <input type="checkbox"/> EPA Contractor <input type="checkbox"/> Federal Non-EPA			
13. TSCA CBI Security Briefing Date (___/___/___) Circle TSCA clearance: Sections [ALL] -or- [3] [4] [5] [6] [8] [13] [20] [21]			
14. Check the type of work to be performed: <input type="checkbox"/> Database Administrator <input type="checkbox"/> Data Entry Staff <input type="checkbox"/> Technical Consultant <input type="checkbox"/> Developer <input type="checkbox"/> RTP Operations/Systems Staff <input type="checkbox"/> Retrieval Staff <input type="checkbox"/> Query (Read Data)			
15. Enter the access termination date of the user identified above: (Month: _____ Date: _____ Year: 19____)			

## Section III - TSCA Systems (see instructions on back - Do not mark in shaded areas)

16. Mainframe Hardware Code:	Account: TSO [Y] [N] Group: _____ Natural (Date: ___/___/___) by _____
16a. Mainframe System to Access (list one):	
17. Mainframe Hardware Code:	Account: TSO [Y] [N] Group: _____ Natural (Date: ___/___/___) by _____
17a. Mainframe System to Access (list one):	
18. LAN Hardware Code:	19. LAN Hardware Code:

## Section IV - Signature Authority (Required before Processing)

20. Requesting Official Name (Type or Print): _____	22. Request Date:
21. Signature of Requesting Official (Required)	23. Phone Number:
24. Document Control Officer Name (Type or Print): _____	26. Date Signed:
25. Signature of Document Control Officer (Required)	27. Phone Number:

**RETURN ALL REQUESTS TO: U.S. ENVIRONMENTAL PROTECTION AGENCY, OFFICE OF POLLUTION PREVENTION AND TOXICS,  
 MAINFRAME/LAN COORDINATOR, (TS-793), 401 M STREET, S.W., WASHINGTON, D.C. 20460**

## Section V - Signature (For Mainframe and LAN Coordinator's Use)

28. Mainframe or LAN Coordinator's Signature:	29. Date Received:
	30. Date Processed:
	31. Date Completed:



## Section VI - Instructions

**GENERAL INSTRUCTIONS:** This registration form is used to request user access to data or removal of privileges previously granted to users on the Mainframe and the LAN. All forms must be signed in Section IV. No request will be processed without the proper signatures.

### Section I: Action - Check all appropriate boxes.

This section gives the user an explanation of each action.

Assign New Id and Initial Password

Check this item if the applicant does not have Mainframe or LAN access. Complete all items in Section II, except 2 and 15. For Mainframe access, the user must also request access to at least one system; therefore "Add User to Accounts" must also be checked. The desired system(s) which the user needs access should be identified in Section III.

Add User to Accounts

Check this item if the user already has access to the Mainframe. Complete all items in Section II, except 14. The desired system(s) which the user needs access should be identified in Section III.

Update User Information

Check this item if the user needs to update employment information. Complete all applicable information in Section II, including item 2. Items 13, 14, and 15, in Section II need not be completed.

Delete User from Accounts

Check this item if the user no longer needs access to specific system(s). The user will not be deleted from the hardware, but will be deleted from the systems identified in Section III. Therefore, complete Section III and items 1, 2, and 3 in Section II.

Delete User from all Systems

Check this item if the user no longer needs access to the Mainframe and LAN hardware. This should be checked when a person terminates employment or no longer needs access to any TSCA system.

### Section II: Users Assigned to

This section refers to the applicant's actual employment duty station. (i.e. If the applicant is a contractor and works at an EPA facility, the address information is the EPA site.)

- Item 1: Enter the name of the users to be added to, or deleted from the system. Use the last name, first name, and middle initial format.
- Item 2: For mainframe users, enter the three character userid assigned to the user identified in item 1 above. If the user needs a userid, leave this item blank. Userids are not required for LAN users.
- Item 3: Enter the user's employer or company name.
- Item 4: Enter the office, division, branch, and section of the user. This applies to EPA employees only.
- Item 5: Enter the user's mailing address.
- Item 6: Enter the user's telephone number.
- Item 7: Enter the user's actual mailing city.
- Item 8: Enter the user's Region.
- Item 9: Enter the user's mail code.
- Item 10: Enter the user's 2-digit mailing state abbreviation.
- Item 11: Enter the user's 5 or 9-digit mailing zip code.
- Item 12: Self-explanatory
- Item 13: Enter last briefing date. Circle all sections of TSCA which the user is authorized to access.
- Item 14: Check the block which describes the task the user will perform.
- Item 15: Enter the date on which the user will no longer need access.

**Section III: TSCA Systems** - This section contains a collection of hardware and systems to access. Each registration form allows users to request access to two Mainframes and two LANs. Each hardware type is identified by a code which should be entered in this section. Use the list below to assist in selecting the desired TSCA hardware and systems to access.

Items 16 & 17: Enter the Mainframe hardware code to which access is requested. Only one code should be entered per item. To obtain access to the IBM 4381 Confidential (CBI) Production, enter code A. To obtain access to the IBM ES9000 Non-Confidential (NCBI) Production and Development, enter code B.

Items 16a & 17a: Enter the Mainframe system to which access is requested. Only one system should be entered per item. The systems on the IBM 4381 CBI Mainframe are: CICIS/CCID Facility (CCF), CAIR, CCID, CHEMD, CICIS, CUS, DAPSS, DMIS, PENTA, SATS, TUPS, Level 8(a), and Batch Retrieval (BR)

The systems on the ES9000 NCBI Production are: CECATS, CICIS, Batch Retrieval (BR) and MITS.

The systems on the ES9000 NCBI Development are: CICIS/CCID Facility (CCF), CAIR, CCID, CHEMD, CICIS, CUS, DAPSS, DMIS, PENTA, SATS, TUPS, Level 8(a), MITS, CECATS, and Batch Retrieval (BR).

Items 18 & 19: Enter the LAN hardware code to which access is requested. Only one code should be entered. To obtain access to the CBITS LAN, enter code C. To obtain access to the Administrative LAN, enter code D. To obtain access to the Image Processing LAN, enter code E. To obtain access to the New Chemical LAN, enter code F.

For NCC and Operations Staff: To obtain mainframe access, select the appropriate hardware code and enter the four character account number in the "Mainframe System to Access (list one)" field.

**Section IV - Signature Authority (Required before Processing):** No request will be processed without the proper signatures.

Items 20 through and 23 should be completed by the Requesting Official who is authorized to approve request. This person should be the supervisor of the applicant listed in item 1 of Section II.

Items 24 through 27 should be completed by the Document Control Officer of the applicant listed in item 1 of Section II.

**Section V - Signature (For Mainframe and LAN Coordinator's Use):** This section should be completed by the Mainframe and LAN Coordinator only.



**UNITED STATES ENVIRONMENTAL PROTECTION AGENCY**

WASHINGTON, D.C. 20460

**MEMORANDUM**

OFFICE OF  
PREVENTION, PESTICIDES AND  
TOXIC SUBSTANCES

**SUBJECT:** Request for EPA Identification Badge

**FROM:** Carolyn Thornton  
OPPT Document Control Officer  
Information Management Division  
Records and Docket Management Branch (7407)

**TO:** C. Steve Ziegler  
Acting Branch Chief  
Security and Property  
Management Branch  
Facilities Management and  
Services Division (3204)

The following **FEDERAL/GRANTEE/AARP/ON-SITE CONTRACTOR** employee with TSCA CBI access authorization has requested:

\_\_\_\_\_ New/Replacement Photo I.D. Badge  
\_\_\_\_\_ New/Replacement RUSCO CARD  
\_\_\_\_\_ Activation/Reactivation of existing RUSCO CARD  
\_\_\_\_\_ Fingerprints be taken for background investigation

Requester, please complete the information below to assist IMD's Records and Docket Management Branch and FMSD's Security Support Staff in processing your request.

**EMPLOYEE NAME:** \_\_\_\_\_  
**SOCIAL SECURITY NO.:** \_\_\_\_\_  
**RUSCO CARD NUMBER:** \_\_\_\_\_

**(BADGE NUMBER NEEDED IF YOU REQUEST  
ACTIVATION OF EXISTING RUSCO CARD)**

**STATUS CODE(s) :** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**AUTHORITY TO ARM/DISMARM (YES \_\_\_\_\_) (NO \_\_\_\_\_)**  
**TSCA CBI ZONE** \_\_\_\_\_

**BAR CODE:** \_\_\_\_\_  
**AUTHENTICATED BY:** \_\_\_\_\_  
**ACTIVATION DATE:** \_\_\_\_\_

Security Support Signature and Date

Return completed form to: Pam Moseley  
TSCA CBI Access Coordinator  
OPPT/IMD/RDMD (7407)

Internet Address (URL) • <http://www.epa.gov>

**MEMORANDUM****SUBJECT:** Request for Building Pass**FROM:**

Project Officer/ Federal SEE Monitor

SEP 6 2000

**TO:**Joyce Stewart  
Security Management Staff

I request that the below listed personnel be issued a Building Pass. The following data is furnished:

<u>NAME</u>	<u>DATE OF BIRTH</u>	<u>ROOM/TELEPHONE#</u>
<b>COMPANY/GRANTEE:</b> _____		
<b>CONTRACT/GRANT NUMBER:</b> _____		
<b>NORMAL HOURS OF WORK:</b> _____ <b>EXPIRATION DATE:</b> _____		
<b>SPECIAL ACCESS:</b> After 6:30 pm ___ Weekends ___ Holidays ___		
<b>LOCATION:</b> WSM ___ CM-2 ___ FAIRCHILD ___ CRYSTAL STATION ___		
501 ___ 14TH ST ___ ROSSLYN ___ CRYSTAL GATEWAY ___		
ARIEL RIOS ___ RONALD REAGAN ___ GLOVER(RIGGS) ___		
FRANKLIN COURT _____		
<b>RUSCO CARD NEEDED:</b> ___ YES ___ NO <b>ROOM#</b> _____ <b>MAIL CODE</b> _____		

As Project Officer/Federal SEE Monitor, I certify I have read the memorandum on instructions for building passes dated 7-8-99 and understand I am responsible for retrieving the above building pass(es) should:

1. The individual(s) transfer or terminate and no longer require access.
2. The individual(s) need for access to EPA be changed to less than 24-hours per week.
3. The contract/ grant expires.

\_\_\_\_\_  
SIGNATURE

PROJECT OFFICER/FEDERAL SEE MONITOR

\_\_\_\_\_  
TELEPHONE#\_\_\_\_\_  
MAIL CODE\_\_\_\_\_  
EPA ID CARD NUMBER of the  
PROJECT OFFICER/ FEDERAL SEE MONITOR  
(Revised 07/99-- all others are obsolete)\_\_\_\_\_  
DIVISION\_\_\_\_\_  
DATE



United States Environmental Protection Agency  
 TSCA Confidential Business Information  
 Document Reconciliation Certification

Name: \_\_\_\_\_ Organization: \_\_\_\_\_ Date: \_\_\_\_\_  
 ID Number: \_\_\_\_\_ Mail Code: \_\_\_\_\_  Federal  Contractor

THE TSCA CBI DOCUMENT TRACKING SYSTEM(S) INDICATED THAT THE DOCUMENTS LISTED BELOW HAVE BEEN LOGGED OUT IN YOUR NAME. PLEASE INVENTORY THESE DOCUMENTS AND INDICATE THEIR CURRENT STATUS.

<u>Document Control Number</u>	<u>Bar Code</u>	<u>Date</u>	<u>Logout Date</u>	<u>Login Status</u>

I HEREBY CERTIFY:

- THAT I HAVE INVENTORIED THE DOCUMENT(S) LISTED ABOVE; THE STATUS OF EACH DOCUMENT IS INDICATED ABOVE.
- ANNIVERSARY / BRIEFING DATE \_\_\_\_\_ (circle one).
- I ATTENDED MY ANNUAL TSCA CBI TRAINING ON \_\_\_\_\_.

SIGNATURE \_\_\_\_\_ DATE \_\_\_\_\_ DOCUMENT CONTROL OFFICER \_\_\_\_\_ DATE \_\_\_\_\_



## Confidentiality Agreement for United States Employees Upon Relinquishing TSCA CBI Access Authority

In accordance with my official duties as an employee of the United States, I have had access to Confidential Business Information under the Toxic Substances Control Act (TSCA, 15 U.S.C. 2601 et seq.). I understand that TSCA Confidential Business Information may not be disclosed except as authorized by TSCA or Agency regulations.

I certify that I have returned all copies of any materials containing TSCA Confidential Business Information in my possession to the appropriate document control officer specified in the procedures set forth in the TSCA Confidential Business Information Security Manual.

I agree that I will not remove any copies of materials containing TSCA Confidential Business Information from the premises of the Agency upon my termination or transfer. I further agree that I will not disclose any TSCA Confidential Business Information to any person after my termination or transfer.


I understand that as an employee of the United States who has had access to TSCA Confidential Business Information, under section 14(d) of TSCA (15 U.S.C. 2613(d)) I am liable for a possible fine of up to \$5,000 and/or imprisonment for up to one year if I willfully disclose TSCA Confidential Business Information to any person.

If I am still employed by the United States, I also understand that I may be subject to disciplinary action for violation of this agreement.

I am aware that I may be subject to criminal penalties under 18 U.S.C. 1001 if I have made any statement of material facts knowing that such statement is false or if I willfully conceal any material fact.

Name <i>(Please type or print)</i>	EPA ID Number
Signature	Date

Please read Privacy Act Statement on reverse before completing.

	United States Environmental Protection Agency Washington, DC 20460	Social Security Number	
<b>Employee Separation or Transfer Checklist</b>			
<b>Part 1. To Be Completed by Employee</b>			
Employee Name	Current Organization and Location	Effective Date	
Type of Action	Address (Forwarding or that of gaining Government unit or agency)		
<input type="checkbox"/> Separation from Government <input type="checkbox"/> Transfer to Other Government Unit			
Reason for Leaving			
<b>Part 2. Responsible Officials Must Complete All Items in this Part</b>			
Please clear the above-named employee. Final salary payment and application for retirement will be delayed until clearance is completed.			
	Clearance Yes    No	Signature and Date	
Item			
<b>Payroll/Travel</b>	Advance Leave		
	LWOP/Health Benefits		
	Outstanding Travel Advance		
	Outstanding Travel Voucher		
	GTR/Airline Ticket		
	Diners' Club (TM) Credit Card		
	Permanent Change of Station Requirements		
	Imprest Fund		
	Jury Duty Fees		
	Salary Checks		
<b>Personnel</b>	Training Termination Statements		
	Completion of Employment Agreements		
<b>Other</b>	Library Issuances		
	Security Termination Statements		
<b>Security/Facilities</b>	Audiovisual Equipment		
	EPA ID Card		
	Keys		
	Parking Permit		
	Special Credentials		
<b>Part 3. Certification and Clearance</b>			
The Administrative Officer/Supervisor must certify that the above-named employee has accounted for the items listed below.			
Item	Clearance Yes    No	Item Clearance Yes    No	
Personal property		CBI documents	
Telephone credit cards		NCC computer user ID	
Property pass(es)		U.S.-Government-issued Credit Card(s)	
SF-44, Purchase Orders		Official Passport (If yes, phone OIA/Passport Office)	
<input type="checkbox"/> Cleared <input type="checkbox"/> Not Cleared (Explain under Remarks)	Signature of Administrative Officer or Supervisor		
Remarks			
<b>Certification</b> I certify that the statements I have made on this form and all attachments thereto are true, accurate, and complete. I acknowledge that any knowingly false or misleading statement may be punishable by fine or imprisonment or both under applicable law.			
<b>Employee Certification</b>			
I certify that all U.S. Government property (including an official passport) and records have been returned (Signature)		Date	
<b>Personnel Office Affirmation of Clearance</b>			
Signature of Servicing Personnel Office	Title	Date	

## Privacy Act Statement

### Authority

**Social Security Number:** Executive Order 9397 dated November 22, 1943.

**Forwarding Address:** Reorganization Plan Number 3 of December 2, 1970.

### Purposes and Uses

**Social Security Number:** Disclosure by you of your Social Security Number (SSN) is voluntary. It will be used to properly identify your records on file with the U.S. EPA in various program areas from which you are obtaining certification of clearance. The information gathered will be used only as needed to complete the clearance process as required by EPA Order 3110.5A.

**Forwarding Address:** Disclosure by you of your forwarding address is voluntary. It will be used in forwarding official papers or appropriate information, and to mail documents to you or to a gaining Government unit or agency.

### Effects of Nondisclosure

**Social Security Number:** Withholding the SSN will cause a delay in the separation process or may result in your not being cleared for separation.

**Forwarding Address:** Withholding the forwarding address will cause a delay in the separation process or may deter your receipt of outstanding paychecks or other authorized documents.



United States Environmental Protection Agency  
Washington, D.C. 20460

## Request for Approval of Contractor Access to TSCA Confidential Business Information

Requesting Official

Signature

Date

Title and Office

Contractor and contract number (if modification)

I. Brief description of contract, including purposes, scope, length, and other important details. (Continue on the back of this form if necessary)

II. What TSCA CBI will be required, and why? (Continue on back if necessary)

III. Will computer access to TSCA CBI be required by the contract? If so, explain why and to what extent on the back of this form.

If you approve this request, this office will initiate procedures to ensure compliance with the "TSCA-CBI Security Manual".

Approval of the Director, OPPT Information Management Division

Approved (Signature)

Date

## EPA ACQUISITION REGULATION

1901  
09/12/00**1552.235-78 Data Security for Toxic Substances Control Act  
Confidential Business Information (Dec 1997).**

As prescribed in 1535.007-70(e), insert the following clause:

**DATA SECURITY FOR TOXIC SUBSTANCES CONTROL ACT  
CONFIDENTIAL BUSINESS INFORMATION (DECEMBER 1997)**

The Contractor shall handle Toxic Substances Control Act (TSCA) confidential business information (CBI) in accordance with the contract clause entitled "Treatment of Confidential Business Information" and "Screening Business Information for Claims of Confidentiality."

(a) The Project Officer (PO) or his/her designee, after a written determination by the appropriate program office, may disclose TSCA CBI to the contractor necessary to carry out the work required under this contract. The Contractor shall protect all TSCA CBI to which it has access (including CBI used in its computer operations) in accordance with the following requirements:

(1) The Contractor and Contractor's employees shall follow the security procedures set forth in the TSCA CBI Security Manual. The manual may be obtained from the Director, Information Management Division (IMD), Office of Pollution Prevention and Toxics (OPPT), U.S. Environmental Protection Agency (EPA), Ariel Rios Building, 1200 Pennsylvania Avenue, Washington, DC 20460. Prior to receipt of TSCA CBI by the Contractor, the Contractor shall ensure that all employees who will be cleared for access to TSCA CBI have been briefed on the handling, control, and security requirements set forth in the TSCA CBI Security Manual.

(2) The Contractor shall permit access to and inspection of the Contractor's facilities in use under this contract by representatives of EPA's Assistant Administrator for Administration and Resources Management, and the TSCA Security Staff in the OPPT, or by the EPA Project Officer.

(3) The Contractor Document Control Officer (DCO) shall obtain a signed copy of EPA Form 7740-6, "TSCA CBI Access Request, Agreement, and Approval," from each of the Contractor's employees who will have access to the information before the employee is allowed access. In addition, the Contractor shall obtain from each employee who will be cleared for TSCA CBI access all information required by EPA or the U.S. Office of Personnel Management for EPA to conduct a Minimum Background Investigation.

(b) The Contractor agrees that these requirements concerning protection of TSCA CBI are included for the benefit of, and shall be enforceable by, both EPA and any affected business having a proprietary interest in the information.

(c) The Contractor understands that CBI obtained by EPA under TSCA may not be disclosed except as authorized by the Act, and that any unauthorized disclosure by the Contractor or the Contractor's employees may subject the Contractor and the Contractor's employees to the criminal penalties specified in TSCA (15 U.S.C. 2613(d)). For purposes of this contract, the only disclosures that EPA authorizes the Contractor to make are those set forth in the clause entitled "Treatment of Confidential Business Information."

(d) The Contractor agrees to include the provisions of this clause, including this paragraph (d), in all subcontracts awarded pursuant to this contract that require the furnishing of CBI to the subcontractor.

(e) At the request of EPA or at the end of the contract, the Contractor shall return to the EPA PO or his/her designee, all documents, logs, and magnetic media which contain TSCA CBI. In addition, each Contractor employee who has received TSCA CBI clearance will sign EPA Form 7740-18, "Confidentiality Agreement for Contractor Employees Upon Relinquishing TSCA CBI Access Authority." The Contractor DCO will also forward those agreements to the EPA OPPT/IMD, with a copy to the CO, at the end of the contract.

(f) If, subsequent to the date of this contract, the Government changes the security requirements, the CO shall equitably adjust affected provisions of this contract, in accordance with the "Changes" clause, when:

- (1) The Contractor submits a timely written request for an equitable adjustment; and,
- (2) The facts warrant an equitable adjustment.

(End of clause)

## EPA ACQUISITION REGULATION

1901

09/12/00

1552.235-75 Access to Toxic Substances Control Act Confidential Business Information (Apr 1996).

As prescribed in 1535.007(b), insert the following provision:

ACCESS TO TOXIC SUBSTANCES CONTROL ACT  
CONFIDENTIAL BUSINESS INFORMATION (APR 1996)

In order to perform duties under the contract, the Contractor will need to be authorized for access to Toxic Substances Control Act (TSCA) confidential business information (CBI). The Contractor and all of its employees handling CBI while working under the contract will be required to follow the procedures contained in the security manual entitled "TSCA Confidential Business Information Security Manual." These procedures include applying for TSCA CBI access authorization for each individual working under the contract who will have access to TSCA CBI, execution of confidentiality agreements, and designation by the Contractor of an individual to serve as a document Control Officer. The Contractor will be required to abide by those clauses contained in EPAAR 1552.235-70, 1552.235-71, and 1552.235-78 that are appropriate to the activities set forth in the contract.

Until EPA has inspected and approved the Contractor's facilities, the Contractor may not be authorized for TSCA CBI access away from EPA facilities.

(End of provision)

## EPA ACQUISITION REGULATION

1901  
09/12/00**1552.235-76. Treatment of Confidential Business Information (TSCA) (Apr 1996).**

As prescribed in 1535.007-70(c), insert the following clause:

## TREATMENT OF CONFIDENTIAL BUSINESS INFORMATION (TSCA) (APR 1996)

(a) The Project Officer (PO) or his/her designee, after a written determination by the appropriate program office, may disclose confidential business information (CBI) to the Contractor necessary to carry out the work required under this contract. The Contractor agrees to use the CBI only under the following conditions:

(1) The Contractor and Contractor's employees shall (i) use the CBI only for the purposes of carrying out the work required by the contract; (ii) not disclose the information to anyone other than properly cleared EPA employees without the prior written approval of the Assistant General Counsel for Information Law or his/her designee; and (iii) return the CBI to the PO or his/her designee, whenever the information is no longer required by the Contractor for performance of the work required by the contract, or upon completion of the contract.

(2) The Contractor shall obtain a written agreement to honor the above limitations from each of the Contractor's employees who will have access to the information before the employee is allowed access.

(3) The Contractor agrees that these contract conditions concerning the use and disclosure of CBI are included for the benefit of, and shall be enforceable by, both EPA and any affected businesses having a proprietary interest in the information.

(4) The Contractor shall not use any CBI supplied by EPA or obtained during performance hereunder to compete with any business to which the CBI relates.

(b) The Contractor agrees to obtain the written consent of the CO, after a written determination by the appropriate program office, prior to entering into any subcontract that will involve the disclosure of CBI by the Contractor to the subcontractor. The Contractor agrees to include this clause, including this paragraph (b), in all subcontracts awarded pursuant to this contract that require the furnishing of CBI to the subcontractor.

(End of clause)





**CONTRACTOR INFORMATION SHEET  
CONTRACTOR TSCA CBI ACCESS/TRANSFER**

1. Contractor Name (list all subcontractors on separate contractor information sheets)	2. Contract Number	3. Prime _____ Sub _____
--	--------------------	-----------------------------

4. Corporate Address	5. Site Address (where TSCA CBI will be stored)
----------------------	---

6. List Previous Contract Number if renewal

	a) Name	b) Soc. Sec. No.	c) Telephone	d) Address/Mail Code
7. EPA Project Officer				
8. EPA DOPO/WAM				
9. EPA Task Mgr.				
10. Contractor Project Officer				
11. Contractor DCO				
12. Contractor Alt. DCO				

13. Description of duties to be performed by contractor that require TSCA CBI access (use attachment if necessary):

14. By Section of TSCA, type(s) of data to be accessed:

15a. Will CBI be transferred off EPA site under contract?  (Y/N)	15b. If CBI will transferred to a site other than listed in item 5 above, list site.	16a. Has a contractor Security Certification Statement been approved by TSCA Security Staff?  (Y/N)	16b. TSCA Security Staff Facility Inspection Date.
17. Desired Date for access to commence	18. Access desired until what date?	19. Contract Expiration Date	20. Is contract renewable?

21. EPA Project Officer Signature and Date

**Please return this form with a copy of:**  
**1. Statement of Work, 2. EPA form 7740-17, 3. CBI Clause from contract, and 4. Security Certification Statement**  
**to: U.S. EPA, TSCA CBI Access Staff, TS-790, 401 M Street, SW, Washington, DC 20460**  
**(202-260-1532)**



## **Privacy Act Statement**

Collection of the information on this form is authorized by Section 14 of the Toxic Substances Control Act (TSCA), 15 USC 2613. EPA uses this information to maintain a record of those persons cleared for access to TSCA Confidential Business Information (CBI) and to maintain the security of TSCA CBI.

Disclosure of this information may be made to Office of Pollution Prevention and Toxics (OPPT) contractors in order to carry out functions for EPA compatible with the purpose for which this information is collected; to other Federal agencies when they possess TSCA CBI and need to verify clearance of EPA and EPA contractor employees for access; to the Department of Justice when related to litigation or anticipated litigation involving the records or the subject matter of the records; to the appropriate Federal, State, or local agency charged with enforcing a statute or regulation, violation of which is indicated by a record in this system; where necessary, to a State, Federal, or local agency maintaining information pertinent to hiring, retention or clearance of an employee, letting of a contract, or issuance of a grant or other magistrate or administrative tribunal; to opposing counsel in the course of settlement negotiations; and to a member of Congress acting on behalf of an individual to whom records in the system pertain.

Furnishing the information on this form, including your Social Security Number, is voluntary but may prevent the contracting organization from being given access to TSCA CBI and may therefore make impossible the performance of any task which requires access to TSCA CBI.

CHECKLIST #1

**CONTRACTOR CHECKLIST FOR**  
**TSCA CBI ACCESS**  
**(ALL INFORMATION MUST BE SUBMITTED BY THE EPA PROJECT OFFICER**  
**TO THE TSCA CBI ACCESS COORDINATOR)**

Yes \_\_\_/No \_\_\_ Will this contract expire within 90 days?  
CONTRACT EXPIRATION DATE \_\_\_\_\_

Yes \_\_\_/No \_\_\_ Will this be a new or recompleted contract?

Yes \_\_\_/No \_\_\_ Are you the PRIME CONTRACTOR?

Yes \_\_\_/No \_\_\_ Will you have a SUBCONTRACTOR(s)? If yes, you will have to submit all the below required forms on them. They will be printed under one Federal Register Notice with their Prime Contractor.

\_\_\_\_\_ **Memo requesting "TSCA CBI Access Authorization" for the CONTRACTOR, from your Division Director to:**

**Director**  
**Information Management Division (7407M)**  
**Office of Pollution Prevention & Toxics**  
**1200 Pennsylvania Ave., NW**  
**Washington, D.C. 20460**

\_\_\_\_\_ **SITE INSPECTION MEMO** (If the site is new, and will be maintaining CBI, they must be inspected/approved in writing by the TSCA Security Staff (TSS) of EAD. If this is a recomplete and the same site is being used, and there is a gap of more than 1 month between the expired and start of the new contract, that facility must be reinspected and verified in writing by TSS also. Address your memo to request a site inspection as follows:

**Memo from your Division Director to:**

**Director**  
**Environmental Assistance Division (7408M)**  
**Office of Pollution Prevention & Toxics**  
**1200 Pennsylvania Ave., NW**  
**Washington, D.C. 20460**

**CONTRACTOR CHECKLIST FOR  
TSCA CBI ACCESS**

(Continued)

\_\_\_\_\_ **EPA Fm 7740-17 (REQUEST FOR APPROVAL OF CONTRACTOR ACCESS TO TSCA CBI)**

\_\_\_\_\_ **EPA Fm 7740-27 (CONTRACTOR INFORMATION SHEET - CONTRACTOR TSCA CBI ACCESS/TRANSFER)**

\_\_\_\_\_ **SOW**

\_\_\_\_\_ **PERIOD OF PERFORMANCE** dates (START & END DATES) for the Base and Four Option Year.

Yes \_\_\_\_\_ /No \_\_\_\_\_ **TSCA CBI CLAUSES** (From the 1996 version of the EPAAR) included or by reference? If these are not in the approved & signed contract, the EPA Project Officer must have a modification to contract that will add these clauses. TSCA CBI clearance cannot be granted to either the contractor or its employees, without these clauses in the contract.

\_\_\_\_\_ **LIST OF STAFF** (Those who will have access under this contract to TSCA CBI.

\_\_\_\_\_ **WAIVER LETTER** (Immediate access to CBI can only be granted by the IMD/DD via a waiver prior to publication in the FR. If you feel one is needed, you must provide a very strong justification for the IMD Division Director)

**SUBJECT:** Request Approval for Interim Access to TSCA CBI for **CONTRACTOR COMPANY NAME** under Contract # \_\_\_\_\_

**FROM:** Office Manager's Name and Title  
Branch and Division Name (MAIL CODE)

**TO:** Director  
Information Management Division (7407M)  
Office of Pollution Prevention & Toxics  
1200 Pennsylvania Ave., NW  
Washington, DC 20460

\_\_\_\_\_ **Draft FRN (TSCA CBI ACCESS COORDINATOR WILL TAKE CARE OF THIS)**

**CONTRACTOR CHECKLIST FOR**  
**TSCA CBI ACCESS**

(Continued)

**NOTE:** ACCESS is normally granted to the contractor 5 days after publication date in the REGISTER, unless an approved waiver for immediate access has been approved by the IMD/DD. Contractor Employees cannot be granted access to TSCA CBI prior to the approval of the Contractor. **Forward all completed packages to:**

U.S. EPA  
ICC Building, Room 6104  
IMD/RDMB (7407M)  
1200 Pennsylvania Ave., NW  
Washington, D.C. 20460  
Attn: Pam Moseley  
202-564-8956

CHECKLIST #2**CONTRACTOR EMPLOYEE CHECKLIST FOR  
TSCA CBI ACCESS****(ALL INFORMATION MUST BE SUBMITTED BY THE EPA PROJECT OFFICER  
TO THE TSCA CBI ACCESS COORDINATOR)**

\_\_\_\_\_ **Request for Building Pass memo (From the PO or FM, addressed to the Security Management Staff) The original must go with you to get your photo I.D., IF APPLICABLE**

\_\_\_\_\_ **Request for EPA Identification Badge (From the OPPT DCO) The original must go with you to get your photo I.D., IF APPLICABLE**

\_\_\_\_\_ **EPA Fm 7740-06 (TSCA CBI ACCESS REQUEST, AGREEMENT AND APPROVAL) A copy of this must go with you to get your photo I.D.**

\_\_\_\_\_ **EPA Fm 7740-25 (TSCA CBI ADP USER REGISTRATION) IF APPLICABLE**

\_\_\_\_\_ **SF 86 (QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS)  
Must be the "Revised Sep 95" version**

- Any cross-outs must be initiated by the applicant
- The Social Security Number must be at the bottom of each page as noted.
- There must not be any gaps in "Residence"
- There must not be any gaps in "Employment"; even if you are unemployed, you must show the periods of unemployment within the flow of your employment record.
- If you were not born in the U.S. (Naturalized, etc.) you must provide the "Place of Birth"
- Any one you list in ITEMS 13 and 14, whose "Country of Birth" or "Country of Citizenship" is not the U.S.A, you must provide their "certificate/registration" in ITEM 15.
- Make sure you sign and date pages "9", "10", and the "Medical Release Form"

\_\_\_\_\_ **Fingerprint Cards- "FD258 Applicant" version (2) (These must go with you when you get your photo I.D. Completed cards must be returned to TSCA CBI Access Coordinator)**

\_\_\_\_\_ **IF YOUR SECURITY OFFICE WILL BE SUBMITTING PAPERWORK FOR THE MBIs OR NACIs, PLEASE SUPPLY DOCUMENTATION AS TO WHEN THE MBI/NACI REQUEST WAS INITIATED OR COMPLETED FAVORABLY.**

CHECKLIST #2

**CONTRACTOR EMPLOYEE CHECKLIST FOR  
TSCA CBI ACCESS**

(continued)

\_\_\_\_\_ **Watch the TSCA CBI Security Video.** Make arrangements through your DCO or call 202-564-8956. Obtain a copy of the TSCA CBI Security Manual.

\_\_\_\_\_ **OPM Fm 147-4 (Reimbursement of OPM Invest.)**; The fee is \$375.00; Contact the OPPT/DCO, or contact the TSCA CBI ACCESS COORDINATOR at 202-564-8956.

\_\_\_\_\_ **BADGE ISSUE:** On-site contractor must to take the following papers to the West Tower I.D. Desk for EPA Badges:

- Original "Request for Bldg Pass Memo"
- Original "Request for EPA I.D. Badge Memo"
- Copy of EPA Form 7740-6

\_\_\_\_\_ **TSCA CBI ACCESS COORDINATOR FILES:** The following must be filed in the individual's access files:

- Copy of "Request for Building Pass Memo"
- Copy of "Request for EPA I.D. Badge Memo"
- Original EPA Form 7740-6
- Copy of EPA Form 7740-25

\_\_\_\_\_ **ADP USER ACCESS:** (For access to the CBI LAN) Provide an original copy of EPA Form 7740-25 to the CHIEF, INFORMATION TECHNOLOGY AND SUPPORT BRANCH of IMD.

**NOTE:** All of the above actions (with the exception of the last item) must be completed and submitted to the TSCA CBI Access Coordinator, prior to granting contractor employees access to TSCA CBI. Contractor Employees cannot be granted access to TSCA CBI prior to the approval of the Contractor. Forward all completed packages to:

U.S. EPA  
ICC Building, Room 6104  
IMD/RDMB (7407M)  
1200 Pennsylvania Ave, NW  
Washington, D.C. 20460  
Attn: Pam Moseley  
202-564-8956

Standard Form 86  
Revised September 1995  
U.S. Office of Personnel Management  
5 CFR Parts 731, 732, and 736

Form approved:  
O.M.B. No. 3206-0007  
NSN 7540-00-634-4036  
86-111

# Questionnaire for National Security Positions

Follow instructions fully or we cannot process your form. Be sure to sign and date the certification statement on page 9 and the release on page 10. *If you have any questions*, call the office that gave you the form.

## Purpose of this Form

The U.S. Government conducts background investigations and reinvestigations to establish that military personnel, applicants for or incumbents in national security positions, either employed by the Government or working for Government contractors, licensees, certificate holders, and grantees, are eligible for a required security clearance. Information from this form is used primarily as the basis for investigation for access to classified information or special nuclear information or material. Complete this form only after a conditional offer of employment has been made for a position requiring a security clearance.

Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or security clearance prospects.

## Authority to Request this Information

Depending upon the purpose of your investigation, the U.S. Government is authorized to ask for this information under Executive Orders 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; and parts 5, 732, and 736 of Title 5, Code of Federal Regulations.

Your Social Security number is needed to keep records accurate, because other people may have the same name and birth date. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

## The Investigative Process

Background investigations for national security positions are conducted to develop information to show whether you are reliable, trustworthy, of good conduct and character, and loyal to the United States. The information that you provide on this form is confirmed during the investigation. Investigation may extend beyond the time covered by this form when necessary to resolve issues. Your current employer must be contacted as part of the investigation, even if you have previously indicated on applications or other forms that you do not want this.

In addition to the questions on this form, inquiry also is made about a person's adherence to security requirements, honesty and integrity, vulnerability to exploitation or coercion, falsification, misrepresentation, and any other behavior, activities, or associations that tend to show the person is not reliable, trustworthy, or loyal.

## Your Personal Interview

Some investigations will include an interview with you as a normal part of the investigative process. This provides you the opportunity to update, clarify, and explain information on your form more completely, which often helps to complete your investigation faster. It is important that the interview be conducted as soon as possible after you are contacted. Postponements will delay the processing of your investigation, and declining to be interviewed may result in your investigation being delayed or canceled.

You will be asked to bring identification with your picture on it, such as a valid State driver's license, to the interview. There are other documents you may be asked to bring to verify your identity as well. These include documentation of any legal name change, Social Security card, and/or birth certificate.

You may also be asked to bring documents about information you provided on the form or other matters requiring specific attention. These matters include alien registration, delinquent loans or taxes, bankruptcy, judgments, liens, or other financial obligations, agreements involving child custody or support, alimony or property settlements, arrests, convictions, probation, and/or parole.

## Organization of this Form

This form has two parts. Part 1 asks for background information, including where you have lived, gone to school, and worked. Part 2 asks about your activities and such matters as firings from a job, criminal history record, use of illegal drugs, and abuse of alcohol.

In answering all questions on this form, keep in mind that your answers are considered together with the information obtained in the investigation to reach an appropriate adjudication.

## Instructions for Completing this Form

1. Follow the instructions given to you by the person who gave you the form and any other clarifying instructions furnished by that person to assist you in completion of the form. Find out how many copies of the form you are to turn in. You must sign and date, in black ink, the original and each copy you submit. You should retain a copy of the completed form for your records.
2. Type or legibly print your answers in black ink (if your form is not legible, it will not be accepted). You may also be asked to submit your form in an approved electronic format.
3. All questions on this form must be answered. If no response is necessary or applicable, indicate this on the form (for example, enter "None" or "N/A"). If you find that you cannot report an exact date, approximate or estimate the date to the best of your ability and indicate this by marking "APPROX." or "EST."
4. Any changes that you make to this form after you sign it must be initialed and dated by you. Under certain limited circumstances, agencies may modify the form consistent with your intent.
5. You must use the State codes (abbreviations) listed on the back of this page when you fill out this form. Do not abbreviate the names of cities or foreign countries.
6. The 5-digit postal ZIP codes are needed to speed the processing of your investigation. The office that provided the form will assist you in completing the ZIP codes.
7. All telephone numbers must include area codes.
8. All dates provided on this form must be in Month/Day/Year or Month/Year format. Use numbers (1-12) to indicate months. For example, June 8, 1978, should be shown as 6/8/78.
9. Whenever "City (Country)" is shown in an address block, also provide in that block the name of the country when the address is outside the United States.

10. If you need additional space to list your residences or employments/self-employments/unemployments or education, you should use a continuation sheet, SF 86A. If additional space is needed to answer other items, use a blank piece of paper. Each blank piece of paper you use must contain **your name and Social Security Number at the top of the page.**



## Final Determination on Your Eligibility

Final determination on your eligibility for access to classified information is the responsibility of the Federal agency that requested your investigation. You may be provided the opportunity personally to explain, refute, or clarify any information before a final decision is made.

## Penalties for Inaccurate or False Statements

The U.S. Criminal Code (title 18, section 1001) provides that knowingly falsifying or concealing a material fact is a felony which may result in fines of up to \$10,000, and/or 5 years imprisonment, or both. In addition, Federal agencies generally fire, do not grant a security clearance, or disqualify individuals who have materially and deliberately falsified these forms, and this remains a part of the permanent record for future placements. Because the position for which you are being considered is a sensitive one, your trustworthiness is a very important consideration in deciding your eligibility for a security clearance. Your prospects of placement or security clearance

are better if you answer all questions truthfully and completely. You will have adequate opportunity to explain any information you give us on the form and to make your comments part of the record.

## Disclosure of Information

The information you give us is for the purpose of investigating you for a national security position; we will protect it from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information is governed by the Privacy Act. The agency which requested the investigation and the agency which conducted the investigation have published notices in the Federal Register describing the systems of records in which your records will be maintained. You may obtain copies of the relevant notices from the person who gave you this form. The information on this form, and information we collect during an investigation may be disclosed without your consent as permitted by the Privacy Act (5 USC 552a (b) ) and as follows:

## PRIVACY ACT ROUTINE USES

1. To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

2. To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

3. Except as noted in Question 24, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute, particular program statute, regulation, rule, or order issued pursuant thereto, the relevant records may be disclosed to the appropriate Federal, foreign, State, local, tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order.

4. To any source or potential source from which information is requested in the course of an investigation concerning the hiring or retention of an employee or other personnel action, or the issuing or retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

5. To a Federal, State, local, foreign, tribal, or other public authority the fact that this system of records contains information relevant to the retention of an employee, or the retention of a security clearance, contract, license, grant, or other benefit. The other agency or licensing organization may then make a request supported by written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

6. To contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to this record for which they have been engaged. Such recipients shall be required to comply with the Privacy Act of 1974, as amended.

7. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy.

8. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

9. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

10. To the National Archives and Records Administration for records management inspections conducted under 44 USC 2904 and 2906.

11. To the Office of Management and Budget when necessary to the review of private relief legislation.

## STATE CODES (ABBREVIATIONS)

Alabama	AL	Hawaii	HI	Massachusetts	MA	New Mexico	NM	South Dakota	SD
Alaska	AK	Idaho	ID	Michigan	MI	New York	NY	Tennessee	TN
Arizona	AZ	Illinois	IL	Minnesota	MN	North Carolina	NC	Texas	TX
Arkansas	AR	Indiana	IN	Mississippi	MS	North Dakota	ND	Utah	UT
California	CA	Iowa	IA	Missouri	MO	Ohio	OH	Vermont	VT
Colorado	CO	Kansas	KS	Montana	MT	Oklahoma	OK	Virginia	VA
Connecticut	CT	Kentucky	KY	Nebraska	NE	Oregon	OR	Washington	WA
Delaware	DE	Louisiana	LA	Nevada	NV	Pennsylvania	PA	West Virginia	WV
Florida	FL	Maine	ME	New Hampshire	NH	Rhode Island	RI	Wisconsin	WI
Georgia	GA	Maryland	MD	New Jersey	NJ	South Carolina	SC	Wyoming	WY
American Samoa Trust Territory	AS TT	Dist. of Columbia Virgin Islands	DC VI	Guam	GU	Northern Marianas	CM	Puerto Rico	PR

## PUBLIC BURDEN INFORMATION

Public burden reporting for this collection of information is estimated to average 90 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Reports and Forms Management Officer, U.S. Office of Personnel Management, 1900 E Street, N.W., Room CHP-500, Washington, D.C. 20415. Do not send your completed form to this address.

**QUESTIONNAIRE FOR  
 NATIONAL SECURITY POSITIONS**

<b>Part 1</b>	Investigating Agency Use Only	Codes	Case Number
<b>Agency Use Only (Complete Items A through P using instructions provided by the investigating agency).</b>			
<b>A</b> Type of Investigation	<b>B</b> Extra Coverage	<b>C</b> Sensitivity Level	<b>D</b> Access
<b>E</b> Nature of Action Code	<b>F</b> Date of Action	Month	Day Year
<b>G</b> Geographic Location	<b>H</b> Position Code	<b>I</b> Position Title	
<b>J</b> SON	<b>K</b> Location of Official Personnel Folder	None NPRC At SON	Other Address ZIP Code
<b>L</b> SOI	<b>M</b> Location of Security Folder	None At Sol NPI	Other Address ZIP Code
<b>N</b> OPAC-ALC Number	<b>O</b> Accounting Data and/or Agency Case Number		
<b>P</b> Requesting Official	Name and Title	Signature	Telephone Number ( ) Date

**Persons completing this form should begin with the questions below.**

<b>1 FULL NAME</b> • If you have only initials in your name, use them and state (IO). • If you have no middle name, enter "NMN." • If you are a "Jr.," "Sr.," "II," etc., enter this in the box after your middle name.	<b>2 DATE OF BIRTH</b>					
Last Name	First Name	Middle Name	Jr., II, etc.	Month	Day	Year

<b>3 PLACE OF BIRTH</b> • Use the two letter code for the State. City	County	State	Country (if not in the United States)	<b>4 SOCIAL SECURITY NUMBER</b>
--	--------	-------	---------------------------------------	---------------------------------

**5 OTHER NAMES USED**  
 Give other names you used and the period of time you used them (for example: your maiden name, name[s] by a former marriage, former name[s], alias[es], or nickname[s]). If the other name is your maiden name, put "nee" in front of it.

#1 Name	Month/Year	Month/Year	#3 Name	Month/Year	Month/Year
	To			To	
#2 Name	Month/Year	Month/Year	#4 Name	Month/Year	Month/Year
	To			To	

**6 OTHER IDENTIFYING INFORMATION**

Height (feet and inches)	Weight (pounds)	Hair Color	Eye Color	Sex (mark one box) <input type="checkbox"/> Female <input type="checkbox"/> Male
--------------------------	-----------------	------------	-----------	---

**7 TELEPHONE NUMBERS**

Work (include Area Code and extension) ( ) Day ( ) ( ) Night ( )	Home (include Area Code) ( ) Day ( ) ( ) Night ( )
--	--

**8 CITIZENSHIP**

Mark the box at the right that reflects your current citizenship status, and follow its instructions.	<input type="checkbox"/> I am a U.S. citizen or national by birth in the U.S. or U.S. territory/possession. → Answer Items b and d	<b>b</b> Your Mother's Maiden Name
	<input type="checkbox"/> I am a U.S. citizen, but I was NOT born in the U.S. → Answer Items b, c, and d	
	<input type="checkbox"/> I am not a U.S. citizen. → Answer Items b and e	

**9 UNITED STATES CITIZENSHIP** If you are a U.S. Citizen, but were not born in the U.S., provide information about one or more of the following proofs of your citizenship.

**Naturalization Certificate (Where were you naturalized?)**

Court	City	State	Certificate Number	Month/Day/Year Issued
-------	------	-------	--------------------	-----------------------

**Citizenship Certificate (Where was the certificate issued?)**

City	State	Certificate Number	Month/Day/Year Issued
------	-------	--------------------	-----------------------

**State Department Form 240 - Report of Birth Abroad of a Citizen of the United States**

Give the date the form was prepared and give an explanation if needed.	Month/Day/Year	Explanation
--	----------------	-------------

**U.S. Passport**

This may be either a current or previous U.S. Passport.	Passport Number	Month/Day/Year Issued
---	-----------------	-----------------------

**10 DUAL CITIZENSHIP** If you are (or were) a dual citizen of the United States and another country, provide the name of that country in the space to the right.

Country
---------

**11 ALIEN** If you are an alien, provide the following information:

Place You Entered the United States:	City	State	Date You Entered U.S. Month Day Year	Alien Registration Number	Country(ies) of Citizenship
--------------------------------------	------	-------	---	---------------------------	-----------------------------

**9 WHERE YOU HAVE LIVED**

List the places where you have lived, beginning with the most recent (#1) and working back 7 years. All periods must be accounted for in your list. Be sure to indicate the actual physical location of your residence: do not use a post office box as an address, do not list a permanent address when you were actually living at a school address, etc. Be sure to specify your location as closely as possible: for example, do not list only your base or ship, list your barracks number or home port. You may omit temporary military duty locations under 90 days (list your permanent address instead), and you should use your APO/FPO address if you lived overseas.

For any address in the last 5 years, list a person who knew you at that address, and who preferably still lives in that area (do not list people for residences completely outside this 5-year period, and do not list your spouse, former spouses, or other relatives). Also for addresses in the last five years, if the address is "General Delivery," a Rural or Star Route, or may be difficult to locate, provide directions for locating the residence on an attached continuation sheet.

Month/Year #1	Month/Year To Present	Street Address	Apt. #	City (Country)	State	ZIP Code
Name of Person Who Knows You		Street Address	Apt.#	City (Country)	State	ZIP Code
						Telephone Number ( )
Month/Year #2	Month/Year To	Street Address	Apt. #	City (Country)	State	ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State	ZIP Code
						Telephone Number ( )
Month/Year #3	Month/Year To	Street Address	Apt. #	City (Country)	State	ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State	ZIP Code
						Telephone Number ( )
Month/Year #4	Month/Year To	Street Address	Apt. #	City (Country)	State	ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State	ZIP Code
						Telephone Number ( )
Month/Year #5	Month/Year To	Street Address	Apt. #	City (Country)	State	ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State	ZIP Code
						Telephone Number ( )

**10 WHERE YOU WENT TO SCHOOL**

List the schools you have attended, beyond Junior High School, beginning with the most recent (#1) and working back 7 years. List College or University degrees and the dates they were received. If all of your education occurred more than 7 years ago, list your most recent education beyond high school, no matter when that education occurred.

- Use one of the following codes in the "Code" block:
  - 1 - High School
  - 2 - College/University/Military College
  - 3 - Vocational/Technical/Trade School
- For schools you attended in the past 3 years, list a person who knew you at school (an instructor, student, etc.). Do not list people for education completely outside this 3-year period.
- For correspondence schools and extension classes, provide the address where the records are maintained.

Month/Year #1	Month/Year To	Code	Name of School	Degree/Diploma/Other	Month/Year Awarded
Street Address and City (Country) of School					State
					ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State
				ZIP Code	Telephone Number ( )
Month/Year #2	Month/Year To	Code	Name of School	Degree/Diploma/Other	Month/Year Awarded
Street Address and City (Country) of School					State
					ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State
				ZIP Code	Telephone Number ( )
Month/Year #3	Month/Year To	Code	Name of School	Degree/Diploma/Other	Month/Year Awarded
Street Address and City (Country) of School					State
					ZIP Code
Name of Person Who Knew You		Street Address	Apt.#	City (Country)	State
				ZIP Code	Telephone Number ( )

Enter your Social Security Number before going to the next page



**11 YOUR EMPLOYMENT ACTIVITIES**

List your employment activities, beginning with the present (#1) and working back 7 years. You should list all full-time work, part-time work, military service, temporary military duty locations over 90 days, self-employment, other paid work, and all periods of unemployment. The entire 7-year period must be accounted for without breaks, but you need not list employments before your 16th birthday. **EXCEPTION:** Show all Federal civilian service, whether it occurred within the last 7 years or not.

• **Code.** Use one of the codes listed below to identify the type of employment:

- 1 - Active military duty stations
- 2 - National Guard/Reserve
- 3 - U.S.P.H.S. Commissioned Corps
- 4 - Other Federal employment
- 5 - State Government (Non-Federal employment)
- 6 - Self-employment (Include business name and/or name of person who can verify)
- 7 - Unemployment (Include name of person who can verify)
- 8 - Federal Contractor (List Contractor, not Federal agency)
- 9 - Other

• **Employer/Verifier Name.** List the business name of your employer or the name of the person who can verify your self-employment or unemployment in this block. If military service is being listed, include your duty location or home port here as well as your branch of service. You should provide separate listings to reflect changes in your military duty locations or home ports.

• **Previous Periods of Activity.** Complete these lines if you worked for an employer on more than one occasion at the same location. After entering the most recent period of employment in the initial numbered block, provide previous periods of employment at the same location on the additional lines provided. For example, if you worked at XY Plumbing in Denver, CO, during 3 separate periods of time, you would enter dates and information concerning the most recent period of employment first, and provide dates, position titles, and supervisors for the two previous periods of employment on the lines below that information.

#1	Month/Year To	Month/Year Present		Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank		
Employer's/Verifier's Street Address					City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)					City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)					City (Country)	State	ZIP Code	Telephone Number ( )

<b>PREVIOUS PERIODS OF ACTIVITY (Block #1)</b>	Month/Year	Month/Year	Position Title		Supervisor			
	To							
	Month/Year	Month/Year	Position Title		Supervisor			
	To							

#2	Month/Year To	Month/Year		Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank		
Employer's/Verifier's Street Address					City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)					City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)					City (Country)	State	ZIP Code	Telephone Number ( )

<b>PREVIOUS PERIODS OF ACTIVITY (Block #2)</b>	Month/Year	Month/Year	Position Title		Supervisor			
	To							
	Month/Year	Month/Year	Position Title		Supervisor			
	To							

#3	Month/Year To	Month/Year		Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank		
Employer's/Verifier's Street Address					City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)					City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)					City (Country)	State	ZIP Code	Telephone Number ( )

<b>PREVIOUS PERIODS OF ACTIVITY (Block #3)</b>	Month/Year	Month/Year	Position Title		Supervisor			
	To							
	Month/Year	Month/Year	Position Title		Supervisor			
	To							

Enter your Social Security Number before going to the next page →

**YOUR EMPLOYMENT ACTIVITIES (CONTINUED)**

Month/Year #4	Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank		
Employer's/Verifier's Street Address			City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)			City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)			City (Country)	State	ZIP Code	Telephone Number ( )
PREVIOUS PERIODS OF ACTIVITY (Block #4)	Month/Year To	Month/Year	Position Title	Supervisor		
	Month/Year To	Month/Year	Position Title	Supervisor		
	Month/Year To	Month/Year	Position Title	Supervisor		

Month/Year #5	Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank		
Employer's/Verifier's Street Address			City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)			City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)			City (Country)	State	ZIP Code	Telephone Number ( )
PREVIOUS PERIODS OF ACTIVITY (Block #5)	Month/Year To	Month/Year	Position Title	Supervisor		
	Month/Year To	Month/Year	Position Title	Supervisor		
	Month/Year To	Month/Year	Position Title	Supervisor		

Month/Year #6	Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank		
Employer's/Verifier's Street Address			City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)			City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)			City (Country)	State	ZIP Code	Telephone Number ( )
PREVIOUS PERIODS OF ACTIVITY (Block #6)	Month/Year To	Month/Year	Position Title	Supervisor		
	Month/Year To	Month/Year	Position Title	Supervisor		
	Month/Year To	Month/Year	Position Title	Supervisor		

**12 PEOPLE WHO KNOW YOU WELL**  
List **three people** who know you well and live in the United States. They should be good friends, peers, colleagues, college roommates, etc., whose combined association with you covers as well as possible the last 7 years. Do not list your spouse, former spouses, or other relatives, and try not to list anyone who is listed elsewhere on this form.

#1	Name	Dates Known Month/Year To Month/Year	Telephone Number ( ) Day ( ) ( ) Night ( )
Home or Work Address		City (Country)	State ZIP Code
#2	Name	Dates Known Month/Year To Month/Year	Telephone Number ( ) Day ( ) ( ) Night ( )
Home or Work Address		City (Country)	State ZIP Code
#3	Name	Dates Known Month/Year To Month/Year	Telephone Number ( ) Day ( ) ( ) Night ( )
Home or Work Address		City (Country)	State ZIP Code

Enter your Social Security Number before going to the next page

**13 YOUR SPOUSE**

Mark one box to show your current marital status and provide information about your spouse(s) in items a, and/or b.

1 - Never married  
 2 - Married

3 - Separated  
 4 - Legally Separated

5 - Divorced  
 6 - Widowed

**a Current Spouse** Complete the following about your current spouse only.

Full Name	Date of Birth	Place of Birth (Include country if outside the U.S.)	Social Security Number
Other Names Used (Specify maiden name, names by other marriages, etc., and show dates used for each name)			Country(ies) of Citizenship
Date Married	Place Married (Include country if outside the U.S.)		State
If Separated, Date of Separation	If Legally Separated, Where is the Record Located? City (Country)		State
Address of Current Spouse, if different than your current address (Street, city, and country if outside the U.S.)			State ZIP Code

**b Former Spouse(s)** Complete the following about your former spouse(s), use blank sheets if needed.

Full Name	Date of Birth	Place of Birth (Include country if outside the U.S.)	State
Country(ies) of Citizenship	Date Married	Place Married (Include country if outside the U.S.)	State
Check One, Then Give Date <input type="checkbox"/> Divorced <input type="checkbox"/> Widowed	Month/Day/Year	If Divorced, Where is the Record Located? City (Country)	State
Address of Former Spouse (Street, city, and country if outside the U.S.)		State ZIP Code	Telephone Number ( )

**14 YOUR RELATIVES AND ASSOCIATES**

Give the full name, correct code, and other requested information for each of your relatives and associates, living or dead, specified below.

- |                     |                          |                   |                    |                                      |
|---------------------|--------------------------|-------------------|--------------------|--------------------------------------|
| 1 - Mother (first)  | 5 - Foster parent        | 9 - Sister        | 13 - Half-sister   | 17 - Other Relative*                 |
| 2 - Father (second) | 6 - Child (adopted also) | 10 - Stepbrother  | 14 - Father-in-law | 18 - Associate*                      |
| 3 - Stepmother      | 7 - Stepchild            | 11 - Stepsister   | 15 - Mother-in-law | 19 - Adult Currently Living With You |
| 4 - Stepfather      | 8 - Brother              | 12 - Half-brother | 16 - Guardian      |                                      |

\* Code 17 (Other Relative)-include only foreign national relatives not listed in 1-16 with whom you or your spouse are bound by affection, obligation, or close and continuing contact. Code 18 (Associates) - include only foreign national associates with whom you or your spouse are bound by affection, obligation, or close and continuing contact.

Full Name (If deceased, check box on the left before entering name)	Code	Date of Birth Month/Day/Year	Country of Birth	Country(ies) of Citizenship	Current Street Address and City (country) of Living Relatives	State
<input type="checkbox"/>	1					
<input type="checkbox"/>	2					
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						

**15 CITIZENSHIP OF YOUR RELATIVES AND ASSOCIATES**

If your mother, father, sister, brother, child, or current spouse or person with whom you have a spouse-like relationship is a U.S. citizen by other than birth, or an alien residing in the U.S., provide the nature of the individual's relationship to you (Spouse, Spouse-like, Mother, etc.), and the individual's name and date of birth on the first line (this information is needed to pair it accurately with information in items 13 and 14).

On the second line, provide the individual's naturalization certificate or alien registration number and use one of the document codes below to identify proof of citizenship status. Provide additional information on that line as requested.

- 1. **Naturalization Certificate:** Provide the date issued and the location where the person was naturalized (Court, City and State).
- 2. **Citizenship Certificate:** Provide the date and location issued (City and State).
- 3. **Alien Registration:** Provide the date and place where the person entered the U.S. (City and State).
- 4. **Other:** Provide an explanation in the "Additional Information" block.

Association #1	Name	Date of Birth (Month/Day/Year)
Certificate/Registration #	Document Code	Additional Information
Association #2	Name	Date of Birth (Month/Day/Year)
Certificate/Registration #	Document Code	Additional Information

**16 YOUR MILITARY HISTORY**

- a Have you served in the United States military?
- b Have you served in the United States Merchant Marine?

	Yes	No
a		
b		

List all of your military service below, including service in Reserve, National Guard, and U.S. Merchant Marine. Start with the most recent period of service (#1) and work backward. If you had a break in service, each separate period should be listed.

- **Code.** Use one of the codes listed below to identify your branch of service:  
 1 - Air Force    2 - Army    3 - Navy    4 - Marine Corps    5 - Coast Guard    6 - Merchant Marine    7 - National Guard
- **O/E.** Mark "O" block for Officer or "E" block for Enlisted.
- **Status.** "X" the appropriate block for the status of your service during the time that you served. If your service was in the National Guard, do not use an "X"; use the two-letter code for the state to mark the block.
- **Country.** If your service was with other than the U.S. Armed Forces, identify the country for which you served.

Month/Year	Month/Year	Code	Service/Certificate #	Status				Country
				O	E	Active	Active Reserve	
To								
To								

**17 YOUR FOREIGN ACTIVITIES**

- a Do you have any foreign property, business connections, or financial interests?
- b Are you now or have you ever been employed by or acted as a consultant for a foreign government, firm, or agency?
- c Have you ever had any contact with a foreign government, its establishments (embassies or consulates), or its representatives, whether inside or outside the U.S., other than on official U.S. Government business? (Does not include routine visa applications and border crossing contacts.)
- d In the last 7 years, have you had an active passport that was issued by a foreign government?

	Yes	No
a		
b		
c		
d		

If you answered "Yes" to a, b, c, or d above, explain in the space below: provide inclusive dates, names of firms and/or governments involved, and an explanation of your involvement.

Month/Year	Month/Year	Firm and/or Government	Explanation
To			
To			

**18 FOREIGN COUNTRIES YOU HAVE VISITED**

List foreign countries you have visited, except on travel under official Government orders, beginning with the most current (#1) and working back 7 years. (Travel as a dependent or contractor must be listed.)

- Use one of these codes to indicate the purpose of your visit:    1 - Business    2 - Pleasure    3 - Education    4 - Other
- Include short trips to Canada or Mexico. If you have lived near a border and have made short (one day or less) trips to the neighboring country, you do not need to list each trip. Instead, provide the time period, the code, the country, and a note ("Many Short Trips").
- Do not repeat travel covered in items 9, 10, or 11.

Month/Year	Month/Year	Code	Country	Month/Year	Month/Year	Code	Country
#1	To			#3	To		
#2	To			#4	To		

This concludes Part 1 of this form. If you have used Page 9, continuation sheets, or blank sheets to complete any of the questions in Part 1, give the number for those questions in the space to the right:

Enter your Social Security Number before going to the next page →

## QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

### Part 2

OFFICIAL  
 USE  
 ONLY

<b>19</b>	<b>YOUR MILITARY RECORD</b>	<b>Yes</b>	<b>No</b>
Have you ever received other than an honorable discharge from the military? If "Yes," provide the date of discharge and type of discharge below.			

Month/Year	Type of Discharge		
------------	-------------------	--	--

<b>20</b>	<b>YOUR SELECTIVE SERVICE RECORD</b>	<b>Yes</b>	<b>No</b>
-----------	--------------------------------------	------------	-----------

- a** Are you a male born after December 31, 1959? If "No," go to 21. If "Yes," go to b.
- b** Have you registered with the Selective Service System? If "Yes," provide your registration number. If "No," show the reason for your legal exemption below.

Registration Number	Legal Exemption Explanation
---------------------	-----------------------------

<b>21</b>	<b>YOUR MEDICAL RECORD</b>	<b>Yes</b>	<b>No</b>
In the last 7 years, have you consulted with a mental health professional (psychiatrist, psychologist, counselor, etc.) or have you consulted with another health care provider about a mental health related condition?			

If you answered "Yes", provide the dates of treatment and the name and address of the therapist or doctor below, unless the consultation(s) involved only marital, family, or grief counseling, not related to violence by you.

Month/Year	Month/Year	Name/Address of Therapist or Doctor	State	ZIP Code
To				
To				

<b>22</b>	<b>YOUR EMPLOYMENT RECORD</b>	<b>Yes</b>	<b>No</b>
Has any of the following happened to you in the last 7 years? If "Yes," begin with the most recent occurrence and go backward, providing date fired, quit, or left, and other information requested.			

- Use the following codes and explain the reason your employment was ended:
- |  |  |  |
|--|--|--|
| 1 - Fired from a job                           | 3 - Left a job by mutual agreement following allegations of misconduct                 | 5 - Left a job for other reasons under unfavorable circumstances |
| 2 - Quit a job after being told you'd be fired | 4 - Left a job by mutual agreement following allegations of unsatisfactory performance |  |

Month/Year	Code	Specify Reason	Employer's Name and Address (Include city/Country if outside U.S.)	State	ZIP Code

<b>23</b>	<b>YOUR POLICE RECORD</b>	<b>Yes</b>	<b>No</b>
For this item, report information regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.			

- a** Have you ever been charged with or convicted of any felony offense? (Include those under Uniform Code of Military Justice)
- b** Have you ever been charged with or convicted of a firearms or explosives offense?
- c** Are there currently any charges pending against you for any criminal offense?
- d** Have you ever been charged with or convicted of any offense(s) related to alcohol or drugs?
- e** In the last 7 years, have you been subject to court martial or other disciplinary proceedings under the Uniform Code of Military Justice? (Include non-judicial, Captain's mast, etc.)
- f** In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s) not listed in response to a, b, c, d, or e above? (Leave out traffic fines of less than \$150 unless the violation was alcohol or drug related.)

If you answered "Yes" to a, b, c, d, e, or f above, explain below. Under "Offense," do not list specific penalty codes, list the actual offense or violation (for example, arson, theft, etc.).

Month/Year	Offense	Action Taken	Law Enforcement Authority/Court (Include City and county/country if outside U.S.)	State	ZIP Code

Enter your Social Security Number before going to the next page →



<b>24</b>	<b>YOUR USE OF ILLEGAL DRUGS AND DRUG ACTIVITY</b>	<b>Yes</b>	<b>No</b>
<p>The following questions pertain to the illegal use of drugs or drug activity. You are required to answer the questions fully and truthfully, and your failure to do so could be grounds for an adverse employment decision or action against you, but neither your truthful responses nor information derived from your responses will be used as evidence against you in any subsequent criminal proceeding.</p> <p><b>a</b> Since the age of 16 or in the last 7 years, whichever is shorter, have you <u>illegally</u> used any controlled substance, for example, marijuana, cocaine, crack cocaine, hashish, narcotics (opium, morphine, codeine, heroin, etc.), amphetamines, depressants (barbiturates, methaqualone, tranquilizers, etc.), hallucinogenics (LSD, PCP, etc.), or prescription drugs?</p> <p><b>b</b> Have you <u>ever</u> illegally used a controlled substance while employed as a law enforcement officer, prosecutor, or courtroom official; while possessing a security clearance; or while in a position directly and immediately affecting the public safety?</p> <p><b>c</b> In the last 7 years, have you been involved in the illegal purchase, manufacture, trafficking, production, transfer, shipping, receiving, or sale of any narcotic, depressant, stimulant, hallucinogen, or cannabis for your own intended profit or that of another?</p>			

If you answered "Yes" to a or b above, provide the date(s), identify the controlled substance(s) and/or prescription drugs used, and the number of times each was used.

Month/Year	Month/Year	Controlled Substance/Prescription Drug Used	Number of Times Used
To			
To			

<b>25</b>	<b>YOUR USE OF ALCOHOL</b>	<b>Yes</b>	<b>No</b>
<p>In the last 7 years, has your use of alcoholic beverages (such as liquor, beer, wine) resulted in any alcohol-related treatment or counseling (such as for alcohol abuse or alcoholism)?</p>			

If you answered "Yes", provide the dates of treatment and the name and address of the counselor or doctor below. Do not repeat information reported in response to item 21 above.

Month/Year	Month/Year	Name/Address of Counselor or Doctor	State	ZIP Code
To				
To				

<b>26</b>	<b>YOUR INVESTIGATIONS RECORD</b>	<b>Yes</b>	<b>No</b>
<p><b>a</b> Has the United States Government ever investigated your background and/or granted you a security clearance? If "Yes," use the codes that follow to provide the requested information below. If "Yes," but you can't recall the investigating agency and/or the security clearance received, enter "Other" agency code or clearance code, as appropriate, and "Don't know" or "Don't recall" under the "Other Agency" heading, below. If your response is "No," or you don't know or can't recall if you were investigated and cleared, check the "No" box.</p>			

<b>Codes for Investigating Agency</b> 1 - Defense Department 2 - State Department 3 - Office of Personnel Management 4 - FBI 5 - Treasury Department 6 - Other (Specify)	<b>Codes for Security Clearance Received</b> 0 - Not Required 1 - Confidential 2 - Secret 3 - Top Secret 4 - Sensitive Compartmented Information 5 - Q 6 - L 7 - Other
--	--

Month/Year	Agency Code	Other Agency	Clearance Code	Month/Year	Agency Code	Other Agency	Clearance Code

<b>b</b>	To your knowledge, have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment? If "Yes," give date of action and agency. <b>Note:</b> An administrative downgrade or termination of a security clearance is not a revocation.	<b>Yes</b>	<b>No</b>

Month/Year	Department or Agency Taking Action	Month/Year	Department or Agency Taking Action

<b>27</b>	<b>YOUR FINANCIAL RECORD</b>	<b>Yes</b>	<b>No</b>
<p><b>a</b> In the last 7 years, have you filed a petition under any chapter of the bankruptcy code (to include Chapter 13)?</p> <p><b>b</b> In the last 7 years, have you had your wages garnished or had any property repossessed for any reason?</p> <p><b>c</b> In the last 7 years, have you had a lien placed against your property for failing to pay taxes or other debts?</p> <p><b>d</b> In the last 7 years, have you had any judgments against you that have not been paid?</p>			

If you answered "Yes" to a, b, c, or d, provide the information requested below:

Month/Year	Type of Action	Amount	Name Action Occurred Under	Name/Address of Court or Agency Handling Case	State	ZIP Code

Enter your Social Security Number before going to the next page →



# UNITED STATES OF AMERICA

## AUTHORIZATION FOR RELEASE OF INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

**I Authorize** any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a security clearance.

**I Understand** that, for financial or lending institutions, medical institutions, hospitals, health care professionals, and other sources of information, a separate specific release will be needed, and I may be contacted for such a release at a later date. Where a separate release is requested for information relating to mental health treatment or counseling, the release will contain a list of the specific questions, relevant to the job description, which the doctor or therapist will be asked.

**I Further Authorize** any investigator, special agent, or other duly accredited representative of the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, the Defense Investigative Service, and any other authorized Federal agency, to request criminal record information about me from criminal justice agencies for the purpose of determining my eligibility for access to classified information and/or for assignment to, or retention in, a sensitive National Security position, in accordance with 5 U.S.C. 9101. I understand that I may request a copy of such records as may be available to me under the law.

**I Authorize** custodians of records and other sources of information pertaining to me to release such information upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

**I Understand** that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 86, and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for five (5) years from the date signed or upon the termination of my affiliation with the Federal Government, whichever is sooner. Read, sign and date the release on the next page if you answered "Yes" to question 21.

Signature ( <i>Sign in ink</i> )		Full Name ( <i>Type or Print Legibly</i> )		Date Signed
Other Names Used			Social Security Number	
Current Address ( <i>Street, City</i> )		State	ZIP Code	Home Telephone Number ( <i>Include Area Code</i> ) (      )

## UNITED STATES OF AMERICA

### AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

#### Instructions for Completing this Release

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position with the Federal government which requires access to classified national security information or special nuclear information or material. As part of the clearance process, I **hereby authorize** the investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgement or reliability, particularly in the context of safeguarding classified national security information or special nuclear information or material?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 86 and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

Signature <i>(Sign in ink)</i>	Full Name <i>(Type or Print Legibly)</i>	Date Signed
Other Names Used		Social Security Number
Current Address <i>(Street, City)</i>	State	ZIP Code
Home Telephone Number <i>(Include Area Code)</i> (      )		

<b>APPLICANT</b>	LEAVE BLANK	TYPE OR PRINT ALL INFORMATION IN BLACK						FBI	LEAVE BLANK
SIGNATURE OF PERSON FINGERPRINTED		LAST NAME <u>NAM</u>	FIRST NAME	MIDDLE NAME					
RESIDENCE OF PERSON FINGERPRINTED		ALIASES <u>AKA</u>	O R I					DATE OF BIRTH <u>DOB</u> Month Day Year	
DATE	SIGNATURE OF OFFICIAL TAKING FINGERPRINTS	CITIZENSHIP <u>CTZ</u>		SEX	RACE	HGT.	WGT.	EYES	HAIR
EMPLOYER AND ADDRESS		YOUR NO. <u>OCA</u>	LEAVE BLANK						
REASON FINGERPRINTED		FBI NO. <u>FBI</u>	CLASS _____						
		ARMED FORCES NO. <u>MNU</u>	REF. _____						
		SOCIAL SECURITY NO. <u>SOC</u>							
		MISCELLANEOUS NO. <u>MNU</u>							

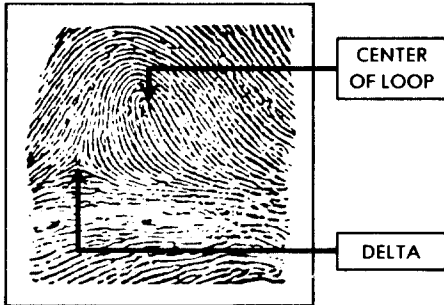
1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING	5. R. LITTLE	
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING	10. L. LITTLE	
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L. THUMB	R. THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY	

FEDERAL BUREAU OF INVESTIGATION  
UNITED STATES DEPARTMENT OF JUSTICE

WASHINGTON, D.C. 20537

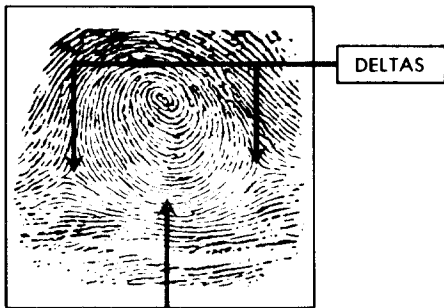
APPLICANT

1. LOOP



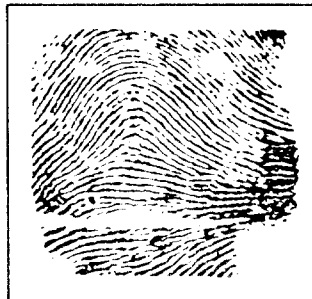
THE LINES BETWEEN CENTER OF LOOP AND DELTA MUST SHOW

2. WHORL



THESE LINES RUNNING BETWEEN DELTAS MUST BE CLEAR

3. ARCH



ARCHES HAVE NO DELTAS

TO OBTAIN CLASSIFIABLE FINGERPRINTS:

1. WASH AND DRY FINGERS THOROUGHLY.
2. ROLL FINGERS FROM NAIL TO NAIL, AND AVOID ALLOWING FINGERS TO SLIP.
3. BE SURE IMPRESSIONS ARE RECORDED IN CORRECT ORDER.
4. IF AN AMPUTATION OR DEFORMITY MAKES IT IMPOSSIBLE TO PRINT A FINGER, MAKE A NOTATION TO THAT EFFECT IN THE INDIVIDUAL FINGER BLOCK.
5. IF SOME PHYSICAL CONDITION MAKES IT IMPOSSIBLE TO OBTAIN PERFECT IMPRESSIONS, SUBMIT THE BEST THAT CAN BE OBTAINED WITH A MEMO STAPLED TO THE CARD EXPLAINING THE CIRCUMSTANCES.
6. EXAMINE THE COMPLETED PRINTS TO SEE IF THEY CAN BE CLASSIFIED, BEARING IN MIND THAT MOST FINGERPRINTS FALL INTO THE PATTERNS SHOWN ON THIS CARD (OTHER PATTERNS OCCUR INFREQUENTLY AND ARE NOT SHOWN HERE).

THIS CARD FOR USE BY:

LEAVE THIS SPACE BLANK

1. LAW ENFORCEMENT AGENCIES IN FINGERPRINTING APPLICANTS FOR LAW ENFORCEMENT POSITIONS.\*
2. OFFICIALS OF STATE AND LOCAL GOVERNMENTS FOR PURPOSES OF EMPLOYMENT, LICENSING AND PERMITS, AS AUTHORIZED BY STATE STATUTES AND APPROVED BY THE ATTORNEY GENERAL OF THE UNITED STATES. LOCAL AND COUNTY ORDINANCES, UNLESS SPECIFICALLY BASED ON APPLICABLE STATE STATUTES DO NOT SATISFY THIS REQUIREMENT.\*
3. U.S. GOVERNMENT AGENCIES AND OTHER ENTITIES REQUIRED BY FEDERAL LAW.\*\*
4. OFFICIALS OF FEDERALLY CHARTERED OR INSURED BANKING INSTITUTIONS TO PROMOTE OR MAINTAIN THE SECURITY OF THOSE INSTITUTIONS.

INSTRUCTIONS:

- \*1. PRINTS MUST FIRST BE CHECKED THROUGH THE APPROPRIATE STATE IDENTIFICATION BUREAU, AND ONLY THOSE FINGERPRINTS FOR WHICH NO DISQUALIFYING RECORD HAS BEEN FOUND LOCALLY SHOULD BE SUBMITTED FOR FBI SEARCH.
  2. PRIVACY ACT OF 1974 (P.L. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY NUMBER IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.
  - \*\*3. IDENTITY OF PRIVATE CONTRACTORS SHOULD BE SHOWN IN SPACE "EMPLOYER AND ADDRESS". THE CONTRIBUTOR IS THE NAME OF THE AGENCY SUBMITTING THE FINGERPRINT CARD TO THE FBI.
  4. FBI NUMBER, IF KNOWN, SHOULD ALWAYS BE FURNISHED IN THE APPROPRIATE SPACE.
- MISCELLANEOUS NO. (M); RECORD; OTHER ARMED FORCES NO. (OAF); PASSPORT NO. (PP); ALIEN REGISTRATION NO. (AR); PORT SECURITY CARD NO. (PS); SELECTIVE SERVICE NO. (SS); VETERANS' ADMINISTRATION CLAIM NO. (VA)



4951 Gleason Avenue, Manassas, VA 20108  
(703) 305-8181 FAX (703) 578-1910

Equivalent to FBI FD-258

**CHECKLIST #4****PROCEDURES FOR TERMINATING  
CONTRACTOR  
ACCESS TO TSCA CBI**

Yes \_\_\_\_\_/No \_\_\_\_\_

**Has the Contractor DCO completed an inventory of all TSCA CBI materials that the CBITS system show as being at the contractor's facility?**

Yes \_\_\_\_\_/No \_\_\_\_\_

**Has the Contractor DCO provided a written inventory to their EPA Project Officer within 30 days.**

Yes \_\_\_\_\_/No \_\_\_\_\_

**Has the Contractor DCO collected all TSCA CBI materials and document control materials (logs & cover sheets) that are in the company's possession?**

Yes \_\_\_\_\_/No \_\_\_\_\_

**Has the Contractor transferred these materials to the TSCA CBI cleared EPA Project Officer (or other cleared official, i.e. DOPO, WAM) within 30 days?**

Yes \_\_\_\_\_/No \_\_\_\_\_

**Has the EPA Project Officer provided a copy of this written inventory to the OPPT DCO and the TSCA Security Staff?**

Yes \_\_\_\_\_/No \_\_\_\_\_

**Has the EPA PO forwarded the reconciled documents to the OPPT DCO within 30 days for inclusion into the official Agency File?**

Please read Privacy Act Statement on reverse before completing this form.



United States Environmental Protection Agency  
Washington, DC 20460

## Confidentiality Agreement for Contractor Employees Upon Relinquishing TSCA CBI Access Authority

Name of Employer

Contractor

Subcontractor

Contract Number

As an employee of the contractor/subcontractor named above performing work for the United States, I have been authorized access to confidential business information (CBI) submitted under the Toxic Substances Control Act (TSCA) (15 USC Section 2601 *et seq.*). This access authority was granted to me in order to perform my work under the contract number cited above.

I understand that TSCA CBI to which I have had access under the contract may be used only for the purposes of performing the contract. I also understand that TSCA CBI may not be disclosed except as authorized by TSCA or EPA regulation.

I certify that I have returned all copies of TSCA CBI materials in my possession to either the appropriate document control officer specified in the EPA-approved security plan in effect at my company or an EPA TSCA document control officer.

I agree that I will not remove any copies of materials containing TSCA CBI from the premises of my company or from EPA premises upon my relinquishment of TSCA CBI access authority. I further agree that I will not disclose any TSCA CBI to any person after my relinquishment of TSCA CBI access authority.

I understand that as a contractor employee who has been authorized access to TSCA CBI, under Section 14(d) of TSCA (15 USC 2613(d)) I am liable for a possible fine of up to \$5,000 and/or imprisonment for up to one year if I willfully disclose TSCA CBI to any person.

If I am still employed by the contractor, I also understand that I may be subject to disciplinary action for violation of this agreement.

I am aware that I may be subject to criminal penalties under 18 USC Section 1001 if I have made any statement of material facts knowing that such statement is false or I willfully conceal any material fact.

Name (Please type or print)

Social Security Number

Signature

Date





United States Environmental Protection Agency  
**Federal Agency, Congress, and Federal Court Sign Out Log**  
TSCA Confidential Business Information

May be TSCA CBI  
When Filled In

Does not contain National  
Security Information (E.O. 12065)

Date Logged Out	Document Control Number/ Copy Number	Number of Pages	Description	Federal Agency, Congress, or Court	Recipient	DCO Initial	Receipt	Date Returned	DCO Initial

EPA Form 7740-24 (10/92) Replaces EPA Form 7710-13 which is obsolete.

Stamp to Use when Material  
contains TSCA CBI

**TSCA CONFIDENTIAL  
BUSINESS INFORMATION  
— DOES NOT CONTAIN NATIONAL —  
SECURITY INFORMATION (E.O. 12065)**

Stamp to Use when Material  
contains No TSCA CBI

**CONTAINS NO CBI**

Enter Document Control Number or  
Bar Code

United States Environmental Protection Agency  
Washington, D.C. 20460

Document Description

Date

# CONFIDENTIAL

TOXIC SUBSTANCES CONTROL ACT  
CONFIDENTIAL BUSINESS INFORMATION


Does not contain National Security Information (E.O. 12065)

The attached document contains Confidential Business Information obtained under the Toxic Substances Control Act (TSCA 15 U.S.C. 2601 et seq.) TSCA Confidential Business Information may not be disclosed further or copied by you except as authorized in the procedures set forth in the TSCA Confidential Business Information Protection Manual.

If you willfully disclose TSCA Confidential Business Information to any person not authorized to receive it, you may be liable under section 14(d) of TSCA (15 U.S.C. 2613(d) for a possible fine up to \$5,000 and/or imprisonment for up to one year. In addition, disclosure of TSCA Confidential Business Information or violation of the procedures cited above may subject you to disciplinary action with penalties ranging up to and including dismissal.

If you are not authorized for TSCA confidential business information (CBI) access, do not look at this document. If you find this document, place it in a sealed envelope or other secure container and immediately give it to your supervisor or a TSCA CBI Document Control Officer for safekeeping and safe return.

EPA Form 7740-9 (rev. 10-03) Previous edition is obsolete

		United States Environmental Protection Agency			Does not contain National Security Information (E.O. 12065)				
		Inventory Log			TSCA Confidential Business Information				
Date Checked Out	Document Control Number/ Copy Number	User Information		Date Returned	DCO Initial	Disposition	Audit		
		EPA ID Number	User's Name						



United States Environmental Protection Agency  
Washington, DC 20460



TSCA CBI Visitors Log

Individual's Name	Organization	Date	Time	Purpose of Visit

United States Environmental Protection Agency  
Washington, DC 20460



## Permanent Transfer Receipt for TSCA Confidential Business Information

I acknowledge receipt of the following documents containing  
TSCA Confidential Business Information.

1. DCN/Copy Number	Description
2. DCN/Copy Number	Description
3. DCN/Copy Number	Description
4. DCN/Copy Number	Description
5. DCN/Copy Number	Description
6. DCN/Copy Number	Description
7. DCN/Copy Number	Description
8. DCN/Copy Number	Description
Date of transfer	Name of Sending DCO/DCA
Name of Recipient	Signature of Recipient DCO/DCA

### INSTRUCTIONS

1. To be used only for permanent transfer of TSCA CBI. Transfers must be made by a DCO/DCA.

2. The sending DCO/DCA must keep the original of this form after it has been signed and returned by the recipient DCO/DCA. The Recipient DCO/DCA must keep a copy of the receipt after returning the original to the sending DCO/DCA.

United States Environmental Protection Agency  
Washington, DC 20460 **EPA Memorandum of TSCA CBI Telephone Conversation****I. EPA Employee Identification**


Name of Employee	Date
Organization	Time

**II. Second Party Identification**

Call Is: <input type="checkbox"/> To <input type="checkbox"/> From	Name
Number	Organization

**III. Concerning what TSCA CBI?****IV. Content**



United States Environmental Protection Agency Washington, DC 20460	
 <b>EPA Temporary Loan Receipt for TSCA Confidential Business Information</b>	
I acknowledge receipt of the following documents containing TSCA Confidential Business Information.	
1. DCN/Copy Number	Description
2. DCN/Copy Number	Description
3. DCN/Copy Number	Description
4. DCN/Copy Number	Description
5. DCN/Copy Number	Description
6. DCN/Copy Number	Description
7. DCN/Copy Number	Description
Date Loaned	Name of Lender
Name of Recipient	Signature of Recipient
<b>Instructions</b>	
<p>1. To be used only for temporary transfer of TSCA CBI. Transfers for more than thirty (30) days must be made through a DCO.</p> <p>2. The lender must keep the original of this form after it has been completed and signed by the recipient, and give the copy to the recipient.</p> <p>3. The lender must give his or her copy of this form to the recipient when the recipient returns the document(s) to the lender. The recipient should destroy both copies.</p>	

***LAPTOP COMPUTER USER AGREEMENT FOR THE CONFIDENTIAL  
BUSINESS INFORMATION CENTER (CBIC)***

**In order to use a laptop in the CBIC, you must read and sign the following user agreement. If you do not sign the agreement, your laptop will have to be secured during your visit to the CBIC. By signing this user agreement, you certify that you are cleared to work with Toxic Substances Control Act (TSCA) confidential business information (CBI) and have read and understand the following rules regarding the use of laptops in the CBIC and agree to abide by these rules:**

1. As a user of TSCA CBI, I will ensure through personal conduct and accountability that I will act consistently with all guidelines established by EPA, contractors, or other Federal agencies to protect, to the best of my ability, all TSCA CBI, as defined in the TSCA Confidential Business Information Security Manual.
2. I understand that the TSCA Confidential Business Information Security Manual describes the Agency's policies and procedures for maintaining confidentiality of business information. If I have difficulty finding the proper guideline in a situation involving CBI, I will consult my Document Control Officer or OPPT's TSCA Security Staff. I will treat the Security Manual as a reference guide for protecting confidential business information, especially with regards to the handling of working papers. I am familiar with the procedures that I am required to frequently use.
3. I will retain exclusive control over the operation of this laptop. I understand that it is my responsibility to ensure that a laptop with CBI data is properly secured.
4. I understand that diskettes and detachable hard disks are required for storage of TSCA CBI data and that I should erase the CBI data from the fixed hard disk, if necessary, using an approved program, before the laptop can be used by a person who is not cleared to work with CBI.
6. I will not use E-mail to send or receive CBI.
7. I will make sure that no one can see any CBI that may be on the laptop screen.
8. I will report any potential disclosures of CBI to my supervisor and the TSCA Security Staff.
9. I will ensure that when using word processing programs on the laptop, the default save feature will be set to save data to the A drive and not the C drive.

Name (please print) \_\_\_\_\_

Company name (please print) \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

**TSCA CBI Protection Manual**  
Appendix CC

---

**CONFIDENTIAL COMMUNICATION**

BY CERTIFIED MAIL: RETURN RECEIPT REQUESTED

Company Address

Dear \_\_\_\_\_,

I am writing to acknowledge your telephone conversation with \_\_\_\_\_ of my office on \_\_\_\_\_ in which you discussed [Company's] claim of confidentiality with respect to information contained within its submission of the TSCA section \_\_\_\_\_ referenced above. I understand from this discussion that [Company] wishes to voluntarily withdraw its claim of confidentiality to the following information, thereby consenting to its immediate public release:

[List numerically the items of information the company has agreed to release]

On behalf of [Company], please confirm that you consent to the above by signing and dating the Agreement on page two of this letter, and returning the original to \_\_\_\_\_ at your earliest convenience.

Please feel free to contact \_\_\_\_\_ at (202) 564-\_\_\_\_\_ if you wish to discuss this matter further. Thank you for your cooperation in the public release of this important (health and safety) information.

Sincerely,

\_\_\_\_\_  
Director  
\_\_\_\_\_  
Division  
Office of Pollution Prevention and Toxics

TSCA CBI Protection Manual  
Appendix DD

---

**40 CFR 2.208**

Substantive criteria for use in confidentiality determinations. Determinations issued under Secs. 2.204 through 2.207 shall hold that business information is entitled to confidential treatment for the benefit of a particular business if--

(a) The business has asserted a business confidentiality claim which has not expired by its terms, nor been waived nor withdrawn;

(b) The business has satisfactorily shown that it has taken reasonable measures to protect the confidentiality of the information, and that it intends to continue to take such measures;

(c) The information is not, and has not been, reasonably obtainable without the business's consent by other persons (other than governmental bodies) by use of legitimate means (other than discovery based on a showing of special need in a judicial or quasi-judicial proceeding);

(d) No statute specifically requires disclosure of the information; and

(e) Either--

(1) The business has satisfactorily shown that disclosure of the information is likely to cause substantial harm to the business's competitive position; or

(2) The information is voluntarily submitted information (see Sec. 2.201(i)), and its disclosure would be likely to impair the Government's ability to obtain necessary information in the future.

**Taking action on TSCA CBI claims that appear unwarranted.**

Under section 4.1.5, any employee who discovers a TSCA CBI claim that appears unwarranted may exercise independent discretion in choosing whether to refer the matter to IMD, or communicate with the submitter. Employees should follow these guidelines:

1. Communicate directly with the submitter. These communications are informal only. Formal actions (other than sending out the request for substantiation in accordance with 40 CFR 2.204(e)) are taken by OGC, except under bullet 4, below. In these informal communications, employee should perform the following tasks:
  - (i) Record the statements and substance of the discussion with the submitter or its representative, including the name and position of the person(s) contacted. Immediately attach notes of the discussion to the claim file.
  - (ii) If the submitter agrees to amend its submission by withdrawing its claim, send the submitter a short letter via regular mail, recounting the conversation and the submitter's agreement to voluntarily amend its claim, and a request that it sign and return to EPA the "Amendment through Voluntary Withdrawal" statement. (see APPENDIX CC).
  - (iii) Notify IMD if the submitter does not amend its claim.
2. EPA employees are permitted to conduct informal inquiries for TSCA CBI claims consistent with 40 CFR 2.204. When an EPA program office believes it appropriate, it can request substantiation of a TSCA CBI claim directly from a submitter. The request should be made in writing, or by telephone with an immediate follow-up written communication. The EPA program office making contact must instruct the submitter to reply in writing. A written request for substantiation issued by a program office must be made in consultation with IMD or OGC, and must be consistent with the requirements of 40 CFR part 2, subpart B, and the Paperwork Reduction Act.
3. Federal employees and EPA program offices, especially Compliance Inspectors, are encouraged to obtain guidance from IMD on CBI reviews. In addition, employees are encouraged to become familiar with the substantive criteria used to determine confidentiality, found in 40 CFR 2.208 [See Appendix DD].
4. The Office of General Counsel (OGC) makes the final determinations concerning eligibility for confidential treatment, pursuant to 40 CFR 2.205. However, an EPA office may deny the claim if it determines that the information claimed as TSCA CBI is clearly not entitled to confidential treatment. Such denials are rare, and should not occur without first consulting with IMD, who may in turn consult with OGC.
5. Follow Regulatory procedures in contacting a submitter regarding the validity of a CBI claim. It is necessary to act consistently with all confidentiality regulations, particularly 40 CFR part 2, subpart B; and relevant *Federal Register* notices. IMD or OGC attorneys should be consulted if any problems arise on TSCA CBI issues.