

INSIDE THIS ISSUE:

Classified Information/Matter	1
DOE Classification and De-classification Program	2
Classification Authority	3
Classification Levels	3
Classification Categories	4
Classification Challenges	5
Access to Classified	5
Restricting L-Cleared Access to Secret Restricted Data	6
SF-312, Classified Information Non-Disclosure Statement	6
Unauthorized Disclosure	7
Penalties for Unauthorized Disclosure	7
Classified Matter Protection and Control (CMPC)	8
Accountable Classified Removable Electronic Media (ACREM)	11
Reporting Unprotected Classified	12
Infractions and Violations of Law	12
Controlled Unclassified Information	13
Security Badges	16
Badge Responsibilities	16
Badge Verification	17
Surrendering Your Badge	17
Badge Cautions	17
Administrative Escorting	18
Escort Responsibilities	18
L-Cleared Access	18
Special Nuclear Material	19
Accountable Nuclear Material	19
Individual's Reporting Requirements	20
Foreign Intelligence Targeting and Recruitment	22
Comprehensive Security Awareness	24
Points of Contact	24

Comprehensive Security Awareness

Comprehensive Awareness Briefing

When an employee is granted a clearance, they are required to complete a Comprehensive Security Awareness briefing before they are allowed initial access to classified information, classified matter, or Special Nuclear Material (SNM).

This booklet is used as a substitute for Computer Based Training (CBT) course 66.02, *Comprehensive Security Awareness Briefing*, for the convenience of individuals coming to work at Pantex who already hold an L- or Q-clearance. The information contained in this booklet is the same information presented in the CBT, to assure consistency of the information provided. As such, the student must successfully pass a written test prior to receiving access at Pantex.

The Comprehensive Security Awareness Briefing is intended to inform you about Federal Safeguards & Security requirements, site-specific security needs, and to ensure you are aware of your Safeguards and Security Responsibilities.

Classified Information/Matter

Regardless of its physical form or characteristics, INFORMATION is considered CLASSIFIED if it requires protection against unauthorized disclosure in the interest of National Security.

Classified MATTER is any combination of documents or material containing classified information. This includes explosives whose shape is classified, and classified parts.

DOE Classification/Declassification Program

The purpose of the DOE classification and declassification program is to identify classified information or matter through a systematic review by trained, authorized personnel. Classification is important to National Security, because it allows proper protection of classified information or matter and limits access to only those with a **NEED-TO-KNOW**.

“Classification” is the process of identifying information requiring protection in the interest of National Security. Security is the process of protecting this information. National Security is the ultimate basis for classification. Information cannot be classified to cover up waste, abuse, fraud, or embarrassment to the government. The Classification Program exists to manage classification guidance and classification authority.

All classified information/material is protected according to federal statutes and Presidential Executive Orders. DOE is responsible, under the Atomic Energy Act of 1954, as amended, for classifying information and material relating to atomic energy and its use in weapons, and under Executive Orders for other aspects of national security. The Atomic Energy Act of 1954 and Executive Order 12958 govern classification policy.

“Declassification” is a determination by an authorized individual that certain information or material no longer requires protection in the interest of National Security.

Declassification can only be conducted by a trained, authorized Declassifier who is designated in writing to perform de-classification decisions. This process requires the cancellation or removal of classification markings on documents. Documents needing

review for declassification should be referred to the Classification Office.



“Classification” is the process of identifying information requiring protection in the interest of National Security.

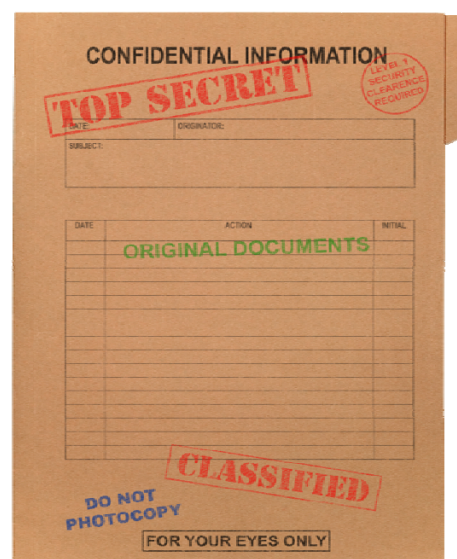
Classification Authority

Trained and appointed Derivative Classifiers (DCs) determine the appropriate classification level, category, and required caveats. The classification process is particularly crucial to the Department of Energy (DOE) because of the development and production of nuclear weapons. DCs, many of whom are experts in their field, are the only persons authorized to make classification determinations.

Classification Levels

Information and material are classified based on Levels and Categories. The classification **LEVEL** indicates the level or degree of damage that could occur to National Security should that information or material be compromised. Information and materials vary in their importance to national security. The greater the risk of damage to national security if disclosed to unauthorized sources, the more sensitive the information is considered to be, and the higher the level of classification it has.

There are three levels of classified information or matter:



Top Secret

(TS)

Unauthorized disclosure of Top Secret information could cause **EXCEPTIONALLY GRAVE DAMAGE** to National Security.

Secret

(S)

Unauthorized disclosure of Secret information could reasonably be expected to cause **SERIOUS DAMAGE** to National Security.

Confidential

(C)

Unauthorized disclosure of Confidential information could reasonably be expected to cause undue risk to common defense and security, or damage to National Security.

Classification LEVEL indicates the level of damage to National Security should that information be compromised.



Classification Categories

Information and material are classified based on Levels and Categories. Categories specify the type of information or material. There are three categories of classified matter:

Restricted Data (RD)

Restricted Data includes all information concerning design, manufacture, or utilization of atomic/nuclear weapons, the production of Special Nuclear Material (SNM), or the use of SNM in the production of energy.

RD is, generally, the most restrictive of the three classification categories.

Restricted Data is not allowed outside the DOE community.

Formerly Restricted Data (FRD)

Formerly Restricted Data is shared between the DOE and the Department of Defense (DoD). Both agencies jointly determine the need to re-categorize information related to military utilization of atomic/nuclear weapons, to remove the information from RD category, and to safeguard the information for National Security purposes.

FRD is subject to the same transmission restrictions that apply to RD.

National Security Information (NSI)

All data concerning Safeguards and Security measures, foreign government information, or other related information dealing with national security issues.

**Classification
CATEGORY
indicates the
type
of information or
material.**

PROFESSIONAL TIP

Acronyms are often used at Pantex and within the DOE community. Familiarize yourself with these acronyms by finding a copy of the Pantex Acronym List on the Pantex Intranet
<http://iw.pxplant.com/programs/brain/brain.html>

Classified information or matter will be identified by a combination of **Level** and **Category**:

Top Secret + Restricted Data = TSRD
 Top Secret + Formerly Restricted Data = TSFRD
 Top Secret + National Security Information = TSNSI
 Secret + Restricted Data = SRD
 Secret + Formerly Restricted Data = SFRD
 Secret + National Security Information = SNSI
 Confidential + Restricted Data = CRD
 Confidential + Formerly Restricted Data = CFRD
 Confidential + National Security Information = CNSI

Classification Challenges

Although authority for making classification determinations rests with Derivative Classifiers, **each employee** is encouraged and expected to challenge the classification of information, documents, or material that he or she believes is improperly classified. Under no circumstances is the employee subject to retribution for making such a challenge. Challenges should be directed to the Classification Office.



Access to Classified

The first requirement for allowing access to classified matter is that the recipient must have a security clearance. As a person who now holds a security clearance, you are personally responsible for all classified matter entrusted to you. By being granted a security clearance, you have met the first of three requirements to have access to classified information.

The second requirement is called “the need-to-know.” Need-to-know is a determination made by an authorized holder of information that a prospective recipient requires access to that information in order to perform official duties.

The third and final requirement you must fulfill in order to have access to classified information is to sign the Standard Form 312 (SF 312), “Classified Information Nondisclosure Agreement.” That form will be available for your signature once you successfully complete the Comprehensive Security Briefing.

As a holder of classified information or matter, **YOU** are responsible for determining a recipient’s identity, clearance, and their need-to-know.

Q-cleared individuals hold the proper access authorization to handle all levels and categories of classified information processed at Pantex, but need-to-know should be validated.

L-cleared individuals **do not** have the proper clearance to receive **Secret Restricted Data** or **TOP Secret** in **any category**.

Classification Level	Classified Matter Category		
	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)
Top Secret	Q	Q	Q
Secret	Q	Q & L	Q & L
Confidential	Q & L	Q & L	Q & L

This table illustrates access to Classified Matter by type of security clearance.

Restricting L-Cleared Access to SRD

Q-cleared employees must be diligent when processing, handling, or storing Secret Restricted Data - especially at Pantex. There are a number of L-cleared individuals employed at the Plant, so Q-cleared employees **MUST** make sure L-cleared employees do not gain physical, visual, or auditory access to Secret Restricted Data at any time. If you suspect an L-cleared employee has obtained access to Secret Restricted Data, contact an Inquiry Official immediately and report the potential incident.

L-cleared employees are NEVER allowed access

To Secret Restricted Data or any Top Secret Information!

Classified Information Nondisclosure Statement

The “Classified Information Nondisclosure Agreement” (SF-312) is a contractual agreement between you and the United States Government, in which you agree to protect classified information according to Federal Government regulations, to only allow access of classified information to authorized individuals, and to never disclose classified information to an unauthorized person.

The primary purpose of SF 312 is to inform you of :

- (1) The trust that is placed in you by providing you access to classified information.
- (2) Your responsibilities to protect that information from unauthorized disclosure.
- (3) The consequences that may result from your failure to meet those responsibilities.

By signing the SF-312, you are signifying you have read the agreement carefully, you will abide by the provisions outlined on the form, and any questions you may have about the form have been answered.



Unauthorized Disclosure



Unauthorized disclosure is a communication or physical transfer of classified or unclassified controlled information or material to an unauthorized recipient. Unauthorized disclosure could potentially cause damage or irreparable injury to the United States, or could be used to advantage by a foreign nation.

Unauthorized disclosure can occur when an individual intends to transfer information/material or by negligent handling.

Penalties for Unauthorized Disclosure

Unauthorized disclosure of classified information is subject to criminal and/or civil penalties, as provided by the Atomic Energy Act of 1954; the Espionage Act; and other security directives. The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations."

Currently, those penalties may include:

- Termination of security clearance
- Removal from any position of special confidence and trust requiring clearance
- Termination of employment
- Punishment under criminal sanctions
- Monetary fines



Classified Matter Protection and Control (CMPC)

As a newly cleared individual, you should be familiar with the “cradle-to-grave” concept used in the Classified Matter Protection and Control (CMPC) program. If your work responsibilities involve handling classified matter, you must receive additional training beyond this security briefing. Not every Pantex employee works with or comes in contact with classified matter. Yet, it is important for all employees to understand the following concepts:

Creating Classified

Classified “matter” can be any combination of documents and/or material containing classified information. Examples include explosives whose shape is classified, classified parts, classified documents, or even classified conversations. Regardless of the type of classified matter, the individual creating it must use equipment that has been approved to process classified. The only exception to this rule is when the individual is creating classified by hand-writing notes or documents. Hand-written classified information must be protected and controlled the same as equipment-generated classified matter.

Marking Classified

Classified must be marked appropriately. Refer to Work Instruction 02.02.04.02.02 for marking requirements.

Prior to classification review, matter that may be classified must be protected at the highest level and category. The originator is responsible for obtaining a classification review by a Derivative Classifier.



Access to Classified

Access to classified information is strictly based on a need-to-know basis. While the proper clearance can be verified by security badge, clearance level alone is not sufficient to determine the "need-to-know." It is the responsibility of the individual distributing classified matter to ensure that the recipient of the classified information has the appropriate security clearance AND need-to-know.

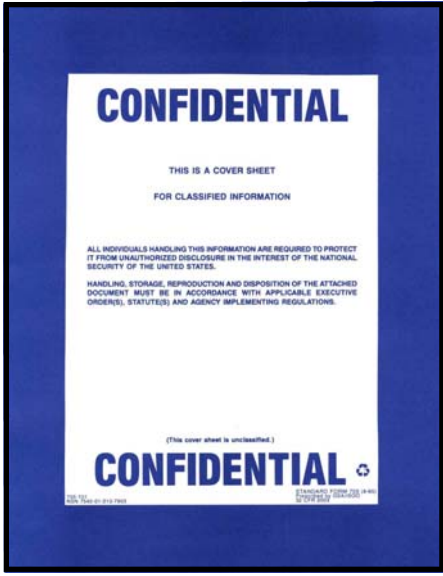
Classified must always be protected from unauthorized access. Control of classified matter may only be given to those who have the appropriate clearance and need-to-know.

CMPC (continued)



Controlling Classified Matter
Whenever classified matter is in use, it must always be under personal attendance, within your line of sight.

The appropriate cover sheets must be used any time a classified document is removed from a safe, vault, or vault-type-room, to protect disclosure of the document.



Storing Classified Matter

When not in use, classified must be locked in a GSA-approved repository, which includes a safe, a vault, or a vault-type-room (VTR).

Examples of each type of GSA-approved repository are pictured below:



Safe



Vault



Vault-type-room

CMPC (continued)

“Broken” classified documents are created when only part of a classified document is printed or reproduced.

These documents must have the markings required on the first page of a draft or finished classified document.

Refer to the current Work Instruction (02.02.04.02.02) on Marking Classified Documents for further detail.

Reproducing Classified Matter

Reproduction of classified documents must be kept to the minimum number of copies for operational necessity and any further reproduction limitations shown on the document. Classified information may be copied only on approved copy machines located in security areas.

These machines will have a sign indicating they are approved for classified reproduction.

Protect and control reproduced classified copies using the same requirements as the original.

When reproducing or printing partial classified documents, often referred to as “broken documents,” make sure the first page of the partial document contains the appropriate markings required for the first page of a classified document. Reference the work instruction for marking classified documents for specific guidance.



Facsimile Transmission of Classified Matter

You must utilize a STU or STE phone to transmit classified information over a fax machine. A log of incoming and outgoing classified facsimile activity is required (PX-1173B). If you do not have a classified fax machine connected to a STU or STE phone, take the information you need to fax to the Communication Center, Building 12-37, and they will fax it for you. When faxing a classified document, make sure the recipient received the transmittal. Get a verbal or written confirmation.



Destruction of Classified Matter

Classified matter must be destroyed beyond recognition or re-composition.

Pantex **does not** currently utilize shredders for destroying classified documents.

Instead, classified documents are disintegrated through the appropriate classified waste stream. Check Work Instruction 02.02.04.02.06 for exact details on how to arrange for destruction of classified matter.

If you ever have questions about the way Pantex destroys classified matter, contact a member of the CMPC team.

Discussion of Classified Information shall take place only in approved security areas. If you are unsure if you are in an approved area, do not discuss classified information. Telephones are one of the greatest tools at our disposal, but they can also be one of our greatest vulnerabilities to the protection of classified resources. Classified information must never be discussed on a conventional telephone. Secure Telephone Units (STU) have been placed in various locations around the Plant and must be used for classified telephone discussions.

Accountable Classified Removable Electronic Media

Classified Removable Electronic Media (CREM) include materials and components manufactured for the purpose of providing non-volatile storage of classified digital data capable of being read by a computer.

“Removable” media is any media that can be separated from the computer for any reason, any portable electronic devices, including laptop computers with fixed internal hard drives, and any media designed to be introduced to and removed from the computer without adverse effect on computer functions.



Electronic media becomes **Accountable CREM (ACREM)** when it is introduced to a computer system that is accredited to process up to and including Secret Restricted Data (SRD) or higher, or when the information contained on the media is classified as SRD or higher. ACREM

procedures are available through the Pantex document management system, or by calling CREM Operations at ext. 7215.

Reporting Unprotected Classified

If you discover classified information or material that is not being properly protected, **you are required by law to report it IMMEDIATELY.** To report unprotected classified, contact an Inquiry Official (Robert Burns, ext. 6243; Brenda Thomas, ext. 6366) or leave a message on the Security Incident Hotline, ext. 6333. During off-shifts, contact the Operations Center at ext. 5000, and they will notify an Inquiry Official.

A condition of your employment is to cooperate with Safeguards & Security personnel looking into potential security incidents. You may also be required to provide a written statement.

Infractions and Violations of Law

“Incidents of Security Concern” occur any time a security rule is violated, and warrant preliminary inquiry and subsequent reporting to DOE Headquarters by a trained, authorized Inquiry Official.

“Infractions” include any knowing, willful, or negligent action that violates the requirements of Executive Order 12958, Classified National Security Information, as amended, or any of its implementing directives, as long as the action does not constitute a violation of law.

Not all incidents of security concern become infractions. Each incident is considered on a case-by-case basis. It is important to note, however, that an infraction will stay on an individual’s government record for 75 years after termination with the Federal Government.

“Violations of Law” include any action or intent that constitutes a violation of US law, any Executive Order, or the implementing directives.



Violations of law are immediately turned over to the appropriate law enforcement authorities, including the Federal Bureau of Investigation.

Incidents of security concern, infractions, and violations of law are all subject to legal and administrative sanctions, to include disciplinary action, possible termination of employment, and possible prosecution in a court of law.

Additionally, unauthorized disclosure of classified information is subject to criminal and/or civil penalties.

Controlled Unclassified Information (CUI)

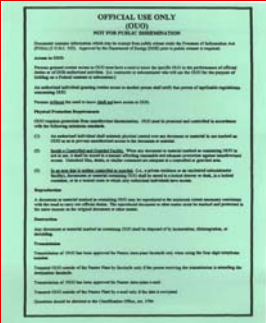
Controlled Unclassified Information (CUI) is broadly defined as controlled unclassified information that may be exempt from public release either by statute, or under the Freedom of Information Act (FOIA) and for which disclosure, loss, misuse, alteration, or destruction may adversely affect national security, governmental interests, or personal privacy. There are two basic types of CUI used at Pantex:

Official Use Only (OUO)

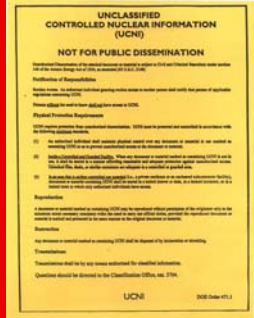
Information identified as unclassified, potentially sensitive, and that may be exempted from public release under the Freedom of Information Act (FOIA).

Unclassified Controlled Nuclear Information (UCNI)

UCNI is defined as unclassified information concerning design and/or security arrangements for nuclear materials and weapons in atomic energy defense programs.



Sample OUO and UCNI cover sheets.



Access to CUI

Both cleared and un-cleared employees are allowed access to CUI as long as they have a need-to-know in the performance of their job duties.

Trained, authorized Reviewing Officials (ROs) are the only personnel on plant site who are authorized to make the determination that information is UCNI. Many DCs are also ROs.

Protection of CUI

Reasonable precautions must be taken to prevent access to OUO and UCNI documents by persons who do not require the information to perform their jobs or other DOE authorized activity.

Destruction of CUI

OUO and UCNI documents can be destroyed by any method suitable for destruction of classified matter. The preferred method at Pantex is the use of disintegration boxes through the waste operations process.

Reproduction of CUI

OUO and UCNI documents may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as the original. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO or UCNI information.



Storage of CUI

Controlled Unclassified Information must be stored behind **at least one lock**. In the Property Protection Area (PPA), OUO and UCNI documents must be stored in a locked room or other locked receptacle such as file cabinets, desks, bookcases. In the Limited Area (LA), Protected Area (PA) and Material Access Area (MAA), OUO and UCNI documents may be stored in unlocked rooms or receptacles such as file cabinets, desks, or book cases.

Transmission of CUI

Transmission requirements are similar for OUO and UCNI. Please note, however, that there are some subtle differences for faxing, transmission over the telephone, and e-mailing.

Transmission by Mail — Offsite

Place in a sealed, opaque envelope or wrapping.

Stamp or write the words:
“To Be Opened by Addressee Only”

Can be mailed by First Class, Express, Certified or Registered Mail or any commercial carrier.

Transmission by Mail — On Site

Place in a sealed, opaque envelope or wrapping.

Stamp or write the words:
“To Be Opened by Addressee Only”

Place in any outgoing mail box. As long as CUI is sealed in an envelope or wrapping, it can be left unattended.

Transmission by Fax — OOU

Faxing OOU documents inside and outside of the plant is an approved process. Prior to faxing an OOU document the recipient must be contacted.

Transmission by Fax — UCNI

When faxing an UCNI document on plant site the recipient must be contacted prior to faxing the document.

Unlike OOU documents, when faxing an UCNI document off-site, a secure means must be used. At Pantex, that “secure means” is an approved fax machine connected to an encrypted telephone.

Transmission by e-mail — Onsite

E-mailing OOU and UCNI documents onsite is approved within the Pantex firewall. The first line of text in the e-mail must indicate that it is OOU or UCNI, or that it contains an OOU or UCNI attachment.

Transmission by e-mail — Offsite

OOU and UCNI transmitted offsite by e-mail MUST be encrypted using a Plant approved encryption package. Contact the Information Technologies Help Desk at ext. 3614 for software availability.

Password protection is NOT an option for OOU or UCNI e-mail.

Transmission by telephone (voice circuits) — Onsite

Discussion of OOU and UCNI information by voice circuits is permitted. If the discussion is on plant site, use only the 4-digit telephone number, and verify the person has a need-to-know before discussing OOU or UCNI over the phone.

Transmission by telephone (voice circuits) — Offsite

If discussion of OOU or UCNI is with someone offsite, encryption must be used.

If encryption is unavailable and other encrypted means is not a feasible alternative, use of regular voice circuits is allowed, but only under unusual circumstances. Employees should exhaust all other means of transmitting the information before discussing OOU or UCNI over unclassified telephones or voice circuits!

Security Badges

Security Badges are an important element of the access control system. It is your identification and allows you access into Pantex facilities. Security Badges show access authorization levels, and additional access control privileges such as Human Reliability Program (HRP) indicators.



Badge Responsibilities



All Personnel are required to **WEAR** their badge at all times while on Pantex property. Badges should be worn photo side out, above the waist, and on the outer most piece of clothing.

If you **LOSE** your badge on site, contact Security to escort you to the Property Protection Area so you can report to Access Control, Building 16-12.

If you **LOSE** your badge off site, report to Access Control, Building 16-12 the next business day.

If your badge is **STOLEN**, report it immediately to the Operations Center at 477-5000.

If you **FORGET** your badge, you may choose to return home to retrieve it (this is the best option), or Access Control can issue a temporary badge for one day. If your badge is lost or forgotten two or more times within a 12 month period, your Division manager will be notified. Division managers handle repeat offenders according to recommendations provided by Labor Relations.

Your badge must be **REPLACED** if:

- Your contract company changes
- Your name changes
- Your physical appearance changes
- It is faded or damaged



Badge Verification

When entering Pantex, the security badge is used as verification to ensure only authorized personnel have access to the facility.

Upon entering the Pantex facility, remove your badge from any holder and present it for examination by Security Police Officer personnel or the automated Argus System.

Surrendering Your Badge

Pantex employees, consultants, and contractors on leave for 30 consecutive days or those who will be gone for an unknown time period are required to return their badge to Access Control.

Security badges are the property of DOE and shall be returned to Access Control if it is requested, expired, no longer valid, required, or upon termination.

Badge Cautions

YOU are responsible for any Security Badge entrusted to you. In order to provide the best protection for Government credentials, the following cautions are provided:

It is illegal to counterfeit, alter, or misuse your badge.

Do not use your badge outside Pantex
UNLESS it is for an official government purpose.

Remove your badge when you are offsite:
DO NOT wear it in public places!

Protect your badge from theft when you are offsite:
DO NOT leave it in plain sight, and
DO NOT LEAVE IT IN YOUR VEHICLE!

Administrative Escorting

Administrative escorts are utilized to prevent uncleared personnel in the Limited Area from gaining physical, visual, or auditory access to classified information.

The employee providing the administrative escort must hold an L- or Q-clearance, and they must be an exempt or non-exempt non-bargaining employee. This includes employees whose clearances are held at Pantex by the main contractor, NNSA Pantex Site Office, local Sandia or Tri-Lab, and some subcontractor personnel approved by DOE.

Individuals performing administrative escorts **cannot** be related in any way to the individual(s) being escorted.

Metal Trades Council employees and Security Police Officers are excluded from performing administrative escorts.

Escort Responsibilities

The employee providing the Administrative Escort must complete a PX-2707 to request authorization to escort an individual. The requestor's signature on the PX-2707 indicates they have read the second page of the form, and will abide by the responsibilities listed on the second page of the form.



If an uncleared or L-cleared individual is being escorted to work on a computer that processes Secret Restricted Data (i.e., a vendor or technician scheduled to work on components), the employee providing the escort must also complete Cyber Security escort training, course #CB 75.39.

L-Cleared Access

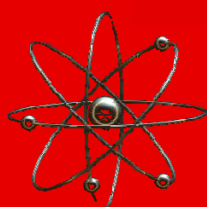
In addition to administrative escort requirements, L-cleared access into any buildings or rooms where Secret Restricted Data is processed, handled, or stored, **MUST** be covered by an approved L-cleared Building Security Plan (PX-5180). A Q-cleared employee is required to escort the L-cleared individual at all times in these areas to make sure the L-cleared employee does not obtain unauthorized access to Secret Restricted Data.

Special Nuclear Material

As part of Pantex Plant's authorization to possess and use accountable nuclear material, Pantex must provide an effective Material Control & Accountability (MC&A) program. This program is responsible for managing certain aspects of special nuclear material.

This responsibility includes generating and maintaining accurate information regarding nuclear material quantity, location, and other characteristics, as well as reporting information to the DOE national nuclear material database.

Accountable Nuclear Material must be controlled, inventoried, measured, and tracked.



Accountable Nuclear Material

The types of accountable material include:

- Special Nuclear Material (SNM)
- Source Nuclear Material
- Other Nuclear Material

All accountable quantities of nuclear material are required to be controlled, inventoried, measured, and tracked through an accountability system. The amount of SNM is characterized by "category." Category I is the highest quantity and Category IV is the lowest quantity group. A Category I or II quantity of nuclear material requires a higher level of physical security protection that includes protection in a Material Access Area (MAA).

Management of accountable nuclear material helps ensure the material is properly characterized, controlled, protected, used, and accounted for, thereby deterring and detecting theft, diversion, or unauthorized use of nuclear material.

Individual's Reporting Requirements

Remember that whether an individual (contractor, subcontractor, etc.) holds a clearance or is in the process of obtaining a clearance, he or she is required to report certain personal information to the Safeguards & Security Administrative Officer within **ONE** working day of the event, unless otherwise specified. Check the Security Awareness Reminder: REPORTING REQUIREMENTS Intranet page for the most up to date requirements, which include:

Arrests

Employees must report all arrests, including dismissed or dropped charges.

Criminal Charges

Employees must report all criminal charges including felony, misdemeanor, public and petty offenses, as defined in the statutes of any sovereign state. Criminal charges do not include traffic or other charges that are specifically differentiated and exempted from statutory criminal offenses.

Detention by Law Enforcement

Employees must report any detention by federal, state or other law enforcement authority for violation of law. The only exception to this reporting requirement is detention for a simple traffic stop.

Traffic Violations

Employees must report any traffic violation for which you receive a fine of \$250 or more unless the traffic violation is alcohol or drug related. Any traffic violation that is alcohol or drug related must be reported regardless of the amount.

Ongoing Contact with Foreign Nationals

Employees must report employment or business-related associations with any foreign national or employees/representatives of a foreign-owned interest.

Hospitalization

Employees must report hospitalization for: treatment of mental illness or other mental condition; treatment for alcohol or drug abuse; any condition that may cause a significant defect of judgment or reliability (the key word is "hospitalization").

Bankruptcy

Employees must report any time they file for personal or business-related bankruptcy.

Foreclosures

“Foreclosure” is the process in which a lender repossesses a property after the owner has defaulted on the mortgage or failed to comply with the terms of the mortgage contract. All foreclosures must be reported.

Wage Garnishment

Employees must report all wage garnishments including, but not limited to, divorce, delinquent debts, or child support.

Prescription Medications

Employees must report all medications for depression, anxiety, or stress to the Safeguards & Security Administrative Officer. All medications must be reported to Medical.

In addition to the reporting requirements listed above, the following information must be reported to Personnel Security:

Change of Marital Status

Employees must report marriage or cohabitation within 45 calendar days.

Name Changes

Employees must report all legal name changes.

Change of Citizenship

Only U.S. Citizens can be employed at Pantex. If you are a U.S. citizen who changes citizenship or acquires dual citizenship, you must report this change to Personnel Security and Counterintelligence.

One more reportable...

...if you are approached by ANY individual seeking unauthorized access to **classified matter, classified information, Special Nuclear Material, sensitive material, sensitive information**, or if anyone starts asking inappropriate questions about your employment at Pantex, IMMEDIATELY report it to the Counterintelligence Office!

Foreign Intelligence Targeting & Recruitment

Military force modernization, economic competition, understanding adversary political plans, and commercial modernization drive foreign collection efforts. As a result, dual-use technologies - those with civilian and military applications - are consistently the targets of foreign collection. To counter these activities, the DOE partners with the United States Intelligence Community in identifying and defeating these activities. Your Pantex Counterintelligence (CI) Field Office is chartered to address foreign intelligence collection efforts and insider betrayal.

As defined by Executive Order 12333: “Counterintelligence” means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.



An intelligence collector’s best source is a trusted person inside a company or organization whom the collector can task to provide them with proprietary or classified information.



The individuals with access to improperly acquire a company’s information are the company’s own employees.

Employees who resort to stealing information exhibit the same motivations and human frailties as the average thief or spy: illegal or excessive use of drugs or alcohol, financial problems, disgruntlement, personal problems, and greed.

To mitigate the threat to Pantex employees from both insider and foreign collection attempts, the DOE implements a required reporting system. If you, or a fellow Pantex employee, experience any of the following, you must report it to the Pantex CI Field Office:

- Foreign travel to a sensitive country or where sensitive subjects will be discussed
- Any substantive professional, personal, or enduring financial relationship with sensitive country foreign nationals
- Any contacts with foreign nationals who make requests that could be attempts at exploitation or elicitation
- Requests for unauthorized access to classified or otherwise sensitive information
- Unusual solicitations (anyone of any nationality)
- Anomalies (behavior exhibited by a foreign national that is inconsistent with the expected norm)



Additional information can be obtained from your Pantex CI Field Office and the CI Web Site, located on the Pantex intranet.

Counterintelligence at Pantex

The Pantex Counterintelligence team is here to support national security initiatives and encourages each employee to report any suspicious activity to:

- Darlene Holseth, Senior CI Officer, ext. 5361
- Bobby Carlton, CI Officer, ext. 5312
- Bruce Johnston, Cyber CI Officer, ext. 3631
- Stephanie Steelman, CI Analyst, ext. 5427
- Michelle Abell, CI Awareness Coordinator, ext. 5374

“Protection Through Teamwork”

Comprehensive Security Awareness

There is no other place in the world like Pantex. National Security - and ultimately global protection - is in **your** hands. It is a huge responsibility and should not be taken lightly.

EVERY employee at Pantex is held accountable for their actions, and each individual must choose to follow established Security rules.



Make sure you understand those rules, and make the right choices each and every day. **The consequences are too high to choose otherwise.**

Pantex Security Points of Contact

- | | |
|---|--------------------|
| 1. Safeguards & Security Division Manager | 477-3939 |
| 2. Access Control (badge office) | 477-3908/3909 |
| 3. Safeguards & Security Administrative Officer | 477-5854/7205 |
| 4. Classification Officer | 477-3948 |
| 5. Classified Matter Protection and Control | 477-7610/6152 |
| 6. Inquiry Officials | 477-6243/6366/3818 |
| 7. Cyber Security | 477-6291/3656 |
| 8. Operations Security (OPSEC) | 477-3905 |
| 9. Safeguards & Security Awareness | 477-3556/5560 |
| 10. Personnel Security | 477-3912 |
| 11. Emergency Operations Center | 477-5000 |

Security Awareness is on the Intranet!

<http://iw.pxplant.com/PantexWeb/functions/security/SecurityAwareness/index.htm>