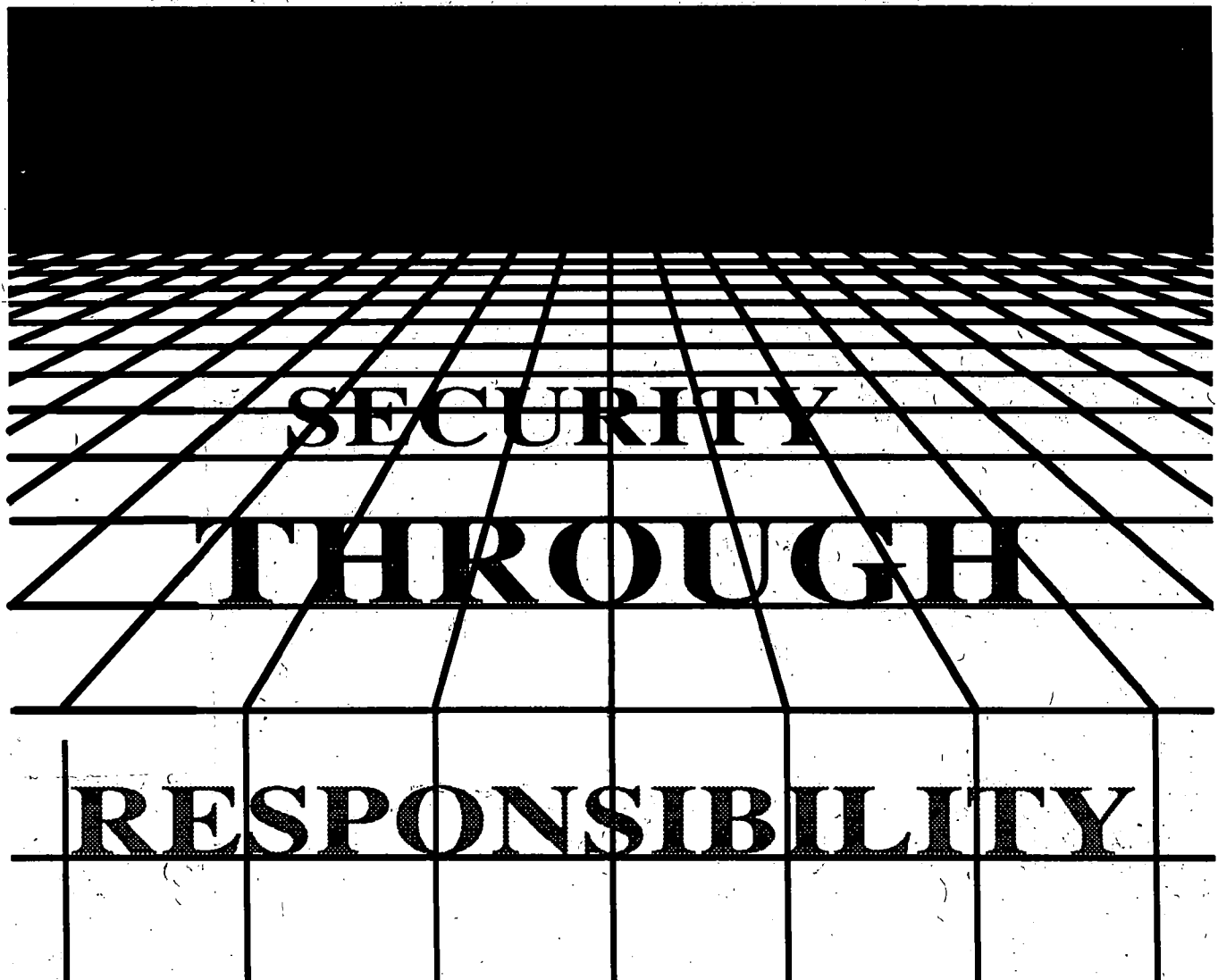




# **TSCA Confidential Business Information Security Manual**



## TABLE OF CONTENTS

LIST OF APPENDICES .....	i
CONTACTS .....	iii
GLOSSARY OF ACRONYMS .....	v
BACKGROUND ON TERMINOLOGY AND EPA OFFICES .....	vii
<b>CHAPTER 1</b>	
<b>INTRODUCTION</b> .....	1
A.    GUIDING PRINCIPLES FOR SITUATIONS OUTSIDE OF THE MANUAL .....	1
B.    MANUAL UPDATES AND REVISIONS TO PROCEDURES .....	2
<b>CHAPTER 2</b>	
<b>HOW TO AUTHORIZE FEDERAL EMPLOYEES, CONTRACT     EMPLOYEES AND CONGRESS FOR ACCESS TO TSCA CBI</b> .....	3
A.    STEPS TO TSCA CBI ACCESS FOR EPA EMPLOYEES .....	4
1.    AUTHORIZING ACCESS .....	4
a.    Completing and submitting the forms .....	4
b.    Forms required to obtain computer access to TSCA CBI data .....	4
c.    Individual access files .....	4
d.    Security briefing .....	5
e.    Approval for TSCA CBI access or waiver for immediate access .....	5
f.    TSCA CBI authorized access list .....	5



2.	REQUIREMENTS FOR MAINTAINING ACCESS . . . . .	6
a.	General information . . . . .	6
b.	Document audit procedure . . . . .	6
c.	Scheduling an annual security briefing . . . . .	6
d.	Failure to reconcile document audit report or attend annual security briefing . . . . .	6
e.	Effect of suspension of access . . . . .	7
f.	Reapplying for TSCA CBI access . . . . .	7
g.	Employee transfers within EPA . . . . .	7
B.	STEPS TO TERMINATING TSCA CBI ACCESS FOR EPA EMPLOYEES . . . . .	7
1.	GENERAL INFORMATION . . . . .	7
2.	REQUIREMENTS FOR TERMINATING ACCESS . . . . .	8
a.	Form 7740-16 . . . . .	8
b.	Document audit procedure . . . . .	8
c.	DCO responsibilities after document audit is completed . . . . .	8
d.	Missing documents . . . . .	9
e.	Employee responsibilities . . . . .	9
C.	STEPS TO TSCA CBI ACCESS FOR CONTRACTORS AND SUBCONTRACTORS . . . . .	10
	AUTHORIZING ACCESS . . . . .	10
1.	Determining whether access to TSCA CBI is necessary . . . . .	10
2.	Secure environment for handling and storing TSCA CBI . . . . .	10
3.	Site inspection . . . . .	11
4.	Required contract language . . . . .	11
5.	Notice to affected businesses . . . . .	11
6.	Facility DCO at the contractor's site . . . . .	12
7.	How to assign a DCO . . . . .	13
8.	Identifying contractor employees for clearance . . . . .	13

D.	HOW TO OBTAIN TSCA CBI AUTHORIZATION FOR EMPLOYEES OF CONTRACTORS AND SUBCONTRACTORS . . . . .	13
1.	AUTHORIZING ACCESS . . . . .	13
a.	Completing and submitting the forms . . . . .	13
b.	Minimum Background Investigation (MBI) . . . . .	14
c.	Individual Access Files . . . . .	14
d.	Security briefing . . . . .	15
e.	Approval for TSCA CBI access or waiver for immediate access . . . . .	15
f.	TSCA CBI authorized access list . . . . .	15
2.	REQUIREMENTS FOR MAINTAINING ACCESS . . . . .	16
a.	General information . . . . .	16
b.	Document audit procedure . . . . .	16
c.	Scheduling an annual security briefing . . . . .	16
d.	Failure to attend an annual security briefing . . . . .	16
e.	Reapplying for TSCA CBI access . . . . .	17
E.	PROCEDURES FOR TERMINATING ACCESS TO TSCA CBI FOR CONTRACTOR EMPLOYEES . . . . .	17
1.	GENERAL INFORMATION . . . . .	17
2.	REQUIREMENTS FOR TERMINATING ACCESS . . . . .	18
a.	Form 7740-18 . . . . .	18
b.	Document audit procedure . . . . .	18
c.	Missing documents . . . . .	18
d.	DCO responsibilities after document audit is completed . . . . .	19
e.	Contractor employee responsibilities . . . . .	19
F.	PROCEDURES FOR TERMINATING ACCESS TO TSCA CBI FOR CONTRACTORS . . . . .	19
	TERMINATING ACCESS TO TSCA CBI WHEN A CONTRACT ENDS . . . . .	19

G.	AUTHORIZING OTHER FEDERAL AGENCIES FOR ACCESS TO TSCA CBI .....	20
1.	GENERAL PROCEDURES FOR EPA OFFICES TO DISCLOSE TSCA CBI TO ANOTHER FEDERAL AGENCY PERFORMING WORK FOR EPA .....	20
a.	Agreement not to disclose TSCA CBI .....	21
b.	Exceptions to agreement .....	21
c.	TSCA CBI access at EPA facilities .....	21
d.	TSCA CBI access at other Federal agencies .....	21
e.	How to assign a DCO .....	21
2.	PROCEDURES FOR ANOTHER FEDERAL AGENCY TO REQUEST ACCESS TO TSCA CBI .....	22
a.	Submit a written request .....	22
b.	Agreement not to disclose TSCA CBI .....	22
c.	Exceptions to agreement .....	22
d.	Notice to affected businesses .....	23
3.	EPA'S PROCESS FOR APPROVING TSCA CBI ACCESS FOR OTHER FEDERAL AGENCIES .....	23
a.	TSCA CBI access at EPA facilities .....	24
b.	TSCA CBI access at other Federal agencies .....	24
4.	REQUESTS FOR ACCESS TO TSCA CBI FROM CONGRESS OR THE GENERAL ACCOUNTING OFFICE .....	25
	Notice to affected businesses .....	25

### CHAPTER 3 RESPONSIBILITIES .....

A.	EMPLOYEE RESPONSIBILITIES .....	27
1.	EPA HOLDS EMPLOYEES PERSONALLY ACCOUNTABLE FOR PROTECTING TSCA CBI .....	27
2.	DOCUMENT AUDIT PROCEDURES .....	28

3.	CHECKING OUT TSCA CBI DOCUMENTS . . . . .	28
	Overdue materials . . . . .	28
4.	DETERMINING WHETHER A DOCUMENT CONTAINS TSCA CBI . . . . .	28
5.	RECEIPT OF MAIL CONTAINING TSCA CBI MATERIAL . . .	29
6.	CHALLENGING TSCA CBI CLAIMS DURING AND AFTER INSPECTIONS . . . . .	29
	a. Informal inquiries . . . . .	29
	b. Formal challenges . . . . .	30
	c. Procedure when performing . . . . .	30
B.	MANAGER RESPONSIBILITIES . . . . .	30
	IN GENERAL . . . . .	30
C.	DOCUMENT CONTROL OFFICER (DCO) RESPONSIBILITIES . . . . .	31
	1. IN GENERAL . . . . .	31
	2. MAINTAINING A DOCUMENT TRACKING SYSTEM . . . . .	31
	a. Automated document tracking systems . . . . .	32
	b. Manual tracking systems . . . . .	33
	3. MAINTAINING THE INVENTORY LOG . . . . .	34
	4. DELIVERING AND RECEIVING TSCA CBI MATERIALS . . . . .	34
	a. Reviewing documents for completeness . . . . .	34
	b. Maintaining a receipt log . . . . .	35
	5. STORAGE OF TSCA CBI MATERIALS . . . . .	35
	6. MAINTAINING RECORDS OF LOCK COMBINATIONS . . . . .	36
	7. CONDITIONS FOR CHANGING LOCK COMBINATIONS . . . . .	36
	8. UPDATING THE TSCA CBI AUTHORIZED ACCESS LIST . . . . .	37
	9. MONITORING AND CONTROLLING WHO OBTAINS TSCA CBI MATERIALS . . . . .	37
	10. MONITORING OVERDUE TSCA CBI MATERIALS . . . . .	37
	11. ASSISTING EMPLOYEES IN DETERMINING WHETHER DOCUMENTS CONTAIN TSCA CBI AND IN SANITIZING DOCUMENTS FOR PUBLIC DISCLOSURE . . . . .	38

12.	SUPERVISING THE REPRODUCTION AND DESTRUCTION OF TSCA CBI MATERIALS .....	38
13.	CONTROLLING THE TRANSFER OF TSCA CBI MATERIALS BETWEEN FACILITIES .....	38
	Packaging and Arranging Transfer of TSCA CBI Material .....	39
14.	ASSISTING EMPLOYEES WITH OBTAINING AND MAINTAINING TSCA CBI ACCESS AUTHORITY .....	39
15.	ASSISTING EMPLOYEE DOCUMENT AUDITS .....	39
16.	PERFORMING AN INVENTORY OF HARD-COPY TSCA CBI DOCUMENTS .....	39
17.	WHEN DCOS TERMINATE THEIR EMPLOYMENT OR RELINQUISH THEIR DCO RESPONSIBILITIES .....	40

#### CHAPTER 4

##### PROCEDURES FOR USING AND PROTECTING TSCA CBI MATERIALS ... 43

###### A. MARKING MATERIALS AS TSCA CBI ..... 43

1. TSCA CBI COVER SHEETS ..... 43
2. TSCA CBI STAMP ..... 43

###### B. PROCEDURES FOR USING TSCA CBI DOCUMENTS INSIDE OR OUTSIDE OF SECURE STORAGE AREAS ..... 43

1. EMPLOYEE RESPONSIBILITIES, IN GENERAL ..... 43
2. PROCEDURES FOR USING TSCA CBI DOCUMENTS  
OUTSIDE OF SECURE STORAGE AREAS ..... 44
  - a. Two types of containers are approved ..... 44
  - b. Open/close signs ..... 44
  - c. More than one person can use a storage  
container ..... 44
3. PROCEDURES FOR USING TSCA CBI DOCUMENTS  
INSIDE SECURE STORAGE AREAS ..... 45

Unauthorized persons inside secure storage areas ..... 45

C.	HOW TO OBTAIN APPROVAL FOR ESTABLISHING A SECURE STORAGE AREA .....	45
D.	SECURING AN AREA .....	46
	SECURE STORAGE AREA REQUIREMENTS .....	46
	1. Maintaining security of lock combinations .....	46
	2. Electronic card keys .....	46
E.	PROCEDURES FOR OBTAINING TSCA CBI .....	47
	1. HOW TO OBTAIN TSCA CBI FROM THE CBIC OR OTHER CENTRALIZED STORAGE FACILITY .....	47
	a. Safeguarding TSCA CBI documents .....	47
	b. Obtaining a receipt for returned documents .....	48
	c. Transferring TSCA CBI materials between a DCO and people under his or her supervision in a centralized secure storage area .....	48
	2. HOW TO OBTAIN TSCA CBI FROM ANOTHER EMPLOYEE WITHIN THE SAME FACILITY .....	48
	Keeping records on transfers .....	49
F.	PROCEDURES FOR TRANSFERRING TSCA CBI TO ANOTHER FACILITY .....	49
	1. IN GENERAL .....	49
	2. PROCEDURES FOR TRANSFERRING TSCA CBI MATERIALS .....	49
	a. Procedures for sending or receiving TSCA CBI materials through the U.S. Postal Service .....	50
	b. Procedures for hand delivery of TSCA CBI materials .....	50
	c. Procedures for transmitting TSCA CBI materials by courier or U.S. Postal Service Express Mail .....	51



G.	PROCEDURES FOR RECEIVING AND SENDING FACSIMILES (FAXES) THAT CONTAIN TSCA CBI	52
1.	PROCEDURES FOR SENDING OR RECEIVING FAXES BETWEEN PERSONS AUTHORIZED FOR ACCESS TO TSCA CBI	52
2.	WHEN INDUSTRY OFFICIALS OR INDUSTRY SUBMITTERS REQUEST THAT TSCA CBI BE FAXED TO THEM	53
3.	WHEN AN INDUSTRY OFFICIAL OR INDUSTRY SUBMITTER ASKS TO FAX TSCA CBI TO EPA	53
4.	WHEN INDUSTRY REQUESTS EPA TO FAX TSCA CBI TO FROM EPA TO THEIR LOCATION	54
H.	DISCUSSING TSCA CBI ON THE TELEPHONE	54
1.	TELEPHONE CALLS WITH PERSONS AUTHORIZED FOR TSCA CBI ACCESS	54
2.	TELEPHONE CALLS WITH SUBMITTERS	54
	Telephone Logs	55
3.	VOICE MAIL CANNOT BE USED TO TRANSMIT TSCA CBI	55
I.	ELECTRONIC MAIL CANNOT BE USED TO TRANSMIT TSCA CBI	55
J.	USE OF TSCA CBI AT TELE-VIDEO CONFERENCES	55
K.	PROCEDURES FOR HANDLING DOCUMENTS AND OTHER MATERIALS PRODUCED BY EMPLOYEES USING TSCA CBI DOCUMENTS	56
1.	NEW TSCA CBI DOCUMENTS	56
2.	NEW NON-CONFIDENTIAL DOCUMENTS	56
3.	PERSONAL WORKING PAPERS	57
a.	Transferring personal working papers to another employee	57
b.	Keeping records on transfers	57
c.	Photocopying personal working papers	57

d.	Transferring personal working papers to a typist . . . . .	57
e.	Procedures for storing personal working papers . . . . .	58
f.	Procedures for destroying personal working papers . . . . .	58
L.	CREATING NON-CONFIDENTIAL MATERIALS FROM TSCA CBI DOCUMENTS . . . . .	58
1.	IN GENERAL . . . . .	58
2.	NON-CONFIDENTIAL DOCUMENTS . . . . .	59
a.	When TSCA CBI data are replaced with non-confidential data or descriptive terms . . . . .	59
b.	When a submitting company drops its claim of confidentiality . . . . .	59
M.	PROCESS FOR DECLASSIFYING TSCA CBI MATERIALS . . . . .	59
	HOW TO DECLASSIFY TSCA CBI MATERIALS . . . . .	59
N.	REPRODUCTION OF TSCA CBI MATERIALS . . . . .	60
1.	IN GENERAL . . . . .	60
2.	EMPLOYEE'S ROLE . . . . .	60
3.	DCO RESPONSIBILITIES . . . . .	61
a.	Control of copies . . . . .	61
b.	Distributing copies to other employees . . . . .	61
c.	Authorizing use of other photocopying machines when machines in secure locations break down . . . . .	61
O.	PROCEDURES FOR DESTROYING TSCA CBI MATERIALS . . . . .	62
1.	IN GENERAL . . . . .	62
2.	WHO IS PERMITTED TO DESTROY TSCA CBI MATERIALS . . . . .	62

a.	EPA and Federal employees .....	62
b.	Contractor employees .....	62
3.	DESTRUCTION METHODS .....	62
4.	DOCUMENTING DESTRUCTION .....	63
P.	USE OR DISCUSSION OF TSCA CBI DURING MEETINGS .....	63
1.	WHAT IS CONSIDERED A MEETING? .....	63
2.	PROCEDURES FOR CIRCULATING DOCUMENT COPIES AT A MEETING .....	63
a.	Personal working papers .....	63
b.	Documents that have been logged out to an employee .....	64
3.	PROCEDURES FOR DISCUSSING TSCA CBI DURING MEETINGS .....	65
a.	Meeting chairperson's duties .....	65
b.	Records of meeting containing CBI must be treated as TSCA CBI .....	65
Q.	TRAVELING WITH TSCA CBI MATERIALS .....	65
1.	IN GENERAL .....	65
2.	MAINTAINING SECURITY FOR TSCA CBI MATERIALS WHILE TRAVELING .....	66
a.	Storing TSCA CBI materials while traveling .....	66
b.	Transferring possession of TSCA CBI materials while traveling .....	66
R.	WORKING WITH TSCA CBI AT A PERSONAL RESIDENCE .....	66
S.	WORKING WITH TSCA CBI MATERIALS ON COMPUTERS .....	67

1.	IN GENERAL .....	67
2.	SETTING UP A LOCAL-AREA NETWORK (LAN) .....	67
3.	USING PERSONAL COMPUTERS (PCS) TO WORK WITH TSCA CBI DATA .....	67
a.	Procedures for using TSCA CBI data on a PC outside of a secure storage area .....	67
b.	Processing and storing TSCA CBI data on floppy and hard disks .....	67
c.	Maintaining security for floppy and detachable hard diskettes containing TSCA CBI data .....	68
d.	Terminating a TSCA CBI PC session for PCs located outside secure storage areas .....	68
e.	Security procedures for PC printouts of TSCA CBI data .....	69
4.	MINI COMPUTERS .....	69
	Security controls for TSCA CBI data on mini computers ..	69
5.	SECURITY FOR TSCA CBI DATA STORED ON CONTRACTOR'S COMPUTERS .....	70
T.	DEVELOPMENT OF PHOTOGRAPHIC MATERIALS .....	70
1.	PHOTOGRAPHS CAN BE CLAIMED AS TSCA CBI .....	70
2.	VIDEO TAPES CAN BE CLAIMED AS TSCA CBI .....	70

## CHAPTER 5

### REPORTING AND INVESTIGATION OF VIOLATIONS OF PROCEDURES, LOST DOCUMENTS, AND UNAUTHORIZED DISCLOSURES .....

71

A.	EMPLOYEE REPORTING PROCEDURES .....	71
1.	ORAL REPORT MUST BE MADE WITHIN ONE WORKING DAY .....	71
2.	WRITTEN REPORT MUST BE MADE WITHIN TWO WORKING DAYS .....	71

Employee's division director or project officer's duties . . . . .	72
B. REVIEW AND INVESTIGATION OF EMPLOYEE'S REPORT . . . . .	72
1. WHEN POSSIBLE VIOLATION OF THIS MANUAL'S SECURITY PROCEDURES HAS OCCURRED . . . . .	72
2. WHEN TSCA CBI MATERIALS CANNOT BE ACCOUNTED FOR . . . . .	73
Notification to the submitting company . . . . .	73
3. WHEN UNAUTHORIZED DISCLOSURE OF TSCA CBI MATERIALS MAY HAVE OCCURRED . . . . .	73
a. Notification to the submitting company . . . . .	73
b. EPA Office of Inspector General . . . . .	73
C. PENALTY GUIDELINES FOR VIOLATION OF THIS MANUAL'S PROCEDURES . . . . .	74
1. DETERMINING THAT A VIOLATION HAS OCCURRED . . . . .	74
2. DETERMINING AN APPROPRIATE REMEDY . . . . .	74
3. CORRECTIVE ACTIONS . . . . .	75
4. ADMINISTRATIVE PENALTIES . . . . .	76
5. CRIMINAL PENALTIES . . . . .	77
6. OPME DIRECTOR CAN ALSO RECOMMEND THAT NO ACTION BE TAKEN . . . . .	77

***LIST OF APPENDICES***

Appendix	Title
1	TSCA CBI Access Request, Agreement, and Approval
2	TSCA CBI ADP User Registration
3	Standard Form 86: Questionnaire for Sensitive Positions
4	Fingerprint Chart
5	Request for Building Pass
6	Request for Approval of Contractor Access to TSCA Confidential Business Information
7	Contractor Information Sheet
8	Procurement Policy Notice 93-07 dated August 1993
9	Confidentiality Agreement for United States Employees Upon Relinquishing TSCA CBI Access Authority
10	Confidentiality Agreement for Contractor Employees Upon Relinquishing TSCA CBI Access Authority
11	EPA Form 3110-1: Employee Separation or Transfer Checklist
12	TSCA CBI Stamp
13	TSCA CBI Cover Sheet
14	TSCA CBI Visitors Log

15	Receipt Log
16	Inventory Log
17	Temporary Loan Receipt for TSCA Confidential Business Information
18	Permanent Transfer Receipt for TSCA CBI.
19	Memorandum of TSCA CBI Telephone Conversation
20	Federal Agency, Congress, and Federal Court Sign-out Log
21	Revision Transmittal Sheet
22	Document Reconciliation/Annual Certification
23	Sample of TSCA CBI Labels
24	Project Officer Checklist

***CONTACTS***

Questions about the procedures in this manual should be directed to

- Chief, TSCA Information Management Branch  
Information Management Division  
Office of Pollution Prevention and Toxics (7407)  
Environmental Protection Agency  
401 M Street, S.W.  
Washington, D.C. 20460  
Phone: (202) 260-0425

Other sources for information are

- OPPT Document Control Officer  
Office of Pollution Prevention and Toxics (7407)  
Environmental Protection Agency  
401 M Street, S.W.  
Washington, D.C. 20460  
Phone: (202) 260-1532 Fax: (202) 260-9555
- TSCA Security Staff  
Office of Pollution Prevention and Toxics (7401)  
Environmental Protection Agency  
401 M Street, S.W.  
Washington, D.C. 20460  
Phone: (202) 260-6475
- Director  
Information Management Division  
Office of Pollution Prevention and Toxics (7407)  
Environmental Protection Agency  
401 M Street, S.W.  
Washington, D.C. 20460  
Phone: (202) 260-3938



- Director  
Office of Program Management and Evaluation  
Office of Pollution Prevention and Toxics (7401)  
Environmental Protection Agency  
401 M Street, S.W.  
Washington, D.C. 20460  
Phone: (202) 260-1761

***GLOSSARY OF ACRONYMS***

<b>ADTS</b>	<b>Automated Document Tracking System</b>
<b>CBI</b>	<b>Confidential Business Information</b>
<b>CBIC</b>	<b>Confidential Business Information Center</b>
<b>CBITS</b>	<b>Confidential Business Information Tracking System</b>
<b>CFR</b>	<b>Code of Federal Regulations</b>
<b>DCO</b>	<b>Document Control Officer</b>
<b>DCA</b>	<b>Document Control Assistant</b>
<b>EPA</b>	<b>United States Environmental Protection Agency</b>
<b>FAX</b>	<b>Facsimile Transmission</b>
<b>FMSD</b>	<b>Facilities Management and Services Division</b>
<b>FRC</b>	<b>Federal Records Center</b>
<b>IG</b>	<b>Inspector General</b>
<b>IMD</b>	<b>Information Management Division</b>
<b>LAN</b>	<b>Local-Area Network</b>
<b>MBI</b>	<b>Minimum Background Investigation</b>
<b>OAM</b>	<b>Office of Acquisition Management</b>
<b>OGC</b>	<b>Office of General Counsel</b>
<b>OPME</b>	<b>Office of Program Management and Evaluation</b>

OPPT	Office of Pollution Prevention and Toxics
OPPT DCO	Office of Pollution Prevention and Toxics Document Control Officer
PC	Personal Computer
PMN	Premanufacture Notification
PO	Project Officer
TIMB	TSCA Information Management Branch
TSCA	Toxic Substances Control Act

***BACKGROUND ON TERMINOLOGY AND EPA OFFICES***

**Authorized access list:** A list of people who are authorized for access to TSCA CBI.

**Contractors and subcontractors:** Individuals who perform work under a contract with the United States government.

**Document control assistants (DCAs):** The OPPT DCO and facility DCOs can nominate DCAs to assist them in performing document control functions. If a procedure in this manual requires that a document be taken to the DCO, the document may be taken to either the facility DCO or DCA.

**Employee document control officer (DCO):** At facilities where there are multiple facility DCOs, each DCO will be assigned responsibility for a number of individual employees. In this role, the facility DCO assists each employee in requesting and renewing TSCA CBI access authorization.

**EPA project officer:** An EPA employee who monitors the technical aspects of a contract that authorizes TSCA CBI access.

**Facility:** Any location where EPA, a government contractor, or another Federal agency stores and uses TSCA CBI. Different security procedures are required at facilities outside of EPA headquarters and at contractor sites; however, the same general procedures are in force at all facilities.

**Facility document control officer (DCO):** The facility DCO is responsible for managing the collection of records and document tracking system for the site where he or she is employed. The number of employees at a facility determines how many facility DCOs there are. For instance, about 30 facility DCOs are assigned to EPA headquarters. The facility DCO also has oversight authority for the receipt, storage, transfer, use, reproduction and destruction of TSCA CBI in his or her organization or facility.

**Hard-copy:** Data (i.e. submissions, printouts, photographs, etc) received or generated on paper.

**Information Management Division (IMD) director:** The IMD director is responsible for day-to-day implementation of TSCA CBI and control programs, including developing policies for the use and handling of TSCA CBI and operating the EPA headquarters Confidential Business Information Center (CBIC).

**Office of Program Management and Evaluation (OPME):** The OPME Director is responsible for oversight of the TSCA Confidential Business Information security function. This includes enforcement of the procedures and provisions contained in the TSCA Confidential Business Information Security Manual. The OPME Director also provides oversight of computer security programs for protection of TSCA CBI.

**Office of Pollution Prevention and Toxics (OPPT) director:** The OPPT director has overall authority for managing TSCA activities, including TSCA security programs.

**OPPT Confidential Business Information Center (CBIC):** 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.

**OPPT document control officer (OPPT DCO):** 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. He or she manages the headquarters CBIC, oversees other DCOs at headquarters, and provides training materials and guidance to all DCOs on appropriate TSCA CBI handling procedures.

**Requesting official:** This is (1) the 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 violations of this manual's procedures.

**Secure storage area (SSA):** 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.

**TSCA CBI:** Information claimed business confidential under EPA's confidentiality regulations at 40 CFR Part 2.

**TSCA CBI materials** are documents or any other information-bearing media that contain TSCA CBI.

**TSCA security staff:** The TSCA security staff is responsible for security-related activities, including reviewing security procedures, performing facility site inspections, and investigating violations of the procedures contained in this manual.

## CHAPTER 1

# INTRODUCTION

This manual sets forth procedures for Environmental Protection Agency (EPA) employees, other Federal employees, contractors, and contractor employees to follow in handling information claimed as confidential business information (CBI) under Section 14 of the Toxic Substances Control Act (TSCA) (15 U.S.C. §2613). That section of TSCA requires EPA to protect from public disclosure CBI obtained under TSCA, and it imposes criminal penalties for the knowing and willful unauthorized release or disclosure of such information. EPA has issued regulations (40 CFR Part 2) that implement TSCA's confidentiality provisions. The procedures in this manual supplement those set forth in TSCA and in 40 CFR Part 2. Where this manual and 40 CFR Part 2 Subpart B conflict, the CFR shall take precedence.

Sections 14(a)(1) and (2) of TSCA permits EPA to authorize Federal employees, contractors and contractor employees access to TSCA CBI when such access is necessary to perform work in connection with the agency's duties under a health or environmental protection statute or for specific law enforcement purposes.

Most TSCA CBI access occurs at EPA Headquarters, where the primary storage and use of TSCA CBI is in the EPA Confidential Business Information Center (CBIC). As required, EPA may authorize CBI access at other facilities, including EPA Regional Offices, other Federal agency offices, and contractor facilities. Procedures for handling, using, and storing TSCA CBI are generally uniform at all facilities. However, some differences in security procedures are required at facilities outside of EPA Headquarters, and at contractor sites.

## **A. GUIDING PRINCIPLES FOR SITUATIONS OUTSIDE OF THE MANUAL**

EPA recognizes that situations not covered by this manual may arise. In such cases, each Federal and contractor employee who is granted TSCA CBI access will act under the following guiding principles:

- Each user of TSCA CBI will ensure through personal conduct and accountability that he or she will act consistently with all guidelines established by EPA, contractors, or other Federal agencies to protect, to the best of his or her ability, all TSCA CBI.
- Each user will support management and other employees in carrying out their responsibilities for the protection, control, and security of TSCA CBI.

## **B. *MANUAL UPDATES AND REVISIONS TO PROCEDURES***

Whenever procedures change for the control, storage, security, and handling of TSCA CBI, EPA will update the relevant pages in this manual. A change transmittal sheet will be issued with each set of revised pages. It is suggested that the change transmittal sheets be filed in the back of the manual in sequential order. This manual includes a security manual update transmittal sheet (Appendix 21), which should be used to record revisions.

## CHAPTER 2

# HOW TO AUTHORIZE FEDERAL EMPLOYEES, CONTRACT EMPLOYEES, AND CONGRESS FOR ACCESS TO TSCA CBI

To obtain clearance for TSCA CBI access, employees of EPA, other Federal agencies, and contractors must fill out EPA Form 7740-6, "TSCA CBI Access Request, Agreement, and Approval" (Appendix 1). In addition, a separate form is sometimes required for obtaining computer access to TSCA CBI.

- Federal employees can obtain the forms from the EPA Form Distribution Centers. If the distribution centers are out of stock, the forms can be obtained from the OPPT DCO.
- Contractors can obtain the forms from their EPA project officer. If necessary, contractors can also obtain the forms from the OPPT DCO.
- Volunteers (non-paid), Law Clerks, students, interns (who are working for academic credit), and others are not Federal employees and are not eligible for TSCA CBI clearance and access. Under no circumstance should any volunteers receive access to information claimed as TSCA CBI.
- Senior Environmental Employment Program (SEEP) or American Association of Retired Persons (AARPs) staff are not Federal employees and are not eligible for TSCA CBI clearance and access. Under no circumstances should SEEP or AARP staff receive access to information claimed as TSCA CBI.



## **A. *STEPS TO TSCA CBI ACCESS FOR EPA EMPLOYEES***

### **1. AUTHORIZING ACCESS.**

a. **COMPLETING AND SUBMITTING THE FORMS.** The first step for EPA employees to obtain TSCA CBI access is the completion of Form 7740-6. The employee must submit the form to the facility DCO.

The DCO reviews the form for completeness and accuracy before forwarding it to the employee's immediate supervisor, to whom this manual will hereafter refer as the employee's requesting official. The requesting official will review the completed form. If the requesting official approves the form, he or she signs line 20 and returns it to the facility DCO. By signing the form, the requesting official verifies that the individual has attended a Security Briefing. The facility DCO will forward the form to the OPPT DCO for review and final approval.

b. **A SEPARATE FORM IS REQUIRED TO OBTAIN COMPUTER ACCESS TO TSCA CBI DATA.** Employees who require online access to TSCA CBI data stored on mini computers, or computers linked by local area network must submit Form 7740-25, "TSCA CBI ADP User Registration Form" (Appendix 2) to the DCO on site, who will forward the form to the OPPT DCO for processing.

c. **INDIVIDUAL ACCESS FILES.** A DCO is responsible for establishing an access file for each employee in his or her organization who is granted authority to access TSCA CBI. The file must contain a copy of all forms or other documentation related to the employee's TSCA CBI clearance. If required by personnel regulations, the "SF 86 Questionnaire For Sensitive Positions" (Appendix 3) should be kept in the employee's official personnel file. The files must be maintained in alphabetical order by employee name. Contractors' access files are kept by the DCOs at their facilities; the OPPT DCO maintains all EPA headquarters employees' access files.

d. **SECURITY BRIEFING IS REQUIRED.** It is the responsibility of requesting officials to ensure that their employees (1) read this manual and (2) attend a security briefing (video or oral) on procedures for handling TSCA CBI documents. Employees must attend a briefing on CBI security procedures before they are allowed access to TSCA CBI. The briefing, on video, is presented weekly by the OPPT DCO. It can also be presented by a facility DCO; DCAs can perform this same functions as a DCO. The DCA can give the DCO the required annual briefing and sign EPA Form 7740-28. If management has not appointed a DCA, the DCO's supervisor (minimum Branch chief level) must certify that the DCO has been briefed (viewed the video) and sign the EPA Form 7740-28. The certification, a memorandum, should be attached to the signed Form 7740-28 and forwarded to the OPPT DCO.

e. **APPROVAL FOR TSCA CBI ACCESS OR WAIVER FOR IMMEDIATE ACCESS.** The OPPT DCO will add the employee's name to the TSCA CBI authorized access list when the employee is approved for TSCA CBI access. The OPPT DCO will notify the employee's DCO of approval by sending him or her the TSCA CBI authorized access list. The employee has 10 days to comply with the OPPT DCO's requirements before final approval is granted.

Facility DCOs must notify the OPPT DCO by the 15th of each month of additions or deletions that must be made to the TSCA CBI authorized access list.

A requesting official may allow an employee access to TSCA CBI before receiving final approval from the OPPT DCO under the following conditions: The requesting official has determined that immediate access is necessary, the required forms have been completed and submitted to the OPPT DCO, and the employee has attended the security briefing.

f. **TSCA CBI AUTHORIZED ACCESS LIST.** After EPA employees are approved for TSCA CBI access, they are listed on the TSCA CBI authorized access list. EPA's CBIC uses the list, with the automated Confidential Business Information Tracking System (CBITS), to control access to TSCA CBI materials. The list includes the names of employees cleared for TSCA CBI computer access and the expiration date for their access. The OPPT DCO provides copies of the access list monthly to DCOs and can answer inquiries about whether an employee is authorized for access to TSCA CBI.

## 2. REQUIREMENTS FOR MAINTAINING ACCESS.

a. **GENERAL INFORMATION.** Each year, EPA employees who are authorized for access to TSCA CBI must follow certain procedures to maintain their access.

b. **DOCUMENT AUDIT PROCEDURE.** The DCO will furnish the employee with a report listing all documents that the DCO's manual or automated inventory log reflects are charged out to that employee. The employee must reconcile the report by (1) verifying that he or she (employee) has the listed documents in his or her (employee) possession and signing the Document Reconciliation Certification (Appendix 22), (2) notifying the DCO that he or she (employee) does not have the documents in his or her (employee) possession and so indicating on the Document Reconciliation Certification, or (3) indicating on the Document Reconciliation Certification that no documents are charged out. If the employee fails to locate the documents, he or she (employee) must follow the procedures discussed in Chapter 5. Once a report is submitted, as required by Chapter 5, the DCO (after receiving written approval from the employee's requesting official) may renew the employee's access.

After the DCO reviews the Document Reconciliation Certification, a copy of the certification form will be filed in the employee's Individual Access File.

c. **SCHEDULING AN ANNUAL SECURITY BRIEFING.** After the Document Reconciliation Certification process is completed, the next step is for the employee to attend a security briefing. The facility DCO is responsible for scheduling annual security briefings for employees. If employees attend a briefing presented by a facility DCO, it is the facility DCO's responsibility to provide their names to the OPPT DCO.

d. **FAILURE TO RECONCILE DOCUMENT AUDIT REPORT OR ATTEND AN ANNUAL SECURITY BRIEFING.** The OPPT DCO will suspend the access authority of any employee who fails to reconcile their audit report or attend a security briefing within a year of his or her last briefing. The OPPT DCO will notify the employee's requesting official of the suspension. If the employee does not attend an annual security briefing within 30 days from the date his or her access expired, the OPPT DCO will on the 31st day terminate the employee's TSCA CBI authorization and deactivate the employee's electronic card key for accessing TSCA CBI secure storage areas, along with all computer access authorization, including user identifications and passwords.

e. **EFFECT OF SUSPENSION OF ACCESS.** Employees who have failed to maintain access to TSCA CBI in accordance with manual procedures are in violation of TSCA security procedures and will have their TSCA CBI access suspended. Such persons may be subject to the penalties identified in Chapter 5. An employee's access to TSCA CBI in his or her possession at the time of suspension does not constitute unauthorized disclosure of CBI as that term is utilized in Chapter 5. However, any disclosure of TSCA CBI to an employee whose access has been suspended does constitute an unauthorized disclosure of CBI.

f. **REAPPLYING FOR TSCA CBI ACCESS.** If an employee has been removed from the TSCA CBI authorized access list, he or she must reapply for TSCA CBI access. Employees who must reapply for TSCA CBI access must follow the procedures in section A.1 of this chapter. Contact the OPPT DCO for specific instructions before submitting renewal forms.

g. **EMPLOYEE TRANSFERS WITHIN EPA.** The OPPT DCO must be notified when an employee transfers to another branch, division, or office if the new position requires TSCA CBI access. It is the responsibility of the employee's former requesting official to notify the OPPT DCO of the transfer so the employee's current access authorization can be cancelled. If the employee's new position requires TSCA CBI access, his or her new requesting official is responsible for submitting a completed Form 7740-6 "TSCA CBI Access Request, Agreement, and Approval."

## **B. STEPS TO TERMINATING TSCA CBI ACCESS FOR EPA EMPLOYEES**

1. **GENERAL INFORMATION.** Authorization for access to TSCA CBI must be terminated when:

- The employee stops working at EPA.
- The employee transfers to a new position in EPA that does not require access to CBI.
- The employee fails to attend the annual security briefing.
- The employee receives an administrative penalty suspending his or her authority to access TSCA CBI.

### **2. REQUIREMENTS FOR TERMINATING ACCESS.**

a. **FORM 7740-16.** When an employee's TSCA CBI clearance is relinquished or revoked, he or she must complete EPA Form 7740-16, "Confidentiality Agreement for United States Employees Upon Relinquishing TSCA CBI Access Authority" (Appendix 9). The employee's requesting official and facility DCO are responsible for ensuring that the employee completes the form within five days after the employee's TSCA CBI access authority is canceled.

The employee must submit the completed form to his or her requesting official, who sends it to the OPPT DCO. The requesting official must also send a copy of the completed form to the facility DCO for placement in the employee's TSCA CBI Access File.

b. **DOCUMENT AUDIT PROCEDURE.** After receiving Form 7740-16, the facility DCO will furnish the employee with a report listing all the documents that the CBITS system and the facility DCO's manual or automated inventory log show as being in the employee's possession. The DCO is responsible for assisting the employee in returning these documents. All of the returned documents must be re-entered into the collection of records before any individual TSCA CBI document charged out to a terminating employee can be reissued to another TSCA CBI-cleared employee.

**c. DCO RESPONSIBILITIES AFTER DOCUMENT AUDIT IS COMPLETED.**

After the document reconciliation is complete, the facility DCO will:

- Request that the OPPT DCO remove the employee's name from the TSCA CBI authorized access list.
- Inform the employee DCO that the employee is no longer authorized for CBI access.
- Request that the OPPT DCO instruct the Facilities Management and Services Division (FMSD), Office of Administration, to invalidate the employee's electronic entry card access for EPA headquarters TSCA CBI secure storage areas.
- Change the combinations to locks for any TSCA CBI secure storage containers to which the employee had access. At EPA headquarters, the facility DCO can request that a security representative of FMSD's Security Management Section change the lock combinations for any TSCA CBI storage containers or secure storage areas.

The OPPT DCO will direct IMD's TSCA Systems Section to invalidate the employee's TSCA CBI computer user identification code and passwords for all mini or micro computer systems to which the employee had access. When the TSCA Systems Section completes the invalidation, the section will provide written confirmation to the OPPT DCO.

**d. MISSING DOCUMENTS.** The facility DCO must assume that a TSCA CBI document is missing when it is not received within 30 days of issuing the employee the list of items charged out to him or her. The procedures for reporting these documents as missing are in Chapter 5 of this manual.

e. **EMPLOYEE RESPONSIBILITIES.** Employees who are relinquishing their TSCA CBI access authority are responsible for returning all TSCA CBI documents and magnetic media in their possession to the facility's DCO. Employees who are terminating their employment must return to FMSD all electronic entry cards for EPA headquarters facilities. Regional or laboratory employees who have electronic entry cards for secure storage areas must relinquish those cards to the issuing office prior to signing Form 7740-16, "Confidentiality Agreement for United States Employees Upon Relinquishing TSCA CBI Access Authority." EPA headquarters employees who are terminating their employment must obtain signatures from the OPPT DCO and FMSD on the "Employee Separation or Transfer Checklist", EPA Form 3110-1 (Appendix 11) when relinquishing their TSCA CBI clearance.

### **C. STEPS TO TSCA CBI ACCESS FOR CONTRACTORS AND SUBCONTRACTORS**

#### **AUTHORIZING ACCESS.**

1. **DETERMINING WHETHER ACCESS TO TSCA CBI IS NECESSARY.** It is EPA's responsibility to decide whether access to TSCA CBI is necessary for a contractor to successfully perform the conditions of a contract with the U.S. government. Depending on the contract, the EPA project officer, the EPA delivery order project officer, or the EPA work assignment manager (in the case of GSA zone contracts) will evaluate the need for TSCA CBI access. (The Project Officers Checklist, appendix 24, will assist project officers in compiling all information required for contractor access to TSCA CBI.)

If it is determined that access is necessary, the EPA project officer (PO), EPA delivery order project officer (DOPO), or the EPA work assignment manager (WAM) must complete EPA Form 7740-17, "Request for Approval of Contractor Access to TSCA Confidential Business Information" (Appendix 6). Form 7740-17 should be submitted as early in the contracting process as possible.

- For new contracts, Form 7740-17 should be submitted to the IMD director with the initial procurement package.

- For existing contracts, a delivery order will probably be necessary to modify the contract. Form 7740-17 should be submitted to the IMD director prior to the modification request.

The EPA project officer must forward the form to his or her division director or a supervisor of equivalent authority, who will sign the form as the requesting official and forward it to the IMD director for final approval and publication in the Federal Register.

**2. EPA CONTRACTORS WHO RECEIVE TSCA CBI MUST SET UP A SECURE ENVIRONMENT FOR HANDLING AND STORING TSCA CBI.** In establishing a secure environment, contractors are bound by (1) the conditions and terms of their contracts with EPA and (2) the requirements of this manual. Each contractor must maintain TSCA CBI in a secure environment that meets or exceeds the requirements contained herein. In addition to the physical security procedures set forth in Chapter 4, a two-barrier system must be used to protect TSCA CBI at any contractor's storage site that is not located within an EPA or other Federal Agency facility.

Barrier 1 must consist at a minimum of perimeter walls that are constructed from "slab to slab" and do not have false ceilings that would permit entry into the contractor's work space by simply climbing over a corridor wall. Doors that provide ingress or egress must have pin tumbler deadbolt locks installed (unless the door is for emergency egress, in which case it would have a crash bar with an audible alarm). All doors providing ingress or egress that have hinge pins exposed to public corridors must be pinned or constructed in such a way so as to prevent removal of the hinge pin.

Barrier 2 must consist of any of the approved storage containers listed in Chapter 4. Contractors should contact the TSCA Security Staff if they have any questions about establishing or maintaining the security of TSCA CBI.

**3. SITE INSPECTION.** After the contractor has established a secure environment for TSCA CBI, the TSCA security staff must inspect the site. TSCA CBI access will not be authorized at the contractor's site without the approval of the TSCA Security Staff.



**4. REQUIRED CONTRACT LANGUAGE.** All contracts that are approved by the IMD director for TSCA CBI access must contain the following contract clauses from the Procurement Policy Notice No. 93-07 of August 1993: Data Security for TSCA CBI (EP52.235-120) (Appendix 8); Access to TSCA Confidential Business Information (EP52.235-100) (Appendix 8a); Control and Security of TSCA Confidential Business Information (EP52.235-105) (Appendix 8b); and Treatment of Confidential Business Information (1552.235-71) (DEVIATION) (Appendix 8c). The EPA project officer is responsible for (1) notifying EPA's Office of Acquisition Management (OAM) contracting officer that the required TSCA CBI language is necessary and (2) forwarding Form 7740-17 to OAM, after the IMD director has signed it.

**5. NOTICE TO AFFECTED BUSINESSES.** Pursuant to 40 CFR Part 2.306(j), EPA must notify affected businesses prior to allowing TSCA CBI access to a contractor or subcontractor. IMD will prepare the notice and, at its discretion will (1) publish it in the Federal Register or (2) send it to individual businesses by letter via certified mail, return receipt requested or (3) be notified by telegram. The affected business must have at least 5 working days of notice (40 CFR 2.306(j)(3)) before access is granted. This means that the contractor cannot be granted access until 5 days after the Federal Register notice is published or the telegram or certified mail is received.

The EPA project officer must initiate the notice process at least 60 days before the date that TSCA CBI access is to begin. The first step is to complete a Contractor Information Sheet (Appendix 7), which the OPPT DCO uses to prepare the notice. The IMD director signs the notice, which signifies that the contractor(s) identified in the notice is authorized for access to TSCA CBI.

The notice must contain the following:

- The identity of the contractor or subcontractor to which TSCA CBI is to be disclosed.
- The contract number.
- An explanation of why access to TSCA CBI is necessary for satisfactory performance of the contract.

- Whether access is authorized only on EPA premises or also at the contractor's or subcontractor's facilities.
- The type of information to be disclosed.
- The period of time for which access to TSCA CBI is authorized.

**6. FACILITY DCO AT THE CONTRACTOR'S SITE.** The contractor DCO (1) serves as the liaison between EPA and the contractor on issues relating to TSCA CBI, (2) assists the EPA facility DCO in requesting and maintaining TSCA CBI access authorization for individual contractor employees (see Chapter 3), and (3) assists in TSCA CBI handling. The contractor DCO serves this function even when contractor employee access to TSCA CBI will occur at EPA facilities. Each contractor with TSCA CBI access must have a contractor DCO.

**7. HOW TO ASSIGN A DCO.** The EPA project officer is responsible for identifying two qualified contractor employees to act as the contractor DCO and the alternate DCO. The EPA project officer must nominate the employees to the OPPT DCO. The nomination, submitted in writing, must include the employees' names, telephone numbers, electronic mail numbers, fax numbers, and mailing addresses. The contractor DCO must be in place before the contractor is allowed access to TSCA CBI. (See Chapter 3 for information about the nomination process.)

**8. IDENTIFYING CONTRACTOR EMPLOYEES FOR CLEARANCE.** After completion of the above requirements, the EPA project officer, EPA delivery order project officer, or the EPA work assignment manager is responsible for conferring with contractor officials to determine which contractor employees require TSCA CBI access authorization. The EPA project officer will request access authorization for these individuals in the manner described in section D of this chapter.

## **D. *HOW TO OBTAIN TSCA CBI AUTHORIZATION FOR EMPLOYEES OF CONTRACTORS AND SUBCONTRACTORS***

After a contractor is authorized for access to TSCA CBI, the contractor's employees must individually request TSCA CBI access authority.

All necessary forms are available from the EPA project officer. If necessary, the forms can also be obtained from the OPPT DCO.

### **1. AUTHORIZING ACCESS.**

a. **COMPLETING AND SUBMITTING THE FORMS.** Each contractor employee who is applying for TSCA CBI access must complete the following forms:

- 1) Form 7740-6, "TSCA CBI Access Request, Agreement, and Approval" (Appendix 1).
- 2) SF-86, "Questionnaire for Sensitive Positions" (Appendix 3).
- 3) FD-258, fingerprint chart (two originals) (Appendix 4).
- 4) Form 7740-25, "TSCA CBI ADP User Registration Form," if online access to a TSCA CBI system or data base is required (Appendix 2).

The completed forms must be submitted to the contractor DCO. After reviewing the forms for accuracy and completeness, the contractor will forward the forms to the EPA project officer. The EPA project officer will review the forms and forward them to the OPPT DCO.

The project officer will either sign line 20 of the general access request form to signify approval of TSCA CBI access or will disapprove access. The project officer will submit the approved forms to the OPPT DCO for review and approval. After completing the review, the OPPT DCO will sign the forms and may submit them to the TSCA security staff and the IMD director for final approval.

b. **MINIMUM BACKGROUND INVESTIGATION (MBI).** All contractor employees who are granted access to TSCA CBI will be required to successfully complete an MBI to maintain TSCA CBI clearance. MBI investigations are conducted by the U.S. Office of Personnel Management at the request of the EPA Inspector General. The EPA project officer or work assignment manager must ensure the MBI investigation requirement is placed in the official statement of work.

c. **INDIVIDUAL ACCESS FILES.** The contractor's facility DCO is responsible for establishing an access file for each contractor employee in his or her organization who is granted authority to access TSCA CBI. The file will contain a copy of all forms or other documentation related to the employee's TSCA CBI clearance. If required by personnel regulations, a copy of the SF 86, "Questionnaire For Sensitive Positions" should be kept in the employee's official personnel file. The access files will be maintained in alphabetical order by employee name and stored with the TSCA CBI collection of records. The OPPT DCO will maintain the Individual Access Files for contract employees who are located at EPA headquarters.

d. **SECURITY BRIEFING IS REQUIRED.** It is the responsibility of the requesting official to ensure that employees (1) read this manual and (2) attend a security briefing on procedures for handling TSCA CBI documents. Employees must attend a briefing on TSCA CBI security procedures before they are allowed access to TSCA CBI. The briefing, given orally or presented on video, is presented weekly by the OPPT DCO, or it can also be presented by a facility DCOs. If employees attend a briefing presented by a facility DCO, it is the facility DCO's responsibility to provide their names to the OPPT DCO.

e. **APPROVAL FOR TSCA CBI ACCESS OR WAIVER FOR IMMEDIATE ACCESS.** The OPPT DCO will add the contractor employee's name to the TSCA CBI authorized access list when the contractor employee is approved for CBI access. The OPPT DCO will notify the contractor employee's DCO of approval by sending the contractor DCO the TSCA CBI authorized access list.

A waiver may be granted by the Director, Information Management Division which will allow a contractor and/or contractor employee(s) access to TSCA CBI before receiving final approval from the OPPT DCO when all of the following conditions are met: the requesting official has determined that immediate access is necessary, the required form(s) have been completed and submitted to the OPPT DCO, the employee(s) have attended the security briefing, the facility at which the employee(s) is working has been inspected and approved by the TSCA security staff, and the Federal Register Notice has been submitted for publication.

f. **TSCA CBI AUTHORIZED ACCESS LIST.** After contractor employees are approved 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. Questions about whether a particular person has TSCA CBI access that can not be answered by consulting the Authorized Access List should be directed to the OPPT DCO. The OPPT DCO provides copies of the access list monthly to DCOs.

## **2. REQUIREMENTS FOR MAINTAINING ACCESS.**

a. **GENERAL INFORMATION.** Each year, contractor employees who are authorized to access TSCA CBI must follow certain procedures to maintain their access. The procedures are listed below in the order in which they must occur.

b. **DOCUMENT AUDIT PROCEDURE.** The contractor DCO will furnish the contractor employee with a report listing all documents that the DCO's manual or automated inventory log shows as charged out to that employee. The employee must reconcile the report by (1) verifying that he or she has the listed documents in his or her possession and signing the Document Reconciliation Certification (Appendix 22), (2) notifying the DCO that he or she does not have the documents and indicating on the Document Reconciliation Certification that the documents are not in his or her possession, or (3) indicating on the Document Reconciliation Certification that no documents are charged out. If the DCO fails to locate any documents, he or she must follow the procedures discussed in Chapter 5.

After the DCO reviews the Document Reconciliation Certification, he or she will file a copy of the certification form in the employee's Individual Access File.

c. **SCHEDULING AN ANNUAL SECURITY BRIEFING.** After the document audit procedure is completed, the next step is for the employee to attend a security briefing. The contractor's facility DCO is responsible for scheduling annual security briefings for employees; the DCA is authorized to give the DCO the required briefing and sign the EPA Form 7740-28. If management has not appointed a DCA, the project officer must certify (by memorandum to the OPPT DCO) that the DCO has read the security manual briefing materials or viewed the TSCA CBI training video and sign the EPA Form 7740-28.

d. **FAILURE TO ATTEND AN ANNUAL SECURITY BRIEFING.** Contractor employees will lose their authorization for access to TSCA CBI if they fail to attend a security briefing within a year of their last briefing. The OPPT DCO will notify an employee's requesting official of the suspension. If the employee does not attend an annual security briefing within 30 days from the date the suspension notice was issued, the OPPT DCO will on the 30th day terminate the employee's TSCA CBI authorization and deactivate the employee's electronic card key for accessing TSCA CBI secure storage areas, along with all computer access authorization, including user identifications and passwords. It is the responsibility of the requesting official to ensure that the employee completes the paperwork connected with TSCA CBI termination (see section E of this chapter).

e. **REAPPLYING FOR TSCA CBI ACCESS.** If an employee has been removed from the TSCA CBI authorized access list, he or she must reapply for TSCA CBI access. To reapply, the employee must follow the procedures in section D.1 of this chapter. Contact the OPPT DCO for specific instructions before submitting renewal forms.

## **E. PROCEDURES FOR TERMINATING ACCESS TO TSCA CBI FOR CONTRACTOR EMPLOYEES**

1. **GENERAL INFORMATION.** Authorization to access TSCA CBI must be terminated when:

- The contract is completed, terminated or in suspense.
- Employment of the contractor employee is terminated.
- Contractor employee's duties that require access to TSCA CBI are terminated.
- The contractor employee fails to attend the annual security briefing.
- The contractor employee breaches the terms of the Confidentiality Agreement of EPA Form 7740-6, "TSCA CBI Access Request, Agreement, and Approval."
- The MBI provides information about the contractor employee based on which the IMD director determines that access will not be granted.

## **2. REQUIREMENTS FOR TERMINATING ACCESS.**

a. **FORM 7740-18.** When a contractor employee's TSCA CBI clearance is suspended, relinquished, or revoked, he or she must complete EPA Form 7740-18, "Confidentiality Agreement for Contractor Employees Upon Relinquishing TSCA CBI Access Authority" (Appendix 10). The employee's requesting official and DCO are responsible for ensuring that the employee completes the form within five days after the employee's TSCA CBI access authority is canceled.

The employee must submit the completed form to his or her requesting official, who sends it to the OPPT DCO. The requesting official must also send a copy of the completed form to the facility DCO for placement in the employee's TSCA CBI Access File.

b. **DOCUMENT AUDIT PROCEDURE.** After receiving Form 7740-18, the facility DCO will furnish the contractor employee with a report listing all the documents that the CBITS system, DAPSS system, and the facility DCO's inventory log show as being in the contractor employee's possession. The contractor employee is responsible for returning these documents. All of the returned documents must be re-entered into the collection of records before any individual TSCA CBI document charged out to the terminating employee can be reissued to another TSCA CBI-cleared employee.

c. **DCO RESPONSIBILITIES AFTER DOCUMENT AUDIT IS COMPLETED.** After the document reconciliation is complete, the facility DCO will:

- Request that the OPPT DCO remove the employee's name from the TSCA CBI authorized access list.
- Inform the employee's DCO that the employee is no longer authorized for TSCA CBI access.
- Request the OPPT DCO to invalidate the employee's electronic entry card access for EPA headquarters TSCA CBI secure storage areas.
- Change the combinations to locks for any TSCA CBI secure storage containers to which the employee had access.

d. **MISSING DOCUMENTS.** The facility DCO must assume a TSCA CBI document is missing when it is not received within 30 days of issuing the contractor employee the list of items charged out to him or her. The procedures for reporting these documents as missing are in Chapter 5.

The OPPT DCO will direct IMD's TSCA Systems Section to invalidate the employee's TSCA CBI computer user identification code and passwords for all mini, or micro computer systems to which the employee had access. When the TSCA Systems Section completes the invalidation, the section must provide written confirmation to the OPPT DCO.



e. **CONTRACTOR EMPLOYEE RESPONSIBILITIES.** Employees who are relinquishing their TSCA CBI access authority are responsible for returning all TSCA CBI documents and magnetic media in their possession to the facility DCO. Employees who are terminating their employment must return to the OPPT DCO all electronic entry cards for EPA headquarters facilities. EPA project officers are responsible for ensuring that all electronic entry cards issued to contractor employees are returned to the OPPT DCO.

#### ***F. PROCEDURES FOR TERMINATING ACCESS TO TSCA CBI FOR CONTRACTORS***

##### **TERMINATING ACCESS TO TSCA CBI WHEN A CONTRACT ENDS.**

On the day a contract is completed or access to TSCA CBI ends under the contract's terms, the contractor DCO must inventory the TSCA CBI materials that the CBITS system, DAPSS system, and the DCO's manual or automated inventory log show as being at the contractor's facility. The contractor DCO must provide the written inventory to the EPA project officer within 30 calendar days. The EPA project officer must provide a copy of the results to the OPPT DCO and the TSCA security staff. The contractor DCO must collect all TSCA CBI materials and document control materials, including logs and cover sheets, that are in the company's possession. The contractor must transfer the materials to the TSCA CBI cleared project officer (or other cleared official, i.e. DOPO, WAM) within 30 calendar days. The EPA Project Officer will forward the reconciled documents to the OPPT DCO within 30 days for inclusion into the official Agency file.

The EPA project officer will review the materials and reconcile the returned materials with the inventory provided by the contractor DCO. The EPA project officer then transfers the materials to the OPPT DCO with instructions for appropriate disposition.

### **G. AUTHORIZING OTHER FEDERAL AGENCIES FOR ACCESS TO TSCA CBI**

TSCA provides that under certain circumstances other Federal agencies may receive access to TSCA data. Specifically disclosure of TSCA CBI to another Federal agency is permitted when the information is necessary for the other agency (1) to perform work for EPA, (2) to perform its duties under any law for the protection of health or the environment, or (3) for specific law enforcement purposes. All persons contemplating disclosure of TSCA CBI to Federal agencies should review 40 CFR §§ 2.209 and 2.306.

#### **1. GENERAL PROCEDURES FOR EPA OFFICES TO DISCLOSE TSCA CBI TO ANOTHER FEDERAL AGENCY PERFORMING WORK FOR EPA.**

When an EPA office is having another Federal agency perform work that requires access to TSCA CBI, EPA generally takes the initiative in arranging to disclose the information to the other agency. The first step to allow disclosure is for the EPA office that is involved to contact the IMD director.

The IMD director will notify the other agency that (1) the information that will be disclosed is CBI and was acquired under the authority of TSCA and that (2) any unauthorized disclosure of the information may subject the other agency's employees to the criminal penalties in Section 14(d) of TSCA (see Chapter 5 of this manual).

When EPA discloses TSCA CBI to another agency to perform work on behalf of EPA as described in 40 CFR §§ 2.209(c) and 2.306(h), no notice to affected businesses is required. The IMD director will notify the agency performing the work whether access is approved.

a. **AGREEMENT NOT TO DISCLOSE TSCA CBI.** The agency that will receive TSCA CBI must provide a written agreement that it will not disclose TSCA CBI.

b. **EXCEPTIONS TO AGREEMENT NOT TO DISCLOSE TSCA CBI.** A Federal agency does not have to provide a written agreement that it will not disclose TSCA CBI under any one of the following circumstances:

- 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's regulations.
- The agency has obtained the consent of each affected business prior to the proposed disclosure.
- The agency has obtained a written statement from the EPA general counsel or an EPA regional counsel that disclosure of the information would be proper under EPA regulations.

c. **TSCA CBI ACCESS AT EPA FACILITIES.** Once approval for 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 clearance for TSCA CBI access are explained in sections A and B of this chapter.

d. **TSCA CBI ACCESS AT OTHER FEDERAL AGENCIES.** When a Federal agency is allowed access to TSCA CBI on its premises, the Federal agency must appoint a facility DCO and must provide a secure environment before documents will be transferred.

e. **HOW TO ASSIGN A DCO.** The requesting official or the facility manager in charge of the facility to which TSCA CBI will be transferred must nominate a facility DCO and an alternate DCO. The nomination, submitted in writing to the OPPT DCO, must include the name, telephone number, electronic mail number, fax number, and mailing address of both nominees. The OPPT DCO will decide whether to approve the nomination. The requesting official or the facility DCO can also nominate document control assistants (DCAs) to assist the DCO in his or her day-to-day duties. DCAs can perform the same duties and responsibilities as the DCOs (i.e. DCAs can annually brief the DCO and sign the EPA Form 7740-28).

2. **PROCEDURES FOR ANOTHER FEDERAL AGENCY TO REQUEST ACCESS TO TSCA CBI.** These procedures must be followed by Federal agencies that are requesting access to TSCA CBI (1) to perform duties under any law for the protection of health or the environment or (2) for a specific law enforcement purpose.

a. **SUBMIT A WRITTEN REQUEST.** To obtain access to TSCA CBI, a Federal agency must submit a written request to the IMD director at least one month before access is needed. The request must state the specific information to which access is requested, why access is necessary (this is the official purpose and will be one of the two reasons stated in the preceding paragraph), and provide supporting details. The request must be signed by an agency official whose authority is at least equivalent to that of an EPA division director.

b. **AGREEMENT NOT TO DISCLOSE TSCA CBI.** The agency that will receive TSCA CBI must provide a written agreement that it will not disclose TSCA CBI.

c. **EXCEPTIONS TO AGREEMENT NOT TO DISCLOSE TSCA CBI.** A Federal agency does not have to provide a written agreement that it will not disclose TSCA CBI under any one of the following circumstances:

- 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's regulations.
- The agency has obtained the consent of each affected business prior to the proposed disclosure.
- The agency has obtained a written statement from the EPA general counsel or an EPA regional counsel that disclosure of the information would be proper under EPA regulations.

d. **NOTICE TO AFFECTED BUSINESSES.** Before EPA allows another Federal agency access to TSCA CBI, EPA must provide written notice to affected businesses except as stated in section G.1 above. The notice must be given at least 10 calendar days before access takes place by Federal Register notice, telegram, or certified mail (return receipt requested). IMD will prepare the notice, which must include

- The identity of the agency to which TSCA CBI access is being allowed.

- The official purpose for the access.
- Whether access is authorized only on EPA premises or also at the other agency's facilities (see section 3 of this chapter).
- The type of information that will be disclosed.
- The period of time for which access to TSCA CBI is being authorized.

**3. EPA'S PROCESS FOR APPROVING TSCA CBI ACCESS FOR OTHER FEDERAL AGENCIES.** The IMD director will review requests for TSCA CBI access from other Federal agencies and will notify the agencies' requesting officials whether TSCA CBI access is approved. If access is approved, the IMD director will notify the other agency that (1) the information that will be disclosed is CBI and was acquired under the authority of TSCA, and that (2) any unauthorized disclosure of the information may subject the other agency's employees to criminal penalties allowed under Section 14(d) of TSCA.

**a. TSCA CBI ACCESS AT EPA FACILITIES.** EPA prefers that TSCA CBI materials remain on EPA premises. When this is not practical, EPA will consider allowing access at another agency's facility.

Once approval for 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 clearance for TSCA CBI access are explained in sections A and B of this chapter. 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 individuals not authorized for TSCA CBI access. TSCA CBI must be transferred from an EPA DCO to a Facility/Agency DCO.

b. **TSCA CBI ACCESS AT OTHER FEDERAL AGENCIES.** Before EPA will grant access at another agency's facility, a facility DCO must be in place. The requesting official or the facility manager in charge of the facility to which TSCA CBI will be transferred must nominate a facility DCO and an alternate DCO. The nomination, submitted in writing to the OPPT DCO, must include the name, telephone number, electronic mail number, fax number, and mailing address of both nominees. The OPPT DCO will decide whether to approve the nomination. The requesting official or the facility DCO can also nominate document control assistants (DCAs) to assist the DCO in his or her day-to-day duties. Other provisions that must be in effect are the following:

- The Federal agency must have security procedures and standards in place that equal or surpass those set forth in this manual.
- EPA's TSCA security staff must inspect and approve the TSCA CBI storage facilities at the Federal agency. The inspection is to be arranged by the official requesting TSCA CBI clearance for his or her agency.
- The Federal agency must appoint a facility DCO before documents will be transferred.
- The official requesting TSCA CBI access authority for his or her agency must provide a written statement of the agency's security procedures for handling TSCA CBI. The statement should state whether (1) the security procedures in this manual have been adopted by the agency without change or (2) how the security procedures being used at the agency differ from those set forth in this manual. The written statement must be provided to the TSCA security staff.

**4. REQUESTS FOR ACCESS TO TSCA CBI FROM CONGRESS OR THE GENERAL ACCOUNTING OFFICE.** EPA, Federal and contractor employees must notify the IMD director immediately when they receive a request from Congress or the General Accounting Office 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, the President of the Senate, a chairman of a committee or subcommittee, or the Comptroller General. All document access will be provided by the OPPT DCO, who will record all transactions on a Federal Agency, Congress, and Federal Court Sign Out Log (Appendix 20).

**NOTICE TO AFFECTED BUSINESSES.** Before EPA allows access to TSCA CBI by Congress or the General Accounting Office, EPA must provide written notice to affected businesses. The notice must be given at least 10 calendar days before access takes place by Federal Register notice, telegram, or certified mail (return receipt requested). IMD will prepare the notice, which must include:

- Whether access is authorized only on EPA premises or also at the other agency's facilities.
- The type of information that will be disclosed.
- The period of time for which access to TSCA CBI is being authorized.

## CHAPTER 3

# RESPONSIBILITIES

### ***A. EMPLOYEE RESPONSIBILITIES***

**1. EPA HOLDS EMPLOYEES PERSONALLY ACCOUNTABLE FOR PROTECTING TSCA CBI.** Proper protective controls must be followed by employees of EPA, other Federal agencies, and Federal contractors who have access to TSCA CBI whenever they handle, store, or transfer any TSCA CBI. EPA holds every employee who has custody of TSCA CBI personally responsible for following proper handling and security procedures.

- Each employee who has access to TSCA CBI is required to (a) immediately inform management if he or she discovers that any procedure contained in this manual does not provide the proper level of protection for TSCA CBI and (b) suggest changes that will strengthen those weaknesses.
- Each employee who has access to TSCA CBI is required to immediately report in writing any violations of this manual's procedures to his or her immediate supervisor, the TSCA security staff, and if applicable, the contractor project officer.

Employees who have access to TSCA CBI are

- Accountable for all TSCA CBI documents that they receive through a DCO or any other employee cleared for TSCA CBI.
- Required to support the programs established by their management and DCO for protecting and handling TSCA CBI.
- Required to attend an annual security briefing prior to renewing their TSCA CBI clearance and to stay informed of TSCA CBI handling controls and security programs.



- Required to complete an annual audit of all TSCA CBI documents charged out to them through a DCO prior to completing the annual security briefing and to sign the Document Reconciliation Certification (Appendix 22) after reconciling the documents listed on the report.
- Required to maintain TSCA CBI in a responsible manner that will not permit access to the data by anyone who has not been properly authorized to view TSCA CBI.

2. **DOCUMENT AUDIT PROCEDURES.** Each year, every employee is required to account for the **hard copy** TSCA CBI documents in his or her possession. This procedure is always the first step of the annual process to recertify employees for TSCA CBI clearance.

The facility DCO will furnish the employee with a list of documents that the DCO's manual or automated inventory log shows the employee has in his or her possession. The employee must certify that the documents are in his or her possession by signing the certification statement inscribed on the document list. The employee must contact the facility DCO immediately if he or she does not have any of the documents on the list.

3. **CHECKING OUT TSCA CBI DOCUMENTS.** Employees are permitted to check out TSCA CBI documents from their facility DCO and to keep the documents for up to a year. However, employees should return TSCA CBI to the facility DCO as soon as the material is no longer needed.

**OVERDUE MATERIALS.** TSCA CBI materials **cannot** be kept for more than one year. Any material kept longer than a year is considered overdue, and the facility DCO will notify the responsible employee. Materials that are not returned to the DCO within 30 days of notification are presumed lost. The DCO must notify his or her division director of lost materials, pursuant to the procedures in Chapter 5.

**4. DETERMINING WHETHER A DOCUMENT CONTAINS TSCA CBI.**

When an employee produces a document, it is that employee's responsibility to decide whether the document contains TSCA CBI. An employee who is unable to determine whether something is confidential should consult with his or her supervisor or DCO. If the issue remains unresolved, the employee should consult the chief of the IMD TSCA Information Management Branch.

**5. RECEIPT OF MAIL CONTAINING TSCA CBI MATERIAL.** If employees receive materials in the mail that are believed to be TSCA CBI, even if they are unlabeled, those materials must be taken immediately to the facility's DCO for proper entry into the document tracking system.

**6. REVIEWING AND CHALLENGING TSCA CBI CLAIMS.** An employee who encounters a TSCA CBI claim that appears to be invalid should bring the issue to the attention of the proper office in EPA.

- EPA employees and Federal employees should contact IMD's TSCA Information Management Branch, which routinely conducts program challenges pursuant to CFR 2.204.
- EPA regional employees should contact the TSCA Information Management Branch or the Office of General Counsel.
- Contractor employees should contact IMD's TSCA Information Management Branch with any questions about TSCA CBI claims.

a. **INFORMAL INQUIRIES.** EPA employees are permitted to conduct informal inquiries concerning TSCA CBI claims consistent with 40 CFR 2.204. When an EPA employee believes it to be appropriate, he or she can request substantiation of a TSCA CBI claim from a submitter. The request should be made by letter.

EPA employees, especially compliance inspectors, are encouraged to obtain guidance for CBI reviews and challenges from the TSCA Information Management Branch. In addition, employees are encouraged to become familiar with the substantive criteria used to determine confidentiality, which are found at 40 CFR 2.208.

b. **FORMAL CHALLENGES.** The Office of General Counsel is responsible for making final determinations concerning challenges to TSCA CBI claims, pursuant to 40 CFR 2.205, with two exceptions. Before acting under these two exceptions, contact the TSCA Information Management Branch or the Office of General Counsel for advice.

- The first exception allows an EPA office to take certain actions if the office determines that the TSCA CBI claim is clearly not entitled to confidential treatment. The exception is defined in 40 CFR 2.204(d)(2); "EPA office" is defined in 40 CFR 2.201(m); the possible actions are defined in 40 CFR 2.205(f).
- The second exception allows the Office of General Counsel to delegate its authority to make final determinations concerning TSCA CBI challenges to any EPA attorney in accordance with 40 CFR 2.205(i).

c. **PROCEDURES PERFORMING A CHALLENGE.** It is incumbent upon those who challenge TSCA CBI claims to act consistently with all TSCA regulations --- particularly 40 CFR 2.201 through 40 CFR 2.205, 40 CFR 2.208, and 40 CFR 2.306--and relevant Federal Register notices. The validity of a TSCA CBI claim must be carefully considered before an EPA employee asks a submitting company to substantiate the claim. IMD and Office of General Counsel attorneys should be consulted if any questions or problems arise on TSCA CBI issues or challenges.

## **B. *MANAGER RESPONSIBILITIES***

**IN GENERAL.** All managers who are responsible for programs involving access to TSCA CBI must ensure that their staff members follow this manual's procedures and any other directive that deals with protection of TSCA CBI. Managers must also ensure that

- Adequate personnel are available to carry out the DCO responsibilities under the manager's supervision.

- Proper physical control measures are implemented in areas where TSCA CBI is maintained.
- Subordinate project officers (POs), delivery order project officers (DOPOs), and work assignment managers (WAMs) follow proper TSCA CBI security procedures while administering contracts.
- They meet quarterly with contractor project officers to ensure that contractor staff are following TSCA CBI security procedures.
- That all employees under their supervision who are required to have access to TSCA CBI maintain a current clearance for TSCA CBI access.

### ***C. DOCUMENT CONTROL OFFICER (DCO) RESPONSIBILITIES***

1. **IN GENERAL.** DCOs manage their facilities' document tracking systems and oversee the receipt, storage, transfer, and use of TSCA CBI by employees in their facilities. All facilities that are authorized for access to TSCA CBI are required to have a facility DCO and an alternate DCO, who will assume the facility DCO's responsibilities during his or her absence.

Facility DCOs must be approved and trained before TSCA CBI can be transferred to any facility. The OPPT DCO is responsible for providing training materials and guidance on appropriate document handling procedures to all DCOs.

2. **THE DCO MAINTAINS A DOCUMENT TRACKING SYSTEM.** The receipt, usage, and transfer of TSCA CBI is tracked through a document tracking system. All TSCA CBI materials submitted to EPA, and those produced by Federal and contractor employees (except as described in Chapter 4, section K), are monitored through this system.

The DCO is responsible for his or her facility's document tracking system. The DCO must ensure that:

- All manual or automated logs are properly maintained, updated and securely stored.
- Document control numbers or unique numerical identifiers are assigned to the documents requiring them.
- Proper procedures are followed when using TSCA CBI materials.

The IMD director has approved several manual and automated tracking systems for use by Federal or contractor DCOs. Use of one of these systems, which are described below, is mandatory. Contact the OPPT DCO for additional information about these tracking systems.

a. **AUTOMATED DOCUMENT TRACKING SYSTEMS.** EPA recommends that DCOs who oversee a high volume of documents and transactions use automated systems to track documents. These systems allow the DCO to track a document's movement from the time it is assigned a document control number or received at EPA until the time it is destroyed or transferred to another TSCA CBI-cleared facility.

At EPA headquarters, the OPPT DCO uses an automated system to track TSCA CBI documents: The Confidential Business Information Tracking System (CBITS). Other DCO(s) use a second automated tracking system, the Automated Document Tracking System (ADTS), to track documents at field installations.

- 1) **Machine-readable bar codes.** CBITS tracking system uses a machine-readable bar code to track TSCA CBI documents. The bar code is affixed to each TSCA CBI document controlled through the headquarters CBIC. Bar codes are also affixed to the electronic entry identification cards of employees with TSCA CBI access authorization. The OPPT DCO uses these bar codes to verify through CBITS that employees are authorized for access to TSCA CBI documents. The OPPT DCO also uses these bar codes to produce annual audit certification reports for employees' completion.
- 2) **Backup for automated document tracking systems.** When an automated TSCA CBI document tracking system is used, the facility DCO must make a backup disk whenever on a regular basis. The backup media is TSCA CBI data and should be protected as such. Any manual logs that are converted into an automated system must be retained until an audit by the TSCA security staff verifies the accuracy of the conversion.

EPA also suggests securing a duplicate set of media (document tracking system) off site to allow for recovery of accountability of documents charged out, if a disaster such as a flood, fire, or other natural disaster strikes. Contact the OPPT DCO and the TSCA Security Staff for assistance in establishing a program.
- 3) **ADTS extends monitoring capability.** ADTS runs on an IBM-compatible PC and provides automated tracking, accountability, and records-management capabilities for TSCA CBI documents stored outside the purview of the OPPT DCO. ADTS is available from the OPPT DCO.

b. **MANUAL TRACKING SYSTEMS.** Manual tracking systems are appropriate for DCOs who are responsible for a low volume of documents and transactions. Certain EPA forms must be used in implementing a manual tracking system. These forms establish the minimum tracking and control requirements for TSCA CBI assigned to facility DCOs. The forms are EPA Form 7740-10, "Receipt Log for TSCA Confidential Business Information," EPA Form 7740-11, "Inventory Log for TSCA Confidential Business Information," and EPA Form 7740-24, "Federal Agency, Congress, and Federal Court Sign Out Log" (see Appendices 15, 16, and 20, respectively).

3. **THE DCO MAINTAINS THE INVENTORY LOG.** Each DCO must maintain an inventory log for TSCA CBI transactions at his or her facility. The inventory log must contain the following information:

- The document control number.
- The date on which a document is checked out from the DCO and the date on which it is returned.
- The identity of the individual checking out the document.
- If the document will 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. **DELIVERING AND RECEIVING TSCA CBI MATERIALS.** All TSCA CBI materials sent by EPA employees or contractors through the mail or by courier must be addressed to and received by a DCO. TSCA CBI materials that are hand carried to a facility or generated by employees at the facility must be taken immediately to the DCO (see Chapter 4).

a. **THE DCO MUST REVIEW DOCUMENTS FOR COMPLETENESS.** The DCO must review all materials received to determine whether they appear complete.

- If the documents do not appear to be complete, the DCO must immediately contact the submitter to determine whether there is an omission.
- If the materials appear to be complete, the DCO must stamp the document as TSCA CBI (Appendix 12). The stamp is applied to at least the first page (or the cover, if the document has one) and the back of the last page (or back cover, if the document has one). The DCO then assigns a document control number to the document, if one has not already been assigned, and attaches a TSCA CBI cover sheet (Appendix 13) to the front of the document. The DCO must write the document control number on the first page of the document.

b. **THE DCO MUST MAINTAIN A RECEIPT LOG.** Each document received by a DCO must be recorded in an automated or manual receipt log (Appendix 15). The DCO must record the following items in the receipt log:

- The document's document control number (if a document control number has not been assigned, the copy number assigned by the DCO should be recorded).
- The date on which the document was received by the DCO.
- The 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.
- The number of pages contained in the document.



- A brief description of the document (e.g., "an engineering report on PMN-Y" or "letter from company X on PMN-W").

**5. STORAGE OF TSCA CBI MATERIALS.** DCOs are responsible for ensuring that employees at their facilities are storing documents properly. This manual establishes storage procedures in Chapter 4, section B.

The DCO supervises the storage of TSCA CBI materials in secure storage containers or in a centralized secure storage area (e.g., the CBIC at EPA headquarters). The sole exception to this is when an employee's duties require that he or she be assigned individual responsibility for a specific secure storage container(s) (i.e. Mosler safe) within an office.

**6. MAINTAINING RECORDS OF LOCK COMBINATIONS.** The facility DCO must maintain a record of the lock combinations on rooms and containers in which TSCA CBI materials are stored. The DCO must also store each combination individually in a sealed envelope. These envelopes should be opened only in emergencies.

At EPA headquarters, there are a number of facility DCOs. Their recordkeeping responsibilities break down as follows:

- Each division in OPPT has a DCO who is responsible for keeping a list of combinations for TSCA CBI storage containers and rooms controlled by the division.
- The OPPT DCO maintains a list of combinations (1) for containers and rooms assigned to IMD and (2) for all containers and rooms in OPPT that don't fall under any specific division's control.
- At EPA headquarters, DCOs in offices other than OPPT maintain a list of combinations for TSCA CBI storage containers and rooms controlled by their offices.

- FMSD keeps a master list of combinations for all TSCA CBI locks at EPA headquarters.

**7. CONDITIONS FOR CHANGING LOCK COMBINATIONS.** The DCO is required to change lock combinations (1) every 12 months, (2) each time a person who knows a combination relinquishes his or her TSCA CBI access authority, (3) when a container is put into or taken out of operation, and (4) if there is a known or possible compromise of TSCA CBI data in the container. At EPA headquarters, DCOs notify FMSD, which changes the combinations.

**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, facility DCOs must notify the OPPT DCO of any employees within their jurisdictions who should be added or deleted from the list.

**9. THE DCO MONITORS AND CONTROLS WHO OBTAINS TSCA CBI MATERIALS.** The steps for obtaining TSCA CBI materials are described below:

- The employee requests a specific TSCA CBI document from his or her DCO.
- The DCO locates the document in the TSCA CBI storage files or obtains it from a another DCO, employee, contractor, or submitter.
- The DCO notifies the employee that the document is available.
- When the employee arrives to pick up the document, the DCO verifies that the requesting employee is authorized for access to the document.
- The DCO logs the document out to the employee using an automated or manual inventory log.

**10. THE DCO MONITORS OVERDUE TSCA CBI MATERIALS.** TSCA CBI materials may not be checked out from a centralized TSCA CBI storage facility for more than one year. DCOs must monitor the inventory log for TSCA CBI materials that have not been returned within the one-year period. The DCO is responsible for notifying employees and their supervisors of overdue materials. This is done by distributing to the employee and his or her supervisor a list of all TSCA CBI documents charged out to the employee before the annual security briefing and TSCA CBI access recertification are accomplished.

If the employee does not return the overdue materials to the DCO within 30 days after notification, the DCO must assume the materials cannot be located. The DCO must notify his or her division director that the materials are lost, pursuant to the procedures in Chapter 5.

**11. 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 author (see Chapter 4, section L). The DCO's role is to provide guidance to the author in making the determination. Employees who are unable to determine whether something is confidential should consult with their supervisor or DCO. If the issue remains unresolved, the employee should consult the chief of the IMD TSCA Information Management Branch. The DCO also instructs document authors in how to sanitize a TSCA CBI document if the document is going to be released to the public.

**12. THE DCO SUPERVISES THE REPRODUCTION AND DESTRUCTION OF TSCA CBI MATERIALS.** The DCO is responsible for controlling and documenting the reproduction and destruction of TSCA CBI materials. TSCA CBI materials except for working papers as discussed in Chapter 4, can be reproduced or destroyed only by the DCO or by a DCA assigned to the task by the DCO. In the latter case, the DCO must supervise the activity. Specific procedures for reproduction and destruction are set forth in Chapter 4, sections N and O.

**13. THE DCO CONTROLS THE TRANSFER OF TSCA CBI MATERIALS BETWEEN FACILITIES.** Two procedures exist for transferring TSCA CBI materials between facilities. The first applies to materials that are already recorded in the document tracking system. If the document is in an employee's possession, the employee must first return the document to his or her facility DCO. The DCO records the date the document is being sent and the name of the DCO who will receive it in the Inventory Log. The DCO also inserts a transfer receipt in the second envelope. The transfer receipt identifies the package's contents. The recipient DCO will sign the transfer receipt and return it to the sender.

The second procedure applies to new materials that are not recorded in the document tracking system. In these cases, the document's author must stamp the document as TSCA CBI and attach a TSCA CBI cover sheet to it. The author then takes the document to his or her DCO who (1) logs the document into the receipt log, (2) assigns it a document control number, and (3) records the date the document is being sent and the name of the DCO who will receive it.

**PACKAGING AND ARRANGING TRANSFER OF TSCA CBI MATERIALS.** Specific information on packaging and arranging transfer of TSCA CBI materials is provided in Chapter 4, section F.

**14. THE DCO ASSISTS EMPLOYEES WITH OBTAINING AND MAINTAINING TSCA CBI ACCESS AUTHORITY.** DCOs are responsible for assisting employees with their TSCA CBI access authority. Procedures for this are set forth in Chapter 2.

**15. THE DCO IS RESPONSIBLE FOR ASSISTING WITH EMPLOYEE DOCUMENT AUDITS.** When an employee is undergoing TSCA CBI recertification or is terminating his or her access to TSCA CBI, the DCO must give the employee a report listing all the documents that the CBITS system, DAPSS system, and the automated or manual inventory log show as being in the employee's possession. All of the returned documents must be re-entered into the collection of records.

**16. EACH YEAR, THE CONTRACTOR DCO MUST PERFORM AN INVENTORY OF HARD-COPY TSCA CBI DOCUMENTS.** Before July 31 of each year, each contractor DCO must inventory all hard-copy TSCA CBI materials in the DCO's document tracking system.

- The DCO must compare the TSCA CBI documents in the receipt log with the transactions listed in the inventory log. This is accomplished by comparing the document control numbers.
- The DCO must inventory the documents in his or her possession. These documents are listed in the receipt log, but not in the inventory log.
- The DCO must review the status (e.g., destroyed or transferred outside the DCO's facility) and location (e.g., checked out to an employee) of materials listed in the inventory log.
- The DCO must locate any documents that have been checked out for more than one year.
- The DCO must review the status of documents indicated in the inventory log as having been destroyed.
- Prior to October 1 of each year, the DCO must submit a written inventory to his supervisor. By October 1, the supervisor must submit the report to the TSCA security staff.

**NOTE:** The procedures in Chapter 5 must be followed if there are any TSCA CBI materials that cannot be located.

**17. WHEN DCOS TERMINATE THEIR EMPLOYMENT OR RELINQUISH THEIR DCO RESPONSIBILITIES.** The procedure that must be followed when DCOs terminate their employment or relinquish DCO responsibilities are the same for DCOs at EPA headquarters, regional offices, other Federal agencies and contractor facilities.

**TSCA CBI MATERIALS MUST BE INVENTORIED.** The outgoing DCO and the incoming DCO must jointly perform an inventory of TSCA CBI materials in the outgoing DCO's collection of records. Both parties must certify 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. If any TSCA CBI materials cannot be located during the audit, the incoming DCO must follow the procedures in Chapter 5.

## **CHAPTER 4**

### **PROCEDURES FOR USING AND PROTECTING TSCA CBI MATERIALS**

All procedures discussed in this chapter apply to employees of EPA, other Federal agencies, and contractors, unless otherwise specified.

#### **A. *MARKING MATERIALS AS TSCA CBI***

1. **TSCA CBI COVER SHEETS MUST BE PLACED ON MATERIALS.** A TSCA CBI cover sheet, EPA Form 7740-9 (Appendix 13), must be affixed to all TSCA CBI hardcopy materials. All other materials (i.e., diskettes, samples, etc.) must have TSCA CBI labels attached (Appendix 23).

2. **THE PHRASE TSCA CBI MUST BE STAMPED ON MATERIALS.** TSCA CBI materials must be marked with a stamp that identifies the materials as TSCA CBI (Appendix 12). The author of the materials is responsible for stamping the document. The stamp must be placed on the front of the first page (or on the cover, if the document has one) and on the back of the last page (or back cover, if the document has one). The author may choose to stamp additional pages of the document. If the document is a copy or is received from outside EPA, the DCO is responsible for stamping the document.

## **B. PROCEDURES FOR USING TSCA CBI DOCUMENTS INSIDE OR OUTSIDE OF SECURE STORAGE AREAS**

1. **EMPLOYEE RESPONSIBILITIES, IN GENERAL.** Employees using TSCA CBI are responsible for ensuring that no unauthorized disclosure of that information occurs. One way of guarding against this is for employees to use TSCA CBI only in secure storage areas (described below). If employees take TSCA CBI outside of the secure storage areas, they must (1) maintain constant control over the TSCA CBI documents in their possession, (2) return the TSCA CBI documents to the DCO, or (3) store the documents in a TSCA CBI-approved storage container.

2. **PROCEDURES FOR USING TSCA CBI DOCUMENTS OUTSIDE OF SECURE STORAGE AREAS.** Employees who are using TSCA CBI documents outside of secure storage areas must never leave the documents where people not authorized for TSCA CBI access might gain access to them. When a TSCA CBI document outside a secure storage area is in an employee's possession and is not in use, the employee must place the document in an approved storage container.

a. **TWO TYPES OF CONTAINERS ARE APPROVED.** Two types of 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.

b. **OPEN/CLOSE SIGNS.** The employee must affix a magnetic open/close sign to each container so the status of the security container is visible at all times. The employee must place the "open" sign on a container when it is opened and the "close" sign on a container when it is closed.



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. The facility DCO is responsible for reviewing all containers under his or her purview to ensure that the proper sign is affixed to them.

c. **MORE THAN ONE PERSON CAN USE A STORAGE CONTAINER.** A storage container may be used by more than one person to store TSCA CBI materials. In these cases, each person using the storage container must be authorized for access to all types of TSCA CBI stored in the container. Each person should be assigned a separate storage space within the storage container and is responsible for any TSCA CBI that he or she stores there.

**3. PROCEDURES FOR USING TSCA CBI DOCUMENTS INSIDE SECURE STORAGE AREAS.** Facilities in which a large volume of TSCA CBI is used will usually contain one or more secure storage areas. For example, at EPA headquarters, the CBIC is a secure storage area. Secure storage areas are used as TSCA CBI work areas, storage areas for TSCA CBI, or both. Only employees who are authorized for access to TSCA CBI are allowed to enter secure storage areas; personnel who are not cleared for access to TSCA CBI must be escorted (at all times) by an employee who is cleared for access to TSCA CBI. When an employee is working in a secure storage area, it is recommended that TSCA CBI be stored in an approved container while not in use, but it is not required. The TSCA security staff is required to maintain a record of the locations of all TSCA CBI secure storage areas.

**TSCA CBI-CLEARED EMPLOYEES MUST ACCOMPANY UNAUTHORIZED PERSONS INSIDE SECURE STORAGE AREAS.** If persons not authorized for access to TSCA CBI must enter a secure storage area for any reason, they must sign a visitor's log and be accompanied at all times by a TSCA CBI-cleared employee.

### ***C. HOW TO OBTAIN APPROVAL FOR ESTABLISHING A SECURE STORAGE AREA***

The IMD director can designate secure storage areas in EPA facilities, other Federal facilities, or contractor facilities when the volume and frequency of TSCA CBI use justifies it. The steps to obtaining approval for a secure storage area are:

1. The facility DCO establishes a secure storage area that meets the security requirements established in this manual.
2. The facility DCO writes a memorandum to the OPME director asking that the TSCA security staff inspect the secure storage area and that it be approved for use. The memorandum is submitted to the DCO's division director, who sends it to the OPME director.
3. The TSCA security staff inspects the secure storage area. The staff will require security improvements, if needed.
4. After the TSCA security staff approves the secure storage area, the facility DCO must designate an employee to assume responsibility for the secured area. This employee is usually the DCO or a DCA. This employee's responsibilities include monitoring the area to ensure that only employees authorized for TSCA CBI access have access to it and ensuring that the devices that secure the area are operating properly.
5. If the secured area functions as a centralized storage area, the facility DCO will maintain the document tracking system for the materials stored in the area. (The OPPT Confidential Business Information Center (CBIC) is the central repository for TSCA CBI documents maintained at Headquarters; the CBIC is a contract operation.)

### ***D. SECURING AN AREA***

**SECURE STORAGE AREA REQUIREMENTS.** Secure storage areas must be secured by (1) a pin tumbler lock, (2) an intrusion alarm, and (3) an electronic card entry system or a changeable push-button door lock.

**1. MAINTAINING SECURITY OF LOCK COMBINATIONS.** DCOs are responsible for controlling access to lock combinations (see Chapter 3, section C.6). DCOs are allowed to disclose combinations only to employees with TSCA CBI access authorization and a need to review the TSCA CBI materials stored in the containers or rooms.

**2. ELECTRONIC CARD KEYS CAN BE USED TO ACCESS SECURE STORAGE AREAS.** Card keys are often used to ingress secure storage areas. The DCO can issue card keys to employees with TSCA CBI access authorization and a need to review the TSCA CBI materials in the secure storage area.

- Employees must use their card keys each time they enter the secure area, even if they enter the room at the same time as others. They are prohibited from loaning their card keys to other employees.
- If an employee needs to enter the secure storage area and does not have a card key or does not have it with him or her, the DCO or DCA must determine whether the individual is authorized for access to TSCA CBI. To do this, the DCO consults the TSCA CBI authorized access list. If the employee is authorized for access, the DCO must require the employee to sign a visitors' log (Appendix 14) before entry. The DCO must retain all visitors' logs for future reference.
- A person who is not authorized for access to TSCA CBI may gain entry to a secure storage area after he or she signs the visitors' log and is escorted at all times by a TSCA CBI cleared person.

## **E. PROCEDURES FOR OBTAINING TSCA CBI**

An employee who is authorized for access to TSCA CBI can obtain a TSCA CBI document

- From the CBIC or other centralized storage facility by contacting the DCO.
- From another employee within the same facility.
- From another facility through the DCO.

**1. HOW TO OBTAIN TSCA CBI FROM THE CBIC OR OTHER CENTRALIZED STORAGE FACILITY.** An employee who wants to obtain TSCA CBI materials from the CBIC (OPPT cleared employees only, other cleared personnel must have their DCO obtain the required TSCA CBI materials from the CBIC) or other centralized TSCA CBI storage facilities must do so through his or her DCO. The DCO will verify that the employee is authorized for access to TSCA CBI, and will then retrieve the requested documents from the storage facility and log them out to the requestor through the facility's document tracking system. TSCA CBI documents can be kept for up to one year or the expiration of the employee's clearance, whichever comes first. However, employees are encouraged to return documents as soon as they are no longer needed.

**a. SAFEGUARDING TSCA CBI DOCUMENTS.** Employees must safeguard all TSCA CBI documents in their possession. To meet this mandate, they are required to (1) return the TSCA CBI documents to the centralized storage

facility at the end of each day, (2) store the TSCA CBI documents in an approved storage container, or (3) work in and maintain the documents in a secure storage area.

b. **OBTAINING A RECEIPT FOR RETURNED DOCUMENTS.** It is not the responsibility of the DCO or DCA to generate a log-in receipt. When returning TSCA CBI documents, an employee can prepare a receipt (an employee may fill out EPA Form 7740-26 for this purpose and mark out the word permanent in the title of the form) for the DCO to sign and return to the employee or to the employee's designee. These receipts can smooth the reconciliation of document records that is required during the annual audit prior to TSCA CBI recertification. (Reminder to DCOs/DCAs: If you sign a receipt for documents, you must ensure that you have received the documents indicated on the form before signing.)

c. **TRANSFERRING TSCA CBI MATERIALS BETWEEN A DCO AND PERSONS UNDER HIS OR HER SUPERVISION IN A CENTRALIZED SECURE STORAGE AREA.** Transfers inside a secure storage area between a DCO and anyone whom he or she supervises are exempt from document transfer logging and loan receipt requirements provided the TSCA CBI material does not leave the centralized secure storage area.

**2. HOW TO OBTAIN TSCA CBI FROM ANOTHER EMPLOYEE WITHIN THE SAME FACILITY.** Employees who want to obtain a TSCA CBI document from its author or owner located in the same facility can request the documents directly. The author or owner must verify that the intended recipient is authorized for access to TSCA CBI. To verify TSCA CBI access, the author or owner should consult the TSCA CBI authorized access list, which is available from the facility DCO. The author or owner can transfer the materials by hand delivery or through his or her facility DCO. Materials that are delivered by hand must be given directly to the recipient. **Inter-office mail must never be used for such transfers.** TSCA CBI materials must never be left unattended in an in-box or on the recipient's desk, unless within a secured storage area.

**NOTE:** Contractor employees are restricted to transferring TSCA CBI documents through their facility DCOs.

**KEEPING RECORDS ON TRANSFERS.** If a transfer is made through the facility DCO, the DCO will record the transfer in the document tracking system. If a transfer is made by hand delivery, the owner or author of the transferred document can choose to obtain a signed loan receipt indicating that the transfer was completed (Appendix 17). These loan receipts should be retained until the documents are returned. If a document is transferred and no loan receipt is obtained, the owner or author of the document will be held responsible and accountable for the document.

Transfers between DCOs for different organizations within the same facility, e.g., transfers from the OPPT DCO to an OPPT division DCO, must be recorded in the document tracking system.

#### ***F. PROCEDURES FOR TRANSFERRING TSCA CBI TO AN EMPLOYEE AT ANOTHER FACILITY***

1. **IN GENERAL.** TSCA CBI materials can be transferred to an employee at another facility as long as that employee is authorized for access to TSCA CBI. These transfers of TSCA CBI materials must be conducted through facility DCOs, in accordance with the procedures set forth below. This ensures that the materials are properly logged out by the DCO. Before any TSCA CBI materials may be transferred to another facility, the facility DCO must notify the receiving DCO that the materials will be sent.

2. **PROCEDURES FOR TRANSFERRING TSCA CBI MATERIALS.** TSCA CBI materials can be transferred to an employee at another facility in one of four ways:

- The DCO can send the materials certified mail through the U.S. Postal Service, return receipt requested.
- The DCO can appoint a TSCA CBI-cleared employee to deliver the materials directly to the facility DCO.
- The DCO can arrange delivery by a courier or by the U.S. Postal Service Express Mail when approved by the immediate supervisor.

- The DCO can transfer the materials via facsimile (see section G of this chapter).

a. **PROCEDURES FOR SENDING OR RECEIVING TSCA CBI MATERIALS THROUGH THE U.S. POSTAL SERVICE.** An employee who wants to mail TSCA CBI material to an EPA or Federal employee must provide the material to his or her DCO. The exception to this is that OPPT employees who are mailing TSCA CBI material to a contractor employee must work through the OPPT DCO. The DCO will send the TSCA CBI material certified mail, return receipt requested. **Regular first class mail must never be used to transfer TSCA CBI.**

- 1) **TSCA CBI materials must be double-wrapped.** The DCO must double-wrap TSCA CBI that will be delivered by the U.S. Postal Service. 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 DCO and a return address. The outer wrapper should be free of any indications that the package contains TSCA CBI.
- 2) **Receipt of contents.** The DCO must include a receipt (Appendix 18) identifying the contents of the package. The Permanent Transfer Receipt for TSCA Confidential Business Information (Appendix 18), when used properly, 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 within the inner envelope. 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 recipient DCO will sign the receipt of contents and return it to the sender within five days of receipt.

b. **PROCEDURES FOR HAND DELIVERY OF TSCA CBI MATERIALS.** TSCA CBI material must be provided to the DCO for proper logging (including the preparation of EPA Form 7740-26, Permanent Transfer Receipt of TSCA Confidential Business Information) before a TSCA CBI-cleared person is permitted to hand carry the material to its destination. The person

carrying the materials must protect it at all times in accordance with the security procedures for transferring TSCA CBI as set forth in this chapter. The receiving DCO must sign EPA Form 7740-26 and return a copy to the sending DCO.

**c. PROCEDURES FOR TRANSMITTING TSCA CBI MATERIALS BY COURIER OR U.S. POSTAL SERVICE EXPRESS MAIL.** With the approval of an employee's requesting official, the DCO can use a courier service or the U.S. Postal Service Express Mail to transfer TSCA CBI materials. The general guideline for use of these services is that time must be of the essence. Unlike certified mail, neither of these services requires each person handling the package to sign for it as it changes hands.

- **TSCA CBI materials must be double-wrapped.** The DCO must double-wrap TSCA CBI that will be delivered by a courier service or by the U.S. Postal Service. 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 DCO and a return address. The outer wrapper should be free of any indications that the package contains TSCA CBI.
- **Receipts are necessary.** The DCO must include a receipt identifying the contents of the package (see page 50). The recipient DCO will sign the receipt and send it back to the sender to verify receipt and contents. The DCO must also obtain a receipt from the courier service employee who picks up the package. All receipts should be retained by the sending DCO for auditing.



d. **TRANSFER OF TSCA CBI TO INDUSTRY.** There will be occasions that industry will request a copy of their submission to the Agency which contains TSCA CBI. In order to received a copy, industry must submit a notarized letter on corporate stationary which is signed by a corporate officer indicating the person authorized to received the copy. The submission must be double wrapped as described above and is sent certified mail via the U.S. Postal Service, certified mail (indicating the person to receive the copy) return receipt requested. The Agency may also initiate correspondence with industry which includes TSCA CBI. The same procedures are required except for the notarized letter.

### **G. *PROCEDURES FOR RECEIVING AND SENDING FACSIMILES (FAXES) THAT CONTAIN TSCA CBI***

1. **PROCEDURES FOR SENDING OR RECEIVING FAXES BETWEEN PERSONS AUTHORIZED FOR ACCESS TO TSCA CBI.** The following security transmission provisions must be followed when transmitting any TSCA CBI by facsimile equipment:

- Only a DCO or DCA is permitted to send a fax containing TSCA CBI, and only a DCO or DCA is permitted to receive the transmission.
- Before a DCO or DCA sends a fax containing TSCA CBI to another DCO or DCA, the sender must verify the employee's access authority by consulting the TSCA CBI authorized access list.
- During transmission, the DCOs sending and receiving the document must completely control the fax machine. They must ensure that no one who is not cleared for TSCA CBI views the document.
- Fax machines that contain internal memory are authorized for transmission of TSCA CBI between EPA, its contractors, and other Federal agencies. After transmission is completed, the sending and receiving DCO must turn off the fax machines in order to ensure that no TSCA CBI data remains in memory.

- Transmission of TSCA CBI is restricted to individually-controlled fax machines. Fax machines located inside secure storage areas are preferred. Central fax receiving centers are not authorized to receive TSCA CBI.
- The DCO sending the fax is responsible for ensuring that the number dialed is correct by verifying the number on the fax transmission confirmation receipt. He or she must attach the receipt to the document that was faxed and place the document in the official document file.

**2. WHEN INDUSTRY OFFICIALS OR INDUSTRY SUBMITTERS REQUEST THAT TSCA CBI BE FAXED TO THEM.** Employees of EPA and of EPA contractors who are cleared for TSCA CBI can transmit TSCA CBI documents to industry officials or submitters. Prior to transmission, the employee must verify that the recipient is authorized to receive a company's TSCA CBI (industry must submit a notarized letter on corporate stationery which is signed by a corporate officer indicating the person authorized to received the copy).

The employee must notify the recipient prior to transmission that the confidentiality of the fax transmission cannot be guaranteed, that EPA's transmission lines are not secure, and that the message will not be scrambled by encryption equipment.

The employee sending the fax must completely control the fax machine and ensure that the transmission is not viewed by anyone not cleared for TSCA CBI. The sender must confirm that the fax transmission was completed successfully by obtaining the fax transmission confirmation receipt and attaching it to EPA Form 7740-12, "Memorandum of TSCA CBI Telephone Conversation" (Appendix 19). The employee must send all of these documents to the facility DCO for the official document file.

**3. WHEN AN INDUSTRY OFFICIAL OR INDUSTRY SUBMITTER ASKS TO FAX TSCA CBI TO EPA.** When someone external to EPA wants to send TSCA CBI via fax transmission, he or she must be notified that EPA can not guarantee the confidentiality of the transmission. At or prior to transmission, the employee who will receive 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 message. Immediately upon receiving the fax, the employee must provide it to the facility DCO for entry into the receipt log.

**4. WHEN AN INDUSTRY OFFICIAL OR INDUSTRY SUBMITTER REQUESTS EPA TO FAX TSCA CBI TO THEIR LOCATION.** When an industry official (including the technical contact) requests the Agency to fax TSCA CBI to their location, it is the responsibility of the sender (Agency) to notify industry (receiver) that EPA's transmission lines are not secure; that no encryption equipment will not be used to scramble the message; and that industry is responsible for guaranteeing the proper procedures have been take for safeguarding the TSCA CBI on the receiving end.

#### ***H. DISCUSSING TSCA CBI ON THE TELEPHONE***

**1. TELEPHONE CALLS WITH EMPLOYEES AUTHORIZED FOR TSCA CBI ACCESS.** Federal employees and contractor employees with TSCA CBI access authority are allowed to discuss TSCA CBI on the telephone with other Federal employees or contractor employees with TSCA CBI access authority. 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 authorized access list. The individual who initiates a discussion that includes TSCA CBI must indicate that the conversation involves TSCA CBI.

**2. TELEPHONE CALLS WITH SUBMITTERS.** Federal and contractor employees with TSCA CBI access authority are allowed to discuss TSCA CBI on the telephone with a submitter employee when all of the following conditions are met:

- The Federal or contractor employee must verify that the submitter employee is authorized by his or her company to discuss TSCA CBI. This can be done by checking the PMN technical contact block or other written documentation.
- The Federal or contractor employee must verify the identity of the submitter employee to whom he or she is speaking.
- The Federal or contractor employee must inform the submitter employee that the telephone lines are not secured.
- The Federal or contractor 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 employee.
- The Federal or contractor employee must state to the submitter employee that discussion of TSCA CBI with a TSCA CBI-cleared Federal or contractor employee on the telephone does not constitute a waiver of any claim of confidentiality.
- The Federal or contractor employee must inform the submitter employee that any further information provided in the telephone conversation can be claimed as confidential.

**TELEPHONE LOGS.** Federal and contractor employees must keep a telephone log of all phone calls with submitters. The phone log must be kept on EPA Form 7740-12, "Memorandum of TSCA CBI Telephone Conversation (Appendix 19). After every conversation with a submitter, Federal and contractor employees must provide their telephone logs to the DCO, who will log them into the document tracking system. All headquarters telephone logs for individual TSCA CBI materials must be inserted into the CBIC's official file for PMN chemicals and existing chemicals.

**3. VOICE MAIL SYSTEMS ARE NOT SECURE.** The Federal or contractor employee must under no circumstances leave messages containing TSCA CBI on voice mail.

## **I. *ELECTRONIC MAIL CANNOT BE USED TO TRANSMIT TSCA CBI***

Use of the EPA electronic mail system or any other electronic mail system to transmit TSCA CBI information is not authorized.

## **J. *USE OF TSCA CBI AT TELE-VIDEO CONFERENCES***

TSCA CBI can be displayed and discussed during tele-video conferences conducted between EPA headquarters and EPA regional offices. The employee who arranges or schedules the tele-video conference is responsible for ensuring that all TSCA CBI security procedures are followed during the conference. These procedures include the following:

- The employee must verify that everyone who attends the tele-video conference is cleared for TSCA CBI.
- The employee must ensure that both conference rooms are secured to prevent unauthorized persons from entering the conference rooms during the tele-video conference.
- The employee must arrange for use of compressed video encryption during transmission, if it is available. For information about tele-video encryption, contact the Security Officer of the EPA National Data Processing Division; telephone (919) 541-4013.

**K. PROCEDURES FOR HANDLING DOCUMENTS  
AND OTHER MATERIALS PRODUCED BY  
EMPLOYEES USING TSCA CBI DOCUMENTS**

1. **NEW TSCA CBI DOCUMENTS.** Documents and other materials produced by Federal and contractor employees using TSCA CBI documents frequently contain TSCA CBI themselves. If a newly created document contains TSCA CBI data, the document's author must stamp it as TSCA CBI, cover it with a TSCA CBI cover sheet (EPA Form 7740-9), and take it to the facility DCO to be logged into the document tracking system at the employee's facility. Personal working papers are sometimes exempt from the logging requirement (see subsection 3 of this section). The DCO will assign the new TSCA CBI document a document control number, which must be written on front of the TSCA CBI cover sheet (EPA Form 7740-9) and on the front of the first page of the document. The DCO will then enter the document into the receipt log and log the document out or retain it for storage.

2. **NEW NON-CONFIDENTIAL DOCUMENTS.** An employee who plans to produce a non-confidential document by sanitizing TSCA CBI must arrange for the chief of IMD's TSCA Information Management Branch to review the document. The employee should contact the chief at least 10 working days prior to release of the document. It is the responsibility of the TSCA Information Management Branch chief to ensure that the sanitization techniques maintain the confidentiality of the TSCA CBI data sources. (For more information, see section L of this chapter.)

3. **PERSONAL WORKING PAPERS.** The notes, outlines, and drafts belonging to an employee who is working with TSCA CBI are considered his or her personal working papers. As long as these papers remain in the employee's possession, they are exempt from logging requirements. When an employee transfers his or her personal working papers to another employee, however, certain security procedures must be followed.

**a. TRANSFERRING PERSONAL WORKING PAPERS TO ANOTHER EMPLOYEE.**

Before allowing another employee within the same facility to acquire a document that is a personal working paper, the author must take the document to his or her facility DCO. The DCO will assign a document control number to the document and log it into the document tracking system. Once the document has been logged into the system, the author can transfer it by hand delivery or through the DCO. A document that is delivered by hand must be given directly to the recipient. **Inter-office mail must never be used for such transfers.** TSCA CBI materials must not be left unattended in an in-box or on the recipient's desk, unless in a secure storage area.

**NOTE: Contractor employees are restricted to transferring TSCA CBI documents through their facility DCOs.**

**b. KEEPING RECORDS ON TRANSFERS.** If the transfer was made through the facility DCO, the DCO will record the transfer in the document tracking system. If the transfer was made by hand delivery, the owner or author of the transferred document can choose to obtain a signed loan receipt (Appendix 17) indicating that the transfer was completed. These loan receipts should be retained until the documents are returned. If a document is transferred and no loan receipt is obtained, the owner or author of the document will be held responsible and accountable for the document.

**c. PHOTOCOPYING PERSONAL WORKING PAPERS.** See N. 2. of this chapter.

**d. TRANSFERRING PERSONAL WORKING PAPERS TO A TYPIST.** A document can be provided to a typist without being logged into the document tracking system if the typist is in the author's division or equivalent office and is authorized for access to TSCA CBI. When the typist completes the job, he or she must return the typed and the original document to the author.

If the author sends the document to a typist outside of his or her division, the transfer must be logged into the document tracking system by the facility DCO. If the typist sends the document to anyone other than the author, the transfer must be logged into the document tracking system by the facility DCO.

- The author must keep a record of transfers to typists until all personal working papers and TSCA CBI materials transferred are returned.
- All the materials used in typing documents containing TSCA CBI, including word processing disks, ribbons, carbons, and waste paper, must be treated as TSCA CBI. TSCA CBI procedures must be used to store these materials and to destroy them.

e. **PROCEDURES FOR STORING PERSONAL WORKING PAPERS.** Personal working papers must be stamped as TSCA CBI, covered with a TSCA CBI cover sheet (EPA Form 7740-9), and otherwise used, stored, and handled like any other TSCA CBI document. The exception to this is that personal working papers are exempt from logging requirements as long as they remain in the possession of their author.

f. **PROCEDURES FOR DESTROYING PERSONAL WORKING PAPERS.** The author of a personal working paper is authorized to destroy such TSCA CBI documents that have never been assigned a document control number. The procedures for destroying TSCA CBI are discussed in section O of this chapter.

## **L. CREATING NON-CONFIDENTIAL MATERIALS FROM TSCA CBI DOCUMENTS**

1. **IN GENERAL.** The responsibility for determining whether documents contain TSCA CBI rests with the document's author. Until the determination is made, the author must treat materials produced from TSCA CBI documents as TSCA CBI.

2. **NON-CONFIDENTIAL DOCUMENTS.** Documents that meet any of the following conditions may be non-confidential:

- TSCA CBI data are not included in a new document or are deleted from an existing document.
- TSCA CBI data are replaced with non-confidential data or



descriptive terms (masked or aggregated data).

- The data or terms used are derived from TSCA CBI data but are not themselves confidential.
- The submitting company has dropped its claim of confidentiality for the information in the document or EPA has determined that the claim is not valid.

a. **WHEN TSCA CBI DATA ARE REPLACED WITH NON-CONFIDENTIAL DATA OR DESCRIPTIVE TERMS.** An employee who plans to produce a non-confidential document by aggregating TSCA CBI must arrange for the chief of IMD's TSCA Information Management Branch to review the document. The employee should contact the chief 10 working days prior to release of the document. It is the responsibility of the TSCA Information Management Branch chief to ensure that the aggregating techniques maintain the confidentiality of the TSCA CBI data sources.

b. **WHEN A SUBMITTING COMPANY DROPS ITS CLAIM OF CONFIDENTIALITY.** When a company drops its claim that information submitted to EPA is TSCA CBI, documents containing that information can be made available to the public. Before making a document publicly available, the document's author or his or her facility DCO must obtain a written statement from the company that the claim has been dropped and the document must be declassified (see section M of this chapter).

### ***M. PROCESS FOR DECLASSIFYING TSCA CBI MATERIALS***

**HOW TO DECLASSIFY TSCA CBI MATERIALS.** The process for declassifying TSCA CBI materials consists of five steps:

1. The employee determines that materials are no longer confidential.
2. The employee brings the materials to his or her DCO and presents the DCO with evidence that they contain no TSCA CBI. If the employee has determined from studying a document that it contains no TSCA CBI, he or she must provide a written explanation to the DCO. If the submitting company has dropped its TSCA CBI claim, the employee should present the DCO with

the submitter's written relinquishment of the claim. Further questions about whether a document contains TSCA CBI should be brought to the chief of IMD's TSCA Information Management Branch for resolution.

3. After being presented with evidence that a document contains no TSCA CBI, the DCO must cross out all TSCA CBI markings on the document and remove the document cover sheet.

4. The DCO must inscribe the document with the statement "Contains no TSCA CBI," sign the document, and date it.

5. The DCO must log the document out of the document tracking system. In the disposition box on the inventory log, the DCO must enter that the document contains no TSCA CBI.

## **N. *REPRODUCTION OF TSCA CBI MATERIALS***

1. **IN GENERAL.** Only a DCO or an employee acting under the supervision of a DCO is allowed to photocopy TSCA CBI materials. Photocopying of TSCA CBI materials should be limited to the maximum extent possible. TSCA CBI materials can be reproduced only at copying machines located in secure storage areas or in non-secure locations that the TSCA security staff has approved for TSCA CBI duplication.

2. **EMPLOYEE'S ROLE.** Employees are permitted to photocopy (at a machine which has been approved by the DCO) their personal working papers and documents for use at meetings (see section P of this chapter). In all other cases, employees must present the materials they want photocopied to the DCO or DCA. The DCO or DCA will photocopy the materials for the employee.

3. **DCO RESPONSIBILITIES.** The DCO is responsible for photocopying materials for employees. The DCO is responsible for obtaining the TSCA security staff's approval for any non-secure TSCA CBI photocopy locations at the DCO's facilities. The DCO is responsible for destroying excess or unusable copies (see section O of this chapter).

a. **CONTROL OF COPIES.** The DCO is responsible for the control of all copies of a TSCA CBI document. The cover sheet on the original must not

be copied for use with the copy. The copies must be stamped by the DCO as TSCA CBI and covered with a TSCA CBI cover sheet (EPA Form 7740-9).

The DCO must log the copies into the document tracking system and assign document control numbers or copy numbers to the copies. The copies should be marked with the same document control number as the original and with a copy number, e.g., 1 of 3, 2 of 3, 3 of 3, etc. The exception to this are personal working papers that are being photocopied for use in a meeting. (Personal working papers are discussed in section K of this chapter.)

**b. DISTRIBUTING COPIES TO OTHER EMPLOYEES.** Two options exist for distributing copies of TSCA CBI documents to other employees. The first option is that the DCO will log each copy out to the individual who is receiving it. The second option is that the DCO will log all of the copies out to the originator; the originator then loans the copies to other employees and obtains signed loan receipts (Appendix 17) indicating that the transfers were completed. These loan receipts should be retained until the documents are returned. If a document is transferred and no loan receipt is obtained, the owner or author of the document will be held responsible and accountable for the document.

**c. AUTHORIZING USE OF OTHER PHOTOCOPYING MACHINES WHEN MACHINES IN SECURE LOCATIONS BREAK DOWN.** The DCO can authorize the photocopying of TSCA CBI materials at machines outside of secure locations if all machines in locations approved for duplicating TSCA CBI materials are inoperable. During the photocopying of TSCA CBI materials, the non-secured machine must be dedicated to the task, and the DCO or DCA must directly supervise the machine. Only employees with TSCA CBI access may be present while TSCA CBI materials are being photocopied. After copying is finished, the operator must pass three blank copies through the machine to ensure that any impressions on the image surfaces of the machine have been erased. If a machine in a non-secure location malfunctions while TSCA CBI materials are being copied, the facility DCO must ensure that the machine is directly supervised by an employee with TSCA CBI access until it is repaired or that an employee with TSCA CBI access inspects the machine's paper path and image surfaces to retrieve any materials containing TSCA CBI that are caught in the machine.

## **O. PROCEDURES FOR DESTROYING TSCA CBI MATERIALS.**

1. **IN GENERAL.** The procedures for destruction of TSCA CBI materials apply to all materials containing TSCA CBI, e.g., draft documents, telephone records, typewriter ribbons, computer printouts, diskettes, tapes, microfiche, and any other TSCA CBI materials logged into a document tracking system. The procedures do not apply to personal working papers that are in the possession of their author.

### **2. WHO IS PERMITTED TO DESTROY TSCA CBI MATERIALS.**

a. **EPA AND FEDERAL EMPLOYEES.** Only the facility DCO or OPPT DCO is permitted to destroy TSCA CBI materials. Federal employees wishing to have TSCA CBI materials destroyed must take them to their facility's DCO.

b. **CONTRACTOR EMPLOYEES.** Contractor DCOs are allowed to destroy TSCA CBI materials after obtaining written permission from their EPA project officer.

3. **DESTRUCTION METHODS.** TSCA CBI materials such as papers, documents, or printouts must be shredded. All other materials, including microfiche, typewriter ribbons, and magnetic media must be burned, degaussed, or chemically destroyed. If EPA regional and field office DCOs are unable to meet these requirements for destruction of microfiche, magnetic media, and typewriter ribbons, they must institute a memorandum of understanding (MOU) with another Federal Agency who can meet the requirements or contract out the function indicating the requirements in the statement of work or work assignment.

4. **DOCUMENTING DESTRUCTION.** The destruction of a TSCA CBI document that has been entered into the document tracking system must be documented. The DCO must enter information about the destruction of the document into the inventory log (Appendix 16) and mark through the original entry in the receipt log (Appendix 15). (At one time, the DCO was required

to keep a destruction log, but that requirement has been dropped. For your convenience during audits, you may want to annotate in your receipt log that the document was destroyed, i.e. shredded).

The TSCA CBI cover sheets in use prior to May 1993 must be inscribed by the DCO with (1) the destruction date, (2) the location at which the document is destroyed, and (3) the 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 should be placed in the CBIC file for that document). The process does not apply to the TSCA CBI cover sheets that have become effective with publication of the revised manual (dated 1/93).

#### ***P. USE OR DISCUSSION OF TSCA CBI DURING MEETINGS***

1. **WHAT IS CONSIDERED A MEETING?** The procedures discussed here apply to scheduled gatherings of five or more people at which TSCA CBI is discussed. The procedures do not apply to informal discussions between a supervisor and an employee or between fewer than five employees working on a matter concerning TSCA CBI.

#### **2. PROCEDURES FOR CIRCULATING DOCUMENT COPIES AT A MEETING.**

a. **PERSONAL WORKING PAPERS.** The author of a TSCA CBI document may circulate photocopies of the document at a meeting without logging the document into the document tracking system if all of the following conditions are met:

- The author attends the meeting, ensures all personnel attending the meeting are cleared for access to TSCA CBI, and is present when the document is discussed.
- The author collects all copies of the document at the end of the meeting.
- The author submits all copies of the document for destruction after the meeting.

- The author numbers the copies (i.e., 1 of 6, 2 of 6, etc.) before distributing them and checks to make sure that all copies are returned at the end of the meeting.

b. **DOCUMENTS THAT HAVE BEEN LOGGED OUT TO AN EMPLOYEE.** An employee who has possession of a TSCA CBI document is permitted to photocopy the document and circulate the photocopies at a meeting (see section N of this chapter) if all of the following conditions are met:

- The employee attends the meeting and is present when the document is discussed.
- The employee collects all copies of the document at the end of the meeting.
- The employee submits all copies of the document for destruction after the meeting.
- The employee numbers the copies (i.e., 1 of 6, 2 of 6, etc.) before distributing them and checks to make sure that all copies are returned at the end of the meeting.
- TSCA CBI materials can be reproduced only at copying machines located in secure storage areas or in non-secure locations that the TSCA security staff has approved for TSCA CBI duplication.

### 3. **PROCEDURES FOR DISCUSSING TSCA CBI DURING MEETINGS.**

a. **MEETING CHAIRPERSON'S DUTIES.** The meeting chairperson is usually the person who has scheduled and organized the meeting. If a chairperson has not been identified, one must be selected at the beginning of the meeting. The chairperson is responsible for ensuring that only people cleared for TSCA CBI access are in the room during discussion involving TSCA CBI. If necessary, the chairperson should consult the TSCA CBI authorized access list to verify TSCA CBI clearance.

The chairperson must also secure the room at the end of the meeting. This includes cleaning all chalkboards, taking any unneeded TSCA CBI

materials to the DCO for destruction (except personal working papers), and clearing the room of any information that could lead to disclosure of TSCA CBI.

b. **RECORDS OF MEETING MUST BE TREATED AS TSCA CBI.** The chairperson must remind those who attend the meeting that they must treat as confidential any notes which contain TSCA CBI taken at the meeting. Notes taken at the meeting are considered personal working papers. They do not have to be logged into the document tracking system as long as they remain in their originator's possession. However, if the originator wants to transfer possession of the notes to someone else, the notes must be submitted to the DCO, who will assign them a document control number and log them into a document tracking system.

A meeting attendee must obtain permission from the chairperson to tape record a meeting. Such recordings may contain TSCA CBI and must be treated like any other TSCA CBI materials.

### ***Q. TRAVELING WITH TSCA CBI MATERIALS***

1. **IN GENERAL.** It is sometimes necessary for a Federal or contractor employee authorized for TSCA CBI access to carry TSCA CBI materials while traveling. If it is impractical to return to work to pick up the materials before departure or to drop them off after return, the employee can obtain permission from his or her immediate supervisor to take the materials home.

2. **MAINTAINING SECURITY FOR TSCA CBI MATERIALS WHILE TRAVELING.** Any employee who travels with TSCA CBI materials is responsible for maintaining proper security for the materials. The facility DCO must log the materials out to the employee before the employee leaves the facility.

a. **STORING TSCA CBI MATERIALS WHILE TRAVELING.** While traveling by plane or other public conveyance, the employee must keep the TSCA CBI materials in his or her possession. TSCA CBI materials cannot be checked with luggage.

If the employee is traveling by car, he or she should store TSCA CBI materials in the locked trunk en route. However, TSCA CBI materials

must never be left in the car overnight.

The most secure place to store TSCA CBI materials while traveling is with the facility DCO at the location that the employee is visiting. When this is not possible, the employee is permitted to store TSCA CBI materials overnight in a hotel safe, if the employee obtains a receipt from the hotel management. TSCA CBI materials placed in a hotel safe must be in a sealed envelope with no indications on the outside that the envelope contains TSCA CBI. If no receipt is available, the employee must keep the TSCA CBI in his or her possession.

**b. TRANSFERRING POSSESSION OF TSCA CBI MATERIALS WHILE TRAVELING.** Sometimes, an employee will be assigned to carry TSCA CBI materials for transfer to another location. After logging out the materials, the DCO at the employee's facility must double-wrap the materials for transfer (see section F.2.a. of this chapter). Immediately upon arrival at the destination, the employee must take the wrapped TSCA CBI materials to the facility DCO. The DCO will unwrap the materials and log them into the document tracking system.

## **R. *WORKING WITH TSCA CBI AT A PERSONAL RESIDENCE***

Normally, employees are not permitted to take TSCA CBI materials to their homes. Under special circumstances, such as recuperation from a long-term illness, a division director or a supervisor of equivalent authority may grant permission for an EPA employee to use TSCA CBI materials at home. The supervisor must provide a complete justification supporting the action to the IMD director. A plan for protecting the TSCA CBI materials while at the employee's residence must also be provided to the IMD director. All normal security precautions in this manual must be followed, and the TSCA security staff will inspect and approve the residence before any TSCA CBI materials are sent there.



## **S. WORKING WITH TSCA CBI MATERIALS ON COMPUTERS**

1. **IN GENERAL.** EPA takes appropriate precaution to safeguard TSCA CBI materials that are entered into or manipulated by computers. In addition to meeting the security requirements of this manual, EPA follows agency information security protection guidelines in protecting TSCA CBI materials. Any computer security plan developed for TSCA CBI information must, at a minimum, meet the requirements found in this manual.

2. **SETTING UP A LOCAL-AREA NETWORK (LAN).** A LAN, linking the personal computers of a small workgroup, can be used in the processing and storage of TSCA CBI data. For further information contact the OPPT TSCA Security Staff.

3. **USING PERSONAL COMPUTERS (PCs) TO WORK WITH TSCA CBI DATA.** TSCA CBI-cleared EPA employees, Federal employees, and contractor employees can use TSCA CBI data on a PC, subject to the restrictions in this manual.

a. **PROCEDURES FOR USING TSCA CBI DATA ON A PC.** The employee must retain exclusive control over the operation of a PC and printer while working on a PC. The employee must ensure that the PC screen is not viewed by anyone who is not authorized for access to TSCA CBI. If the employee leaves the PC for any reason, he or she must terminate the computer session as described in (d) below.

b. **PROCESSING AND STORING TSCA CBI DATA ON DISKETTES AND DETACHABLE HARD DISKS.** Diskettes and detachable hard disks are preferred for storage of TSCA CBI data. Employees can obtain diskettes for TSCA CBI storage from a local supply source using the Government credit card. An employee can use any diskette to store TSCA CBI information after labeling (see appendix 23 for label examples, the OPPT DCO will provide the label format in WordPerfect upon request) it as containing TSCA CBI.

Hard disks can be used to process and store TSCA CBI data under limited conditions:

- TSCA CBI data can be processed on a PC's fixed hard disk when the PC is located in a secure storage area.
- If an employee is working with TSCA CBI data on a PC with a fixed hard disk in an unsecured area, the employee must erase the hard disk at the end of each session and verify the erasure. To erase the hard disk, the employee must use an approved utility program at the end of each session. Contact the TSCA security staff for a list of approved utility programs.
- Detachable hard disks can be used to store TSCA CBI data, and their use is encouraged. The hard disks must be removed from the PC after each session, unless the PC is located in a secure storage area.

**c. MAINTAINING SECURITY FOR DISKETTES, MAGNETIC MEDIA, OPTICAL DISK, AND DETACHABLE HARD DISKS CONTAINING TSCA CBI DATA.** The procedures for storing TSCA CBI hard-copy materials apply to storage of diskettes, magnetic media (magnetic tape and data cartridge), optical disk, and detachable hard disks (see section B of this chapter). When disks are no longer needed or are damaged, they should be given to the DCO for destruction (see section O of this chapter).

**d. TERMINATING A TSCA CBI PC SESSION FOR PCs LOCATED OUTSIDE SECURE STORAGE AREAS.** Proper termination of a PC session involving TSCA CBI data consists of the following steps:

- 1) The employee should transfer the TSCA CBI data to a diskette, magnetic media, optical disk or detachable hard disk.
- 2) The employee should verify that the transfer was completed.
- 3) The employee should ensure that a backup file does not exist for the TSCA CBI that was processed during the session.

- 4) The employee should remove the diskette, magnetic media, optical disk or detachable hard disk from the PC.
- 5) The employee should erase the data from the hard disk using an approved program.
- 6) The employee should verify that the erasure has taken place.
- 7) The employee should turn off the PC.

**e. SECURITY PROCEDURES FOR PC PRINTOUTS OF TSCA CBI DATA.**

The security procedures for storing TSCA CBI hard-copy materials apply to storage of TSCA CBI data that is printed on a PC printer and to storage of the printer's ribbon (see section B of this chapter). **An employee using a printer with internal memory, such as a laser printer, must turn off the printer after each TSCA CBI printing session and verify that no TSCA CBI data remain in the printer's memory cache or buffer.**

**4. MINI COMPUTERS.** Mini computers can be used to process TSCA CBI data if they are approved by the TSCA security staff. To obtain approval, the facility DCO must prepare a security plan describing (a) how TSCA CBI data would be protected during processing and (b) how access to the mini computer would be restricted. The plan should be submitted to the TSCA security staff.

**SECURITY CONTROLS FOR TSCA CBI DATA ON MINI COMPUTERS.** At a minimum, the mini computer must be located inside a TSCA CBI secure storage area. Additional hardware and software controls should supplement the physical security controls. No dial-in access to this type of computer will be approved unless proper software or hardware encryption devices are in place. The security plan must adhere to all requirements of this manual. For further details, contact the TSCA security staff.

**5. SECURITY FOR TSCA CBI DATA STORED ON CONTRACTOR'S COMPUTERS.** EPA contractors cannot place TSCA CBI on a mainframe computer system, mini computer system, or shared-logic computer system without written authorization from EPA. A contractor's computer system and site must be inspected and approved by the TSCA security staff before the data can be transferred.

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

## ***T. DEVELOPMENT OF PHOTOGRAPHIC MATERIALS***

**1. PHOTOGRAPHS CAN BE CLAIMED AS TSCA CBI.** When a company claims that photographs taken during EPA inspections and plant visits are TSCA CBI, the film must be shipped to the OPPT DCO for processing and development. Processing or development by a private or commercial laboratory is prohibited.

The film should be labeled as TSCA CBI, double-wrapped, and prepared for shipment following the same procedures used for shipment of any other TSCA CBI media (see section F of this chapter). It should be sent to OPPT DCO, Information Management Division, (7407) EPA, 401 M St. S.W., Washington, D.C. 20460. The OPPT DCO will arrange for development and return photographs and negatives to employees within 30 days. If faster turnaround is required, the OPPT DCO should be contacted to arrange special handling.

**2. VIDEO TAPES CAN BE CLAIMED 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 should be handled and controlled as any other TSCA CBI material.

## **CHAPTER 5**

# **REPORTING AND INVESTIGATION OF VIOLATIONS OF PROCEDURES, LOST DOCUMENTS AND UNAUTHORIZED DISCLOSURES**

All employees who are authorized for TSCA CBI access are required to follow this manual's procedures, which secure TSCA CBI from unauthorized public disclosure. They are responsible for reporting (1) possible violations of security procedures, (2) the loss or misplacing of TSCA CBI materials, and (3) any unauthorized disclosure of TSCA CBI materials.

The security procedures in this manual are enforceable by administrative penalties, set forth in this chapter. The OPME director advises the employee's division as to the applicability of these penalties.

### ***A. EMPLOYEE REPORTING PROCEDURES***

#### **1. ORAL REPORT MUST BE MADE WITHIN ONE WORKING DAY.**

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

- TSCA CBI security procedures have been violated.
- TSCA CBI materials have been lost or misplaced.
- An unauthorized person has obtained access to TSCA CBI data.

b. Contractor employees must provide oral notice of the above to their project officer.

**2. WRITTEN REPORT MUST BE MADE WITHIN TWO WORKING DAYS.** Within two working days, the employee must follow up the oral report with a written report. EPA or Federal employees must provide the written report to their division director. Contractor employees must provide the written report to their project officer.

The written report must describe (1) the possible violation of procedures, (2) the unauthorized disclosure of TSCA CBI, or (3) the materials believed lost or misplaced. It must also include a description of any relevant circumstances or facts known by the employee.

The employee or his or her supervisor may examine files and discuss the matter with other individuals to try to determine what occurred. However, only the TSCA security staff is authorized to conduct interviews, review logs, and carry out a detailed investigation.

**EMPLOYEE'S DIVISION DIRECTOR OR PROJECT OFFICER'S DUTIES.** The employee's division director or project officer must review the employee's report and provide any additional comments or information that may be relevant. The division director or project officer must forward the report to the OPME director within two working days of receiving it. If the division director or project officer reviews the employee's report and determines that no violation of procedures, loss of TSCA CBI, or unauthorized disclosure has occurred, the division director or project officer is not required to forward the report to the OPME director.

## **B. *REVIEW AND INVESTIGATION OF EMPLOYEE'S REPORT***

The OPME director will review the employee's written report and unless the OPME director concludes that no violation of procedures, loss of TSCA CBI or unauthorized disclosure has occurred, will request an investigation by the TSCA security staff.

**1. WHEN POSSIBLE VIOLATION OF THIS MANUAL'S SECURITY PROCEDURES HAS OCCURRED.** The OPME director must notify the TSCA security staff of any alleged violation of this manual's procedures. In such a case, the OPME director will (1) direct the TSCA security staff to investigate the reported violation, and (2), after the investigation, notify the supervisors of the affected employee(s) of the range of appropriate sanctions. Supervisors are responsible for imposing sanctions.

The OPME director will also confer with the affected employee(s) supervisor(s) to identify procedures for handling, using, or storing TSCA CBI materials that will prevent recurrence of violations.

**2. WHEN TSCA CBI MATERIALS CANNOT BE ACCOUNTED FOR.** The OPME director will immediately review the employee's report of lost or misplaced TSCA CBI documents and decide whether evidence indicates that the TSCA security staff should begin an investigation.

**NOTIFICATION TO THE SUBMITTING COMPANY.** The OPME director must notify the IMD director that TSCA CBI data is missing. The OPME director must provide a written notice to the company within four working days of receiving the employee's report. The written notice must identify the lost or misplaced document and state the date on which it was discovered to be lost or misplaced.

**3. WHEN UNAUTHORIZED DISCLOSURE OF TSCA CBI MATERIALS MAY HAVE OCCURRED.** The OPME director will immediately review the employee's report that TSCA CBI may have been disclosed to someone who is not authorized for access to it. He or she will determine whether evidence indicates that the TSCA security staff should begin an investigation.

a. **NOTIFICATION TO THE SUBMITTING COMPANY.** If the TSCA security staff's investigation determines that it was likely an unauthorized disclosure occurred, the OPME Director must notify the affected company. The OPME director must provide a written notice to the company within four working days of receiving the TSCA Security Staff's report. The written notice must contain a description of the TSCA CBI that may have been disclosed and the date of the disclosure.

b. **NOTIFICATION NOT REQUIRED.** If the TSCA Security Staff's investigation determines that it was unlikely that an unauthorized disclosure occurred, no notice is required.

c. **EPA OFFICE OF INSPECTOR GENERAL.** If the TSCA security staff's investigation reveals any evidence of a knowing and willful unauthorized disclosure of TSCA CBI, the matter must be immediately transferred to the EPA Office of Inspector General.

### **C. PENALTY GUIDELINES FOR VIOLATION OF THIS MANUAL'S PROCEDURES**

The OPME director is responsible for enforcing the procedures in this chapter. It is up to him or her to assess the possible breach of TSCA CBI security or procedures and determine an appropriate action, which can include recommending administrative penalties or referral for criminal charges. Responsibility for implementing the OPME's recommended action rests with the division director of an EPA or Federal employee or, for contractor employees, with the division director who requested TSCA CBI access for the contractor.

The purpose of the penalties described in this chapter is to prevent or discourage the recurrence of violations. Penalties imposed or actions taken must be fair, consistent, and well-reasoned.

1. **DETERMINING THAT A VIOLATION HAS OCCURRED.** The OPME director reviews the employee's written report and the TSCA security staff's report on its investigation to determine whether an employee has violated this manual's procedures, lost TSCA CBI or disclosed TSCA CBI to an unauthorized person.

2. **DETERMINING AN APPROPRIATE ACTION.** If a violation has occurred, the OPME director must notify the individual's division director that a violation has occurred and explain the potential administrative penalties and corrective actions. Actions can include one or both of the following: (1) administrative penalties and (2) corrective actions.



To determine an appropriate action the relevant Director must weigh:

- The seriousness of the violation and the potential for unauthorized disclosure of TSCA CBI because of the violation.
- The degree of the employee's error.
- Whether the individual has previously committed a similar violation.
- Whether the individual has previously committed any other violation.
- The frequency with which the individual uses or handles TSCA CBI in the course of fulfilling his or her duties.

**3. CORRECTIVE ACTIONS.** The OPME director should recommend corrective actions when (1) an administrative penalty would be too severe a remedy and (2) the corrective action is likely to prevent or discourage future violations either by the individual or by other individuals.

**4. ADMINISTRATIVE PENALTIES.** The OPME director should recommend that an administrative penalty is appropriate if an individual was grossly negligent or if the individual has previously incurred a prior violation, even if the violation was not serious. Administrative penalties are listed below.

<b>NATURE OF OFFENSE</b>	<b>1ST OFFENSE</b>	<b>2D OFFENSE</b>	<b>3D OFFENSE</b>
CBI is not compromised and breach is unintentional	counseling by supervisor to oral reprimand	Oral reprimand to written suspension within same calendar year as 1st offense	1-day suspension to removal within same calendar year as 2nd offense
CBI is compromised but breach is unintentional	oral or written reprimand to 5-day suspension	1-day to 5-day suspension within same calendar year as 1st offense	7-day suspension to removal within same calendar year as 2nd offense
Deliberate procedural violation*	30-day suspension to removal	removal	

\* This category covers only deliberate procedural violations that do not result in the unauthorized disclosure of TSCA CBI. If OPME'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.

**5. CRIMINAL PENALTIES.** The OPME director must notify the EPA Inspector General if an individual willfully disclosed TSCA CBI to any person not authorized to receive it. The individual who disclosed TSCA CBI may be liable under Section 14(d) of TSCA (15 U.S.C. 2613(d) for a fine of up to \$5,000 and/or imprisonment for up to one year. In addition, disclosure of TSCA CBI or violation of the procedures cited above may subject an individual to disciplinary action with penalties ranging up to and including dismissal.

The purpose of taking a corrective action is to prevent or discourage future violations. Corrective actions may be procedural, instructional, or disciplinary in nature. Such actions include training, revision of work procedures, removal of the individual's name from the TSCA CBI authorized access list, and other options.

**6. OPME DIRECTOR CAN ALSO RECOMMEND THAT NO ACTION BE TAKEN.** The OPME director has the option of recommending that no action be taken if 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.

## INDEX

administrative penalties 7-8,71-77

aggregation of TSCA CBI 38,58-60

annual briefing 6,7,15,16,27

audit of documents ii,6-9,16-20,27-28,32-33,39,41,47

Authorized Access List 5-8,15,17,37,46,48-49,52-53,54,65,76

automated document tracking systems 5,8,16,19,31-33

backup for automated document tracking systems 33

bar codes 32-33

broken reproduction machines 61-62

CBIC v,vii,viii,1,5,32-33,36,44,45,46,47,55,63

CBITS 5,8,18-19,32,39

certified mail 49-52

challenging TSCA CBI claims 29-30,59-60

computer access authority 3-7,9,15-17,62,67-70

Congressional access 25

Congressional Access Log 25, Appendix 20

Contractors and Contractor employees i,vii,1,10-20,27-31,35,37,43,48,50,54-55,62,70,71,74

copies 60-64

copy numbers 61,64

corrective actions 74-77

couriers vii,34,49-52

creating new TSCA CBI documents 28-29,38,56-58

creating TSCA non-CBI documents 38,56,58-59

criminal penalties 1,20,23,74-77

DCO relinquishes responsibilities 40-41

declassifying TSCA CBI materials 59-60

destruction of TSCA CBI materials vii,34,38,62-63,65

Destruction Log 63

Director, Office of Pollution Prevention and Toxics vii

Division Director 10,14,22,28,38,45,67,71-74

Diskettes 43,62,67-69

Document Control Assistants v,vii,29,31-33,38-40,46-47,49,55-58,60-63,65-66

Document Control Officers (DCOs) v,vi,viii,3-9,12-22,24-25,27-41,43-53,55-63,65-66,68-70

document control numbers 32,40,61

document tracking system v,vii,29,31-33,38-40,46-47,49,55-58,60-63,65-66

double-wrapping TSCA CBI materials 50-52,66,70

electronic entry cards 9,19

electronic mail 13,21,24,55

facsimiles containing TSCA CBI, sending and receiving 52

final confidentiality determination 29-30,38,60

## forms

TSCA CBI Access Request, Agreement and Approval,  
7740-6: 3,7,17, Appendix 1  
TSCA CBI ADP User Registration, 7740-25: 4,14, Appendix 2  
Standard Form 86: Questionnaire for Sensitive Positions: i,4,14, Appendix 3  
Fingerprint chart, FD-258: 14, Appendix 4  
Request for Approval of Contractor Access to TSCA CBI,  
7740-17: 10, Appendix 6  
Contractor Information Sheet: i,12, Appendix 7  
Confidentiality Agreement for US Employees Upon  
Relinquishing TSCA CBI Access Authority,  
7740-16: 8-9, Appendix 9  
Confidentiality Agreement for Contractor Employees Upon  
Relinquishing TSCA CBI Access Authority,  
7740-18: 18, Appendix 10  
Employee Separation or Transfer Checklist,  
3110-1: 9, Appendix 11  
Receipt Log for TSCA CBI, 7710-10: i,33,35,39,40,53,56,63, Appendix 15  
Inventory log Log for TSCA CBI, 7710-11 i,6,8,16,18-20,28,33-34,37,39-  
40,60,63, Appendix 16  
Federal Agency, Congress, and Federal Court Sign-out  
Log, 7710-13: 25, Appendix 20

guiding principle 1-2

hand delivery 48-50,57

hard disks 67-68

hard-copy TSCA CBI vii,39-40,68-69

hotel safe, storage of TSCA CBI in 66

IMD Director iii,vii,10-12,14,17,20,23,25,32,45,67,73

individual access files 4,6,14,16

Inventory; inventory log Log for TSCA CBI i,6,8,16,18-20,28,33-34,37,39-  
40,60,63, Appendix 16

language, required contract 11, Appendix 8

loan receipts ii,49,57,61

local area network 67

lock combinations 9,36,46

lost documents (materials) 28,38,71-73

luggage, storage of TSCA CBI in 66

mailing TSCA CBI 13,21,24,50

maintaining access authorization 3-8,13-16,31,38-39

managers' responsibilities 30

manual tracking systems 33

manual updates 2, Appendix 21

meetings 60,63,65

meeting chairperson 65

mini computers 4,69

Minimum Background Investigation v,14

missing documents 9,19

monthly access listing 5,15

new documents 28,34-35,56

notice to affected businesses 11,20,23,25

OPPT DCO vi,vii,viii,4-10,12,14-21,31-33,36-37,49,62,68,70

other agencies, authorizing for TSCA CBI 2-3,20-24,27,40,43,52

overdue documents (materials) 28,37-38

PCs 4,67-68,70

personal working papers 56-58,60-63,65

photographic materials 70

printouts 62,69

project officer ii,vii,viii,10-14,16,19-20,72

Receipt Log i,33,35,39,40,53,56,63, Appendix 15

relinquishing TSCA CBI access authority i,8-9,18-19

reporting violations 8-9,27,71,75

reproduction of TSCA CBI materials vii,38,60-61,64

requesting officials viii,4-8,10,15-18,21-22,24

residences, use of TSCA CBI in 66-67

return of TSCA CBI to a DCO 8-9,18-20,28,43,48

return receipts 12,23,25,49-50,52

ribbons and microfiche 58,62,69

sanitizing documents 38,56

secure storage areas viii,7,9,17-18,36,43-48,52,57,60,64,68-69

security briefing 4-8,15-17,27-28,38

storage containers 9,11,19,36,43-44,48

storage of TSCA CBI materials 1,2,7,11,31,35-37,45,63,67-69

subcontractors vii,10-13

submitter drops claim 29-30,60

telephone discussion of TSCA CBI 53-55

telephone logs ii,53-55, Appendix 19

tele-video conferences 55-56

termination of access i,6-9,16-19,39

terminology vii-x



transfer of TSCA CBI between employees 7,17,48-49,57-58,65

traveling with TSCA CBI materials 65-66

TSCA CBI Labels Appendix 23

TSCA CBI Stamp i,35,39,43,56,58,61

TSCA CBI Cover Sheets i,35,39,43,56,58,60-61,63

TSCA Security Staff iii,ix,10-23,41,55,57,61-63,65,66,69,7011, 14-15,19,24-  
25,27,33,40,45-46,60-61,64,67-70,72-74

typing TSCA CBI materials 58

unaccounted for TSCA CBI materials 6,9,16,19,28,38,49,57,62,71-72

unauthorized disclosure of TSCA CBI materials 7,20,23,43,71-74,76

video-tapes 5,15-16,70

violations of this manual's procedures viii,ix,7,27,71-72,74,77

Visitors Log i,45,47

waiver for immediate access 5,15

Please read Privacy Act Statement and instructions on reverse before completing this form.

Form approved. OMB No. 2070-0075. Approval expires 01-31-95.

United States Environmental Protection Agency  
Washington, DC 20460**TSCA CBI Access Request, Agreement and Approval****Section I.-Access Request**

1. Name (Last, First, MI)	2. Social Security Number	3. Telephone Number
4. Requestor (Agency/Office/Division/Branch)	5. Document Control Officer (DCO)	6. DCO Telephone Number
7. TSCA Sections for which access is required. Check all that apply. Use blank space to request other sections not listed. ALL <input type="checkbox"/> -OR- 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 8 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 21 <input type="checkbox"/>		
8. Justification for TSCA CBI access. Select appropriate code from instructions on reverse side. (Check one or all that apply.) A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> Other <input type="checkbox"/> List Justification on reverse side		

**Section II. - Contract Information - Contractor Employees Only**

9. Employer's Name	10a. Employer's Address	10b. City	10c. ST	10d. Zipcode
11. Contract Number	12. EPA Project Officer	13. EPA Project Officer Telephone		

**Section III. - OPPT Secure Storage Area Access - HQ Federal and HQ Contractor Employees Only**

14. Check if EPA ID Badge (RUSCO-7M). Badge is required. <input type="checkbox"/> Yes (New) <input type="checkbox"/> Need Replacement <input type="checkbox"/> No (List Present EPA ID Badge Number _____ ) (List Present OPPT Barcode _____ ) OR <input type="checkbox"/> Need Barcode	
15. List OPPT Restricted areas by Division to which physical access is required. Home Division (24 hour access) <input type="checkbox"/> Other Divisions (6A.M.- 6P.M. only) <input type="checkbox"/> Access to CBIC only <input type="checkbox"/> IMD (DCO and IMD Computer Rms.) <input type="checkbox"/>	
16. List OPPT areas by Division and Room Number for which Alarm Activation/Deactivation Authority is requested.	

**Section IV. - Confidentiality Agreement**

I understand that I will have access to certain Confidential Business Information submitted under the Toxic Substances Control Act (TSCA, 15 USC 2601 et seq.). This access has been granted in accordance with my official duties relating to the Environmental Protection Agency programs.

I understand that TSCA CBI may be used only in connection with my official duties and may not be disclosed except as authorized by TSCA and Agency regulations. I have read and understand the procedures set forth in the TSCA Confidential Business Information Security Manual. I agree that I will treat any TSCA CBI furnished to me as confidential and that I will follow these procedures.

I understand that 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 not authorized to receive it. In addition, I understand that I may be subject to disciplinary action for violation of this agreement with penalties ranging up to and including dismissal.

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.

17. Signature of Employee	18. Date
---------------------------	----------

**Section V.- Requesting Official Approval**

19. TSCA CBI Security Briefing Date	20. Name and Signature of Requesting Official. (Immediate Supervisor - EPA Project Officer for Contractors) As the immediate supervisor of (or the EPA Project Officer for) the above mentioned employee, I certify he/she has successfully completed a TSCA CBI Security Briefing on the date shown.	
	Name <input type="text"/> Signature <input type="text"/>	21. Date <input type="text"/>

**Section VI.- OPPT Security Approval**

22. Date Received	24. Approved (TSCA Security Official Signature)	25. Approval Date
DCO Code <input type="text"/>	Barcode <input type="text"/>	Status Code <input type="text"/> Alarm Zones <input type="text"/>
Data Entry Date and Initials		1. <input type="text"/> 2. <input type="text"/>

### Paperwork Reduction Act Notice

The public reporting burden for this 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 Chief, Information Policy Branch (PM-223), US Environmental Protection Agency, 401 M Street, SW, 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.

### 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 (OPPT) contractors in order to carry out functions for EPA compatible with 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; 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 this system pertain.

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

### Instructions for Form Completion

#### Section I - To be completed by all

1. List Full Name
2. List Social Security Number
3. List Telephone number of person in item 1
4. List Full Acronym of Requesting Office (ie. EPA Office in which the individual works or for contractor employees, the EPA Office with whom the contract is with)
5. List the immediate Document Control Officer for the office in which the individual works
6. List the telephone number of the Document Control Officer
7. Check the TSCA Sections for which access is requested or check ALL if applicable
8. Circle the appropriate Access Justification Code

**A. 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.**

**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.**

**C. 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.**

**D. List Justification here** \_\_\_\_\_

---



---



---



---



---



---

#### Section II - To be completed by Contractor Employees only

9. List Employer's name
- 10a-d. List Employer's address
11. List Contract number
12. List EPA Project Officer's name
13. List EPA Project Officer's telephone number

#### Section III - To be completed by HQ Federal and HQ Contractor employees only

**NOTE: These procedures apply only to employees requiring access to OPPT Secure Storage areas. All others follow standard Agency procedures.**

14. Check either box a, b, c or (c&d) for EPA ID badge or Contractor Building Pass. If box c is checked, write in badge number.

**a. Yes** - Check if new employee getting first EPA ID Badge. (New programmed badge and barcode)

**b. Need Replacement** - Check if replacement ID Badge is needed (replacement badge and barcode)

**c. No** - Existing badge needs programming. List ID Badge no.

**d. Need Barcode** - Check if existing badge does not have an OPPT barcode on it. (OPPT barcodes are for logging documents out of the OPPT Confidential Business Information Center only)

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.

**Home Division** - List Division in which employee works

**Other Divisions** - List other OPPT Divisions for which unrestricted daytime access is requested

**CBIC Only** - To be checked for those who only need to access the Confidential Business Information Center.

**IMD Areas** - Employees who need to regularly access the IMD Document Control Office Suite should circle DCO in the fourth block. Only IMD staff and contractors who work in IMD computer rooms should circle IMD Computer Rooms.

16. List OPPT areas by Division and Room numbers for which Alarm Activation/Deactivation authority is requested. Generally, this is employees home Division only.

#### Section IV - To be completed by all

17. Employee Signature (must be original)

18. Signature Date

#### Section V - To be completed by all

19. Enter date employee attended TSCA CBI Security Briefing
20. Immediate Supervisor/EPA Project Officers name and sign.
21. Date of signature

#### Section VI - To be completed by OPPT Security

---



---



---

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** - This section contains a collection of hardware and systems to access. Each registration form allows users to request access to two Mainframe and two LAN. Each hardware type is identified by a code which should be entered in this section. Use the list below to assist you 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.

# Questionnaire for Sensitive Positions (For National Security)

Read this information carefully. Follow the instructions fully or we cannot process your form.

## Why do we need the information you will give us and how will we use it?

The U.S. Government has conducted background investigations for over 50 years. It does this to establish that applicants for or incumbents in sensitive positions, either employed by the Government or working for the Government under contract, are eligible for a required security clearance or for performing sensitive duties. We use the information from this form primarily as the basis for an investigation that will be used to determine your eligibility for a national security position.

The information you give us is for Official Use Only; we will protect it from unauthorized disclosure. Authorized disclosures include the Privacy Act Routine Uses shown on this form. The information you provide in response to question 25a on use of illegal drugs will not be provided for use in any criminal proceedings against you.

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 clearance prospects.

## What authority do we have to ask you for the information requested on this form?

The U.S. Government is authorized to ask for this information under Executive Order 10450; section 2165 of title 42, U.S. Code; parts 5, 732, and 736 of Title 5, Code of Federal Regulations, and other statutes authorizing background investigations. We ask for your Social Security number to keep our 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.

## What is the investigative process?

Background investigations for national security are conducted to develop information to show whether or not a person is reliable, trustworthy, of good conduct and character, and loyal to the United States. The information you provide on this form, including any specific agency instructions of Question 14c., and any other special instructions, is confirmed by investigation. Your current employer must be contacted, even if you indicated on your SF 171, or other form, that you do not want the present employer contacted. In addition to the questions on this form, inquiry also is made about a person's adherence to security requirements, mental or health disorders, dishonest conduct, sexual misconduct, vulnerability to blackmail or coercion, falsification, misrepresentation and any other behavior, activities, or associations that tend to show the person is not reliable, trustworthy, or loyal.

An interview with you is a normal part of the investigative process. This Personal Subject Interview is generally the first step in the investigation, and is conducted under oath, affirmation, or unsworn declaration. It provides you the opportunity to update, clarify, and explain more completely information on your form, which often helps to complete your investigation faster.

If your investigation requires a Personal Subject Interview, you will be contacted in advance by telephone or mail to arrange a time and location for the interview. It is important that the interview be conducted as soon as possible after you are contacted. Postponements will delay the processing of your investigation. Declining an interview 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.

Documents that verify any significant claims or activities may also be requested, for example: alien registration; naturalization certificate; originals or certified copies of college transcripts or degrees; high school diploma; professional license(s) or certificate(s); military discharge certificate(s) (DD Form 214); marriage certificate(s); passport; and/or business license(s). You also may be asked to bring documents that pertain to information provided in your answers to questions on the form or other matters requiring specific attention. These matters include: termination or discharge from employment; delinquent loans or taxes, bankruptcy, judgments, liens, or other financial obligations; and arrests, convictions, probation and/or parole.

## Who makes a final determination?

Final determination on your eligibility for a national security position and your being granted a clearance is the responsibility of the OPM or the Federal agency that requested your investigation. You may be provided the opportunity to personally explain, refute, or clarify any information before a final decision is made.

## How is this form organized?

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 alcohol consumption. In answering Part 2, you should keep in mind that your answers to questions are considered together with the information obtained in the investigation to reach an appropriate adjudication for a sensitive position.

## What are the penalties for inaccurate or false statements?

The U.S. Criminal Code provides that knowingly falsifying or concealing a material fact is a felony which may result in fines of up to \$10,000, or 5 years imprisonment, or both. In addition, Federal agencies generally fire, do not grant clearance, or disqualify individuals who have materially and deliberately falsified these forms, and this remains a part of our 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 security clearance. Your prospects of placement or clearance are better if you answer all questions truthfully and completely. In the course of an interview with a Federal official you will have

adequate opportunity to explain any information you give us on the form and make your comments part of the record.

### How is the SF 171 used with this form?

For competitive civil service positions, a copy of the Application for Federal Employment (SF 171), or a form provided to you, will be attached to the SF 86. For certain other and contractor positions, the SF 171 is not required. You will be advised by the office assisting you.

### How is this form filled out?

1. Follow the instructions of the person who gave you the form and any other supplementary information 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 ink, the original and each copy you submit.

2. You will need a continuation sheet(s), SF 86A, if in the last 15 years you have lived in more than 6 residences, attended more than 3 schools, or had more than 7 employments/self-employments/unemployments.

If additional space is needed, 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.

3. Type or legibly print your answers. We cannot accept your form if it is not legible.

4. You must use the State codes (abbreviations) listed in the box below when you fill out your form.

5. The 5-digit postal ZIP codes are needed to speed the processing of your investigation. The office that provided you with the form will assist you in completing the ZIP codes.

6. 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.

7. When providing dates, you may use numbers 1-12 to indicate months if you don't believe you have enough space to write the month; and for the same reason, for year you may show the last two numbers in the year. For example, June 8, 1967, could be shown as 6/8/67, or January 1984 could be shown as 1/84.

If you have any questions, call the office that gave you the form. Be sure to sign and date the certification statement on page 9 and complete the release on page 10. Any forms that are not completed according to these instructions will be returned. This will delay the processing of your case.

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	Wisconsin	WI
Florida	FL	Maine	ME	New Hampshire	NH	Rhode Island	RI	West Virginia	WV
Georgia	GA	Maryland	MD	New Jersey	NJ	South Carolina	SC	Wyoming	WY
American Samoa	AS	Dist. of Columbia	DC	Guam	GU	Northern Marianas	CM	Puerto Rico	PR
Trust Territory	TT	Virgin Islands	VI						

### PRIVACY ACT ROUTINE USES

This record and information in this record may be used in disclosing information:

- To designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government, having a need to evaluate qualifications, suitability, and loyalty to the United States Government and/or a security clearance or access determination;
- To designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government, and the District of Columbia Government, when such agency, office, or establishment conducts an investigation of the individual for purposes of granting a security clearance, or for the purpose of making a determination of qualifications, suitability, or loyalty to the United States Government, or access to classified information or restricted areas;
- To designated officers and employees of agencies, offices, and other establishments in the executive, judicial, or legislative branches of the Federal Government, having the responsibility to grant clearances, to make a determination regarding access to classified information or restricted areas, or to evaluate qualifications, suitability, or loyalty to the United States Government, in connection with performance of a service to the Federal Government under a contract or other agreement;
- To intelligence agencies for use in intelligence activities;
- To any source from which information is requested in the course of an investigation, 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;
- To the Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order where

there is an indication of a violation or potential violation of civil or criminal law or regulation:

- To an agency, office, or other establishment in the executive, legislative, or judicial branches of the Federal Government, or the District of Columbia Government, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency;
- To Federal agencies as a data source for management information through the production of summary descriptive statistics and analytical studies in support of the functions for which the records are maintained or for related studies;
- To a congressional office in response to an inquiry made at the request of that individual;
- In litigation before a court or in an administrative proceeding being conducted by a Federal agency;
- To the National Archives and Records Administration for records management inspections;
- To the Office of Management and Budget in connection with private relief legislation;
- To respond to a request for discovery or for appearance of a witness; and
- To the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, or the Federal Labor Relations Authority, in connection with functions vested in those agencies.

### Public Burden Information

Public burden reporting for this collection of information is estimated to vary from 30 minutes to 180 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 6410, Washington, D.C. 20415; and to the Office of Management and Budget, Paperwork Reduction Project (3206-0007), Washington, D.C. 20503. Do not send your completed form to the addresses in this box.

Standard Form 86

Revised December 1990

U.S. Office of Personnel Management

FPM Chapter 732

# **QUESTIONNAIRE FOR SENSITIVE POSITIONS (For National Security)**

Form approved:  
O.M.B. No. 3206-0007  
NSN 7540-00-634-4036  
86-110

## **Part 1**

OPM  
USE  
ONLY

Codes

Case Number

*Agency Use Only (Complete items A through P using instructions in FPM Supplement 296-33)*

**A** Type of Investigation ☐ **B** Extra Coverage ☐ **C** Sensitivity Level ☐ **D** Access ☐ **E** Nature of Action Code ☐ **F** Date of Action ☐ Month ☐ Day ☐ Year ☐

**G** Geographic Location ☐ **H** Position Code ☐ **I** Position Title ☐

**J** SON ☐ **K** Location of Official Personnel Folder ☐ None ☐ Other Address ☐ ZIP Code ☐

**L** SOI ☐ **M** Location of Security Folder ☐ None ☐ Other Address ☐ ZIP Code ☐

**N** OPAC-ALC Number ☐ **O** Accounting Data and/or Agency Case Number ☐

**P** Requesting Official ☐ Name and Title ☐ Signature ☐ Telephone Number ☐ FTS ( ) Date ☐

Persons completing this form should begin with the questions below. Please type or print your answers.

**1 FULL NAME** • If you have only initials in your name, use them and State (IO). • If you are a "Jr.," "Sr.," "II," etc., enter this in the box after your middle name. **2 DATE OF BIRTH**

Last Name ☐ First Name ☐ Middle Name ☐ Jr., II, etc. ☐ Month ☐ Day ☐ Year ☐

**3 PLACE OF BIRTH** • Use the two letter code for the State. **4 SOCIAL SECURITY NUMBER**

City ☐ County ☐ State ☐ Country (if not in the United States) ☐

**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.

Name ☐ Month/Year ☐ To ☐ Name ☐ Month/Year ☐ To ☐

Name ☐ Month/Year ☐ To ☐ Name ☐ Month/Year ☐ To ☐

**6 OTHER IDENTIFYING INFORMATION** Height (feet and inches) ☐ Weight (pounds) ☐ Hair Color ☐ Eye Color ☐ Sex (mark one box) ☐ Female ☐ Male

**7 TELEPHONE NUMBERS** Work (include Area Code and extension) ☐ Home (include Area Code) ☐

( ) Day ☐ ( ) Night ☐ ( ) Day ☐ ( ) Night ☐

**8 CITIZENSHIP** **a** Mark the box at the right that applies to you and follow the instructions next to the box you marked.

☐ I am a U.S. citizen by birth in the U.S. Answer Items b and d

☐ I am a U.S. citizen, but I was NOT born in the U.S. Answer Items b, c, and d

☐ I am not a U.S. citizen. Answer Items b and e

**b** Your Mother's Maiden Name ☐

**C 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 ☐

**d 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 ☐

**e 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 of Citizenship ☐



**9 WHERE YOU HAVE LIVED**

Fill in your full address for every place you have lived beginning with the present (#1) and working backward 15 years.

- If you attended school away from your permanent residence, list the address you lived at while attending school.
- For any address in the past 3 years:
  - List a person who knew you at that address, preferably someone who still lives in that area.
  - If address listed is "General Delivery," a Rural Route, or Star Route, provide directions for locating the residence on an attached continuation sheet, and show the block #.

<b>#1</b>	Month/Year Month/Year	Street Address	Apt. #	City (Country)	State	ZIP Code
Present	To					
Name of Person Who Knows You		Street Address	Apt. #	City (Country)	State	ZIP Code
		Telephone Number ( )				
<b>#2</b>	Month/Year Month/Year	Street Address	Apt. #	City (Country)	State	ZIP Code
	To					
Name of Person Who Knows You		Street Address	Apt. #	City (Country)	State	ZIP Code
		Telephone Number ( )				
<b>#3</b>	Month/Year Month/Year	Street Address	Apt. #	City (Country)	State	ZIP Code
	To					
Name of Person Who Knows You		Street Address	Apt. #	City (Country)	State	ZIP Code
		Telephone Number ( )				
<b>#4</b>	Month/Year Month/Year	Street Address	Apt. #	City (Country)	State	ZIP Code
	To					
Name of Person Who Knows You		Street Address	Apt. #	City (Country)	State	ZIP Code
		Telephone Number ( )				
<b>#5</b>	Month/Year Month/Year	Street Address	Apt. #	City (Country)	State	ZIP Code
	To					
Name of Person Who Knows You		Street Address	Apt. #	City (Country)	State	ZIP Code
		Telephone Number ( )				
<b>#6</b>	Month/Year Month/Year	Street Address	Apt. #	City (Country)	State	ZIP Code
	To					
Name of Person Who Knows You		Street Address	Apt. #	City (Country)	State	ZIP Code
		Telephone Number ( )				

**10 WHERE YOU WENT TO SCHOOL**

Fill in information about schools you have attended, beyond Junior High School, beginning with the most recent (#1) and working backward 15 years. Also list College or University degrees received beyond 15 years.

- For schools you attended in the past 3 years, list a person who knew you at school (such as an instructor or a student).
- For correspondence schools and extension classes, list records location address.
- In the "Code" block, use one of these codes: 1 - High School      2 - College/University      3 - Vocational/Trade School

<b>#1</b>	Month/Year Month/Year	Code	Name of School	Degree/Diploma/Other (show each degree and date received if Code 2)	Month/Year
	To				
Street Address and City (Country) of School					State ZIP Code
					( )
Name of Person Who Knew You		Street Address and City (Country)		State	ZIP Code
				Telephone Number	( )
<b>#2</b>	Month/Year Month/Year	Code	Name of School	Degree/Diploma/Other (show each degree and date received if Code 2)	Month/Year
	To				
Street Address and City (Country) of School					State ZIP Code
					( )
Name of Person Who Knew You		Street Address and City (Country)		State	ZIP Code
				Telephone Number	( )
<b>#3</b>	Month/Year Month/Year	Code	Name of School	Degree/Diploma/Other (show each degree and date received if Code 2)	Month/Year
	To				
Street Address and City (Country) of School					State ZIP Code
					( )
Name of Person Who Knew You		Street Address and City (Country)		State	ZIP Code
				Telephone Number	( )

Enter your Social Security Number before going to the next page →

**Fill in your employment activities, beginning with the present (#1) and working backward 15 years. INCLUDE:**

- IN THE NUMBERED ACTIVITY SECTION USE ONE OF THESE CODES IN THE CODE BLOCK:**

- FOR EACH ACTIVITY SECTION, provide information requested. For example, if you had worked at XY Plumbing in Denver, CO, for 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 in the appropriate blocks below that information. (For locations outside the U.S., show city and country.)**

PREVIOUS PERIODS OF THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

[illegible]

PREVIOUS PERIODS OF THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

<u>Month</u>	<u>Year</u>	<u>Code</u>	<u>Employer's Name/Military Service/Employment or Self-Employment Verifier</u>

PREVIOUS PERIODS OF THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

**YOUR EMPLOYMENT ACTIVITIES (Continued)**

<b>#4</b>	Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
	To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

Month/Year	Month/Year	Your Position Title & Supervisor's Name	Month/Year	Month/Year	Your Position Title & Supervisor's Name
To			To		
To			To		

<b>#5</b>	Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
	To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

Month/Year	Month/Year	Your Position Title & Supervisor's Name	Month/Year	Month/Year	Your Position Title & Supervisor's Name
To			To		
To			To		

<b>#6</b>	Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
	To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

Month/Year	Month/Year	Your Position Title & Supervisor's Name	Month/Year	Month/Year	Your Position Title & Supervisor's Name
To			To		
To			To		

<b>#7</b>	Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
	To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

Month/Year	Month/Year	Your Position Title & Supervisor's Name	Month/Year	Month/Year	Your Position Title & Supervisor's Name
To			To		
To			To		

Enter your Social Security Number before going to the next page

--	--	--	--	--	--	--	--	--	--

**12 PEOPLE WHO KNOW YOU WELL**List **two people** who know you well and live in the United States.

• Don't list spouse, other relatives, or former spouses.

• Try not to list anyone mentioned in item 9, 10, or 11.

Name #1		Number Years Known	Telephone Number: ( ) Day ( ) or Night ( )	
Home Address		City (Country)	State	ZIP Code
Name #2		Number Years Known	Telephone Number: ( ) Day ( ) or Night ( )	
Home Address		City (Country)	State	ZIP Code

**13 YOUR OUTSIDE ACTIVITIES**

List any activities which you may wish to have considered as reflecting favorably on your reputation for leadership, responsibility, honesty, and integrity in the last 15 years. (Response Optional)

Month/Year	Month/Year	Activity	Location of Activity	
			City (Country)	State
#1	To			
#2	To			
#3	To			

**14 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. In the last 15 years, have you had continuing contact with a national of any foreign country designated by the agency instructing you to fill out this form? (NOTE: If the agency wants you to answer this question, it will provide you with a list of countries.)

Yes	No

If you answered "Yes" to a, b, or c, explain in the space below:

**15 FOREIGN COUNTRIES YOU HAVE VISITED**

List foreign countries you have visited, beginning with the most current (#1) and working backward 15 years.

• Do not include countries covered in items 9, 10, and 11.

• In the "Code" block, use one of these codes: 1 - Business

2 - Pleasure

3 - Education

4 - Other

Month/Year	Month/Year	Code	Country	Month/Year	Month/Year	Code	Country
#1	To			#3	To		
#2	To			#4	To		

**16 YOUR MILITARY HISTORY**

- a. Have you served in the United States military? .....
- Have you served in the United States Merchant Marine? .....
- If your answer to both questions is "No," GO TO QUESTION 17.
- If your answer to either question is "Yes," GO TO b.

Yes	No

- b. Starting with the most current (#1) and working backward, enter information for all periods of active service into the table below.

• Mark "O" block for Officer or "E" block for Enlisted.

• In the "Code" block, use one of these codes:

1 - Air Force 2 - Army 3 - Navy 4 - Marine Corps 5 - Coast Guard 6 - Merchant Marine 7 - National Guard

Month/Year	Month/Year	Code	Service/Certificate #	O	E	Status (Mark "X" in appropriate blocks - use State Code for National Guard)					
						None	Active Duty	Active Reserve	National Guard (show State)	Inactive Reserve	Retired
#1	To										
#2	To										
#3	To										
#4	To										

Enter your Social Security Number before going to the next page

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

1 - Mother (first)	4 - Stepfather	7 - Stepchild	10 - Stepbrother	13 - Half-sister	16 - Guardian
2 - Father (second)	5 - Foster parent	8 - Brother	11 - Stepsister	14 - Father-in-law	
3 - Stepmother	6 - Child (adopted also)	9 - Sister	12 - Half-brother	15 - Mother-in-law	

Page 6

## TSCA CBI Security Manual

Standard Form 86  
Revised December 1990  
U.S. Office of Personnel Management  
FPM Chapter 732

**QUESTIONNAIRE FOR  
SENSITIVE POSITIONS  
(For National Security)**

Form approved  
O.M.B No 7206-0007  
NSN 7540-01-634-4026  
86-110

## Part 2

## 20 YOUR SELECTIVE SERVICE RECORD

- 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.

Yes	No

**Registration Number**

### Legal Exemption Explanation

## 21 YOUR MILITARY RECORD

- a. Have you ever received other than an honorable discharge from the military? If "Yes," provide:  
**Date of Discharge (Month and Year):** \_\_\_\_\_ **Type of Discharge:** \_\_\_\_\_
- b. Have you ever been subject to court-martial or other disciplinary proceedings under the Uniform Code of Military Justice? If "Yes," list any disciplinary proceedings in the last 15 years and all courts-martial. (Include non-judicial and Captain's mast, etc.)

Yes	No

Month/Year	Charge or Specification / Action Taken	Place (City and county/country if outside the United States)	State

## 22 YOUR EMPLOYMENT RECORD

Has any of the following happened to you in the last 15 years? If "Yes," begin with the most recent occurrence and go backward, providing date fired, quit, or left, and other information requested.

Yes	No

**Use the following codes and explain the reason your employment was ended:**

- 1 - Fired from a job  
2 - Quit a job after being told you'd be fired  
3 - Left a job by mutual agreement following allegations of misconduct  
4 - Left a job by mutual agreement following allegations of unsatisfactory performance  
5 - Left a job for other reasons under unfavorable circumstances

Month/Year	Code	Specify Reason	Employer's Name and Address	State	ZIP Code

**23 YOUR POLICE RECORD** (Do not include anything that happened before your 16th birthday.)

- a. Have you ever been charged with or convicted of any felony offense?
- 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 5 years, have you been arrested for, charged with, or convicted for any offense(s) not listed in response to a, b, c, or d above? (Leave out traffic fines of less than \$100.)

	Yes	No

**If you answered "Yes" to a, b, c, d, or e above, explain your answer(s) in the space provided.**

Month/Year	Offense	Action Taken	Law Enforcement Authority or Court (City and county/country if outside the U.S.)	State	ZIP Code

## 24 YOUR MEDICAL RECORD

- a. Have you experienced problems on or off the job because of any emotional or mental condition?**
- b. Have you ever seen a health care professional for any of the types of problems mentioned above?**

	Yes	No

**If you answered "Yes" to questions a or b, explain below.**

Month/Year	Month/Year	Explanation
To		
To		

**Enter your Social Security Number before going to the next page**

[illegible]

**25 ILLEGAL DRUGS AND ALCOHOL**

Yes No

- a. In the last 5 years, have you used, possessed, supplied, or manufactured any illegal drugs? When used without a prescription, illegal drugs include marijuana, cocaine, hashish, narcotics (opium, morphine, codeine, heroin, etc.), stimulants (cocaine, amphetamines, etc.), depressants (barbiturates, methaqualone, tranquilizers, etc.), hallucinogenics (LSD, PCP, etc.). (NOTE: The information you provide in response to this question will not be provided for use in any criminal proceedings against you.)

- b. Have you experienced problems (disciplinary actions, evictions, formal complaints, etc.) on or off a job from your use of illegal drugs or alcohol?

If you answered "Yes" to question a or b above, provide information relating to the types of substance(s), the nature of the activity, and any other details relating to your involvement with illegal drugs or alcohol. Include any treatment or counseling received.

Month/Year	Month/Year	Type of Substance	Explanation
To			
To			
To			

**26 YOUR INVESTIGATIONS RECORD**

Yes No

- a. Has the United States Government ever investigated your background? 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.

Codes for Investigating Agency				Codes for Security Clearance Received			
1 - Defense Department	4 - FBI			0 - Not Required	3 - Top Secret	6 - Q-Nonresponsive	
2 - State Department	5 - Treasury Department			1 - Confidential	4 - Sensitive Compartmented Information	7 - L	
3 - Office of Personnel Management	6 - Other (Specify)			2 - Secret	5 - Q-Sensitive	8 - Other	
Month/Year	Agency Code	Other Agency	Clearance Code	Month/Year	Agency Code	Other Agency	Clearance Code

- 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.

Yes No

Month/Year	Department or Agency Taking Action	Month/Year	Department or Agency Taking Action

**27 YOUR FINANCIAL RECORD**

Yes No

- a. In the last 5 years, have you, or a company over which you exercised some control, filed for bankruptcy, been declared bankrupt, been subject to a tax lien, or had legal judgment rendered against you for a debt? If you answered "Yes," provide date of initial action and other information requested below.

Month/Year	Type of Action	Name Action Occurred Under	Name/Address of Court or Agency Handling Case	State	ZIP Code

- b. Are you now over 180 days delinquent on any loan or financial obligation? Include loans or obligations funded or guaranteed by the Federal Government. (If an SF 171, Application for Federal Employment, will be attached, you do not need to repeat Federal Government delinquencies. See the instructions headed, "How is the SF 171 used with this form?")

Yes No

If you answered "Yes," provide the information requested below:

Month/Year	Type of Loan or Obligation and Account #	Name/Address of Creditor or Obligor	State	ZIP Code

Enter your Social Security Number before going to the next page

→ | | | - | | | - | | |

**28 YOUR ASSOCIATION RECORD**

- a. In the last 15 years, have you been an officer or a member or made a contribution to an organization dedicated to the violent overthrow of the United States Government and which engages in illegal activities to that end, knowing that the organization engages in such activities with the specific intent to further such activities?
- b. In the last 15 years, have you knowingly engaged in any acts or activities designed to overthrow the United States Government by force? If you answered "Yes" to a or b, explain in the space below:

Yes	No

**Continuation Space**

Use the continuation sheet(s) (SF 86A) for additional answers to questions 9, 10, and 11. Use the space below to continue answers to all other questions and any information you would like to add. If more space is needed than what is provided below, use a blank sheet(s) of paper. Start each sheet with your name and Social Security Number. Before each answer, identify the number of the question.

After completing Parts 1 and 2 of this form and any attachments, you should review your answers to all questions to make sure the form is complete and accurate, and then sign and date the following certification and sign and date the release on page 10. If you attach an SF 171, Application for Federal Employment, make sure that it is updated and that any information added to the SF 171 is initialed and dated.

**Certification That My Answers Are True**

I read each question asked of me and understood each question. My statements on this form, and any attachments to this form, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both.

Signature (Sign in Ink) \_\_\_\_\_ Date \_\_\_\_\_

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 U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, and any authorized Federal agency, to obtain any information relating to my activities from schools, residential management agents, employers, criminal justice 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, and criminal history record information.

**I Understand** that, for financial or lending institutions, medical institutions, hospitals, health care professionals, and other sources of information, a separate specific release will or may be needed, and I may be contacted for such a release at a later date.

**I Further Authorize** the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, and any other authorized agency, to request criminal record information about me from criminal justice agencies for the purpose of determining my eligibility for, assignment to, or retention in, a sensitive position, in accordance with 5 U.S.C. 9101.

**I Authorize** custodians of records and 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 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 two (2) years from the date signed.

Signature (Sign in Ink)		Full Name (Type or Print Legibly)		Date Signed	
Other Names Used				Social Security Number	
Current Address (Street, City)				State	ZIP Code
				Home Telephone Number (Include Area Code)	
				( )	

CONTINUATION SHEET FOR QUESTIONNAIRES  
SF 86, SF 85P, AND SF 85For use with the SF 86, Questionnaire for Sensitive Positions (for National Security);  
SF 85P, Questionnaire for Public Trust Positions;  
and SF 85, Questionnaire for Non-Sensitive Positions

INSTRUCTIONS: Use this form to continue your answers to "Where You Have Lived" and/or "Your Employment Activities." Follow the instructions on the form for the particular questions you are answering and give information in the same sequence. Use as many continuation sheets as you need to furnish all the requested information.

Your Name	Your Social Security Number																		
-----------	-----------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

## WHERE YOU HAVE LIVED (Continued)

Month/Year To	Month/Year To	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 To	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 To	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 To	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 To	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 To	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												

## YOUR EMPLOYMENT ACTIVITIES (Continued)

Month/Year To	Month/Year To	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title															
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

Month/Year To	Month/Year To	Your Position Title & Supervisor's Name	Month/Year To	Month/Year To	Your Position Title & Supervisor's Name

Month/Year To	Month/Year To	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title															
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #

Month/Year To	Month/Year To	Your Position Title & Supervisor's Name	Month/Year To	Month/Year To	Your Position Title & Supervisor's Name

**YOUR EMPLOYMENT ACTIVITIES (Continued)**

Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #**

Month/Year	Month/Year	Your Position Title & Supervisor's Name		Month/Year	Month/Year	Your Position Title & Supervisor's Name	
To				To			
To				To			

Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #**

Month/Year	Month/Year	Your Position Title & Supervisor's Name		Month/Year	Month/Year	Your Position Title & Supervisor's Name	
To				To			
To				To			

Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #**

Month/Year	Month/Year	Your Position Title & Supervisor's Name		Month/Year	Month/Year	Your Position Title & Supervisor's Name	
To				To			
To				To			

Month/Year	Month/Year	Code	Employer's Name/Military Service/Unemployment or Self-Employment Verifier	Your Position Title		
To						
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 THE SAME ACTIVITY AND LOCATION - IF CONTINUATION SHEET IS USED, SHOW BLOCK #**

Month/Year	Month/Year	Your Position Title & Supervisor's Name		Month/Year	Month/Year	Your Position Title & Supervisor's Name	
To				To			
To				To			

Enter your Social Security Number



Standard Form 86A (Back)

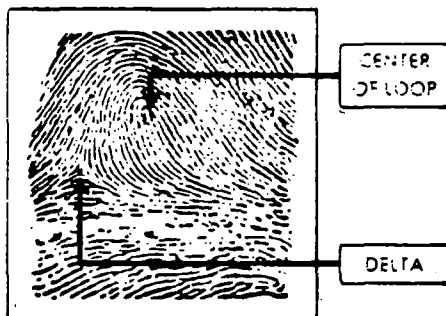
December 1990

**RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY**

**FEDERAL BUREAU OF INVESTIGATION  
UNITED STATES DEPARTMENT OF JUSTICE  
WASHINGTON, D.C. 20537**

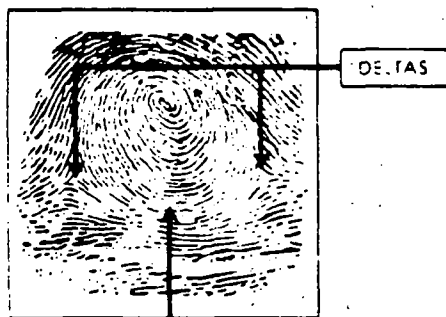
**APPLICANT**

**1. LOOP**



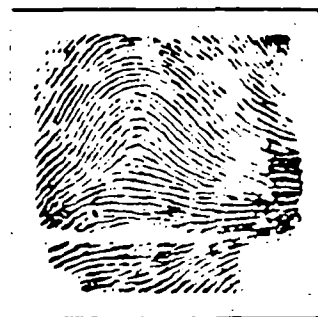
THE LINES BETWEEN CENTER OF LOOP AND DELTA MUST SHOW

**2. WHORL**



THESE LINES RUNNING BETWEEN DELTAS MUST BE CLEAR

**3. ARCH**



ARCHES HAVE NO DELTAS

**TO OBTAIN CLASSIFIABLE FINGERPRINTS:**

1. USE BLACK PRINTER'S INK
2. DISTRIBUTE INK EVENLY ON INKING SLAB
3. WASH AND DRY FINGERS THOROUGHLY
4. ROLL FINGERS FROM NAIL TO NAIL AND AVOID ALLOWING FINGERS TO SLIP
5. BE SURE IMPRESSIONS ARE RECORDED IN CORRECT ORDER
6. IF AN AMPUTATION OR DEFORMITY MAKES IT IMPOSSIBLE TO PRINT A FINGER, MAKE A NOTATION TO THAT EFFECT IN THE INDIVIDUAL FINGER BLOCK
7. 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
8. 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. RECORD, OTHER ARMED FORCES NO. PASSPORT NO. (PP); ALIEN REGISTRATION NO. (AR); PORT SECURITY CARD NO. (PS); SELECTIVE SERVICE NO. (SS); VETERANS ADMINISTRATION CLAIM NO. (VA).



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY  
WASHINGTON DC 20460

JAN 18 1991

**MEMORANDUM**

**SUBJECT:** Request for Building Pass

**FROM:** Ann M. Linnertz, *H. M. Linnertz* Chief  
Security and Property Management Branch

**TO:** Project Officers

Building passes are intended only to identify contractors entering one of the EPA Headquarters buildings and are not intended for contractors to use as identification to cash checks, enter other government facilities, obtain airline tickets, rent vehicles or obtain hotel reservations.

Building passes will be issued only to contractor employees who work on-site for 24 hours or more a week. Management personnel who periodically visit on-site personnel shall not be issued Building Passes. Project Officers whose personnel are on-site less than 24 hours a week must provide a memorandum explaining the need for a building pass.

Couriers shall not be issued building passes.

All information must be typed or neatly printed on the request form. If the printed name of the Project Officer cannot be read, the form will be returned without action.

The Pass and ID Office is open from 8:30 am to 3:30 pm, Monday through Friday and operates on a first come first serve basis. Individuals requiring building passes should either bring the Request for Building Pass with them or mail it to the Security Office (PM-215). Forms will be maintained in a suspense file for 30 days after it is received and then returned to sender indicating that no action was taken. If a request for a building pass is handcarried by the applicant, it shall be valid only for 30 days from the date it is signed by the Project Officer.

Questions should be addressed to the Security Management Section at 382-6352.

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

Project Officer

**TO:** H. Brooks Hamlin, Chief  
Security Management Section

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 NAME:</b>	_____	
<b>CONTRACT NUMBER:</b>	_____	<b>EXPIRATION DATE</b> _____
<b>NORMAL HOURS OF WORK:</b>	_____	
<b>SPECIAL ACCESS:</b>	After 6:30 pm _____	Weekend _____ Holiday _____
<b>LOCATION:</b>	WSM _____ CM-2 _____	FAIRCHILD _____ CRYSTAL STATION _____

I understand as Project Officer, I am responsible for retrieving the above building pass(es) should:

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

**PROJECT OFFICER'S SIGNATURE** \_\_\_\_\_**TELEPHONE #** \_\_\_\_\_**MAIL CODE** \_\_\_\_\_**PO'S ID NUMBER** \_\_\_\_\_**PO's DIVISION** \_\_\_\_\_**DATE** \_\_\_\_\_

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





# 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				
<p>Please return this form with a copy of:</p> <p>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)</p>				

**DATA SECURITY FOR TSCA CONFIDENTIAL BUSINESS INFORMATION  
(EP52.235-120) (AUG 1993)**

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, 401 M Street, SW, Washington, DC 20460. Prior to receipt of TSCA CBI by the Contractor, the Contractor shall submit a certification statement to the Director of the EPA IMD, with a copy to the Contracting Officer (CO), certifying 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 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.

**L.XX ACCESS TO TSCA CONFIDENTIAL BUSINESS INFORMATION  
(EP52.235-100) (AUG 1993)**

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 some or all of its employees 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 EP52.235-120 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.

Appendix 8(b)

**Section K**

**K.XX CONTROL AND SECURITY OF TSCA CONFIDENTIAL BUSINESS  
INFORMATION**

**(EP52.235-105) (AUG 1993)**

**The offeror certifies that--**

**-- the Contractor and its employees have read and are familiar with the requirements for the control and security of TSCA CBI contained in the manual entitled "TSCA Confidential Business Information Security Manual". (See also EP52.235-120 elsewhere in this solicitation.)**

**TREATMENT OF CONFIDENTIAL BUSINESS INFORMATION  
(1552.235-71) (DEVIATION) (AUG 1993)**

(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 Contracts and Information Law; 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.

## **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 (Please type or print)	EPA ID Number
Signature	Date

## 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.



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

Please read Privacy Act Statement on reverse before completing.

		United States Environmental Protection Agency Washington, DC 20460		Social Security Number	
Employee Separation or Transfer Checklist					
Part 1. To Be Completed by Employee					
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					
Part 2. Responsible Officials Must Complete All Items in this Part					
Please clear the above-named employee. Final salary payment and application for retirement will be delayed until clearance is completed.					
		Clearance		Signature and Date	
Item		Yes	No		
Payroll/Travel	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				
Personnel	Training Termination Statements				
	Completion of Employment Agreements				
Other	Library Issuances				
	Security Termination Statements				
Security/ Facilities	Audiovisual Equipment				
	EPA ID Card				
	Keys				
	Parking Permit				
	Special Credentials				
Part 3. Certification and Clearance					
The Administrative Officer/Supervisor must certify that the above-named employee has accounted for the items listed below.					
Item		Clearance		Item	
		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.

Appendix 12

**TSCA CONFIDENTIAL  
BUSINESS INFORMATION**

DOES NOT CONTAIN NATIONAL  
SECURITY INFORMATION (E.O. 12065)

United States Environmental Protection Agency  
Washington, DC 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 Security 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.

**CONFIDENTIAL**

EPA Form 7740-13 (10-85)



May be TSCA CBI  
When Filled In

United States Environmental Protection Agency

# Receipt Log

TSCA Confidential Business Information

Does not contain National  
Security Information (E.O. 12065)

Date Received	Document Control Number/ Copy Number	Number of Pages	Received From (Enter Company/EPA Office, City, and State)	Description	Audit



United States Environmental Protection Agency


# Inventory Log

TSCA Confidential Business Information

Does not contain National  
Security Information (E.O. 12065)

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	
 <b>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> <ol style="list-style-type: none"><li>1. To be used only for temporary transfer of TSCA CBI. Transfers for more than thirty (30) days must be made through a DCO.</li><li>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.</li><li>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.</li></ol>	

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**



May be TSCA CBI  
When Filled In

United States Environmental Protection Agency

# Federal Agency, Congress, and Federal Court Sign Out Log

TSCA Confidential Business Information

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 TSCA CBI Security Manual Update Transmittal Sheet**

[illegible]



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

Name: \_\_\_\_\_  
SSN: \_\_\_\_\_

Organization: \_\_\_\_\_  
Mail Code: \_\_\_\_\_ [ ] Federal [ ] Contractor

Date: \_\_\_\_\_

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

I HEREBY CERTIFY:

[ ] THAT I HAVE INVENTORIED THE DOCUMENT(S) LISTED ABOVE; THE STATUS OF EACH DOCUMENT IS INDICATED ABOVE.

[ ] I ATTENDED MY ANNUAL TSCA CBI BRIEFING ON \_\_\_\_\_

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
DATE

\_\_\_\_\_  
DOCUMENT CONTROL OFFICER

\_\_\_\_\_  
DATE