

CMPC Essentials

(Cleared Subcontractors)

ST 66.15

This document has been reviewed by a DC/RO and has been determined to be UNCLASSIFIED, not UCN, and contains no CUI based on current classification guidance. This review does not constitute a review for CUI outside of classification guidance and does not constitute clearance for Public Release.

Name: Scott Minton

Date: 11/21/2024

Pantex eDC/RO ID: 878696

CMPC Essentials (Cleared Subcontractors)

You may be asking yourself, what is CMPC?

CMPC is classified matter protection and control, and it is your responsibility to protect and control classified matter from cradle to grave.

- As an employee who has access to classified matter (CM), you will be responsible for properly protecting and controlling CM that may be accessed, originated (i.e., generated, created), reviewed, marked, reproduced, received, transmitted, accounted for, stored, permanently buried, released for emergency, or destroyed. The basic knowledge and tools you need to properly control CM are identified so you can protect the classified information to which you are entrusted.
- All personnel with security clearances whose responsibilities include working with CM must receive CMPC training and/or briefings appropriate to their duties prior to receiving access to CM. Additionally, they must receive refresher training and/or briefings to ensure continued reinforcement of requirements.
- If for any reason you do not understand or if you have questions regarding this training or any CMPC requirements, you may contact the CMPC Office at 806-477-6000 for more guidance or clarification.

CMPC Essentials (Cleared Subcontractors)

Classified Documents

Classified information exists in many forms, maintaining a cradle-to-grave life cycle. The cradle-to-grave life cycle of classified information, which exists as a physical form (such as documents), must be protected from origination to destruction, to preclude unauthorized disclosure of our nation's classified assets.

Written documents, verbal communication, the shape of a weapon part, residue, electronic data, and digital data are some examples. A document is a physical medium (regardless of its physical form or characteristics) used to convey information.

Other examples of classified documents are provided in the following table:

CMPC Essentials (Cleared Subcontractors)

Classified Documents (cont.)

Aperture card	File folder	Photograph
Chart	Final paper	Printer ribbon
Computer media	Maps	Recording
Developed film	Microfiche	Sheet film
Draft	Microfilm	Sketch
Drawing	Microform	Slide
E-mail	Negative roll	Sticky notes
Engraving	Notebook	Transparency
Exposed film	Painting	Typewriter ribbon
Facsimile	Photographic print	Working note/paper
Sound recordings by magnetic, optical, or any other electronic means		
Video recordings by magnetic, optical, or any other electronic means		
Reproduction of things by any means or process		
Any other medium, or combination thereof, containing or revealing classified information		

CMPC Essentials (Cleared Subcontractors)

Classified Material

In addition to classified documents, classified material may also reveal classified information. Classified material can be made of any substance (regardless of its physical or chemical form). Examples of classified material are provided in the following table:

Accessory	Metal
Assembly	Parts
Bulletin boards	Product of any kind
Chemical compound	Radio
Component	Raw material
Electronic equipment	STE
In-process material	Telephone
Manufactured commodity	Television
Machinery	White board
Visual Teleconference Communication (VTC)	
Any other equipment, or combination thereof, containing or revealing classified information	

CMPC Essentials (Cleared Subcontractors)

Origination and classification requirements for classified matter

When you originate (create) any type of document or material within a classified subject area, as the originator, it is your responsibility to do the following:

- Protect the information at the highest potential classification level and category
- Obtain a review to determine its classification
- Mark all CM according to the classification determination

NOTE: It is the originator's (owner's) responsibility to properly mark the CM.

CMPC Essentials (Cleared Subcontractors)

Required markings for classified matter

Refer to the following table for an overview of the classification levels and categories:

Classification Level	Classified Matter Category			
	Restricted Data (RD)	Formerly Restricted Data (FRD)	National Security Information (NSI)	Transclassified Foreign Nuclear Information (TFNI)
Top Secret	TS/RD	TS/FRD	TS/NSI	TS/TFNI
Secret	S/RD	S/FRD	S/NSI	S/TFNI
Confidential	C/RD	C/FRD	C/NSI	C/TFNI

CMPC Essentials (Cleared Subcontractors)

Generic Marking Requirements:

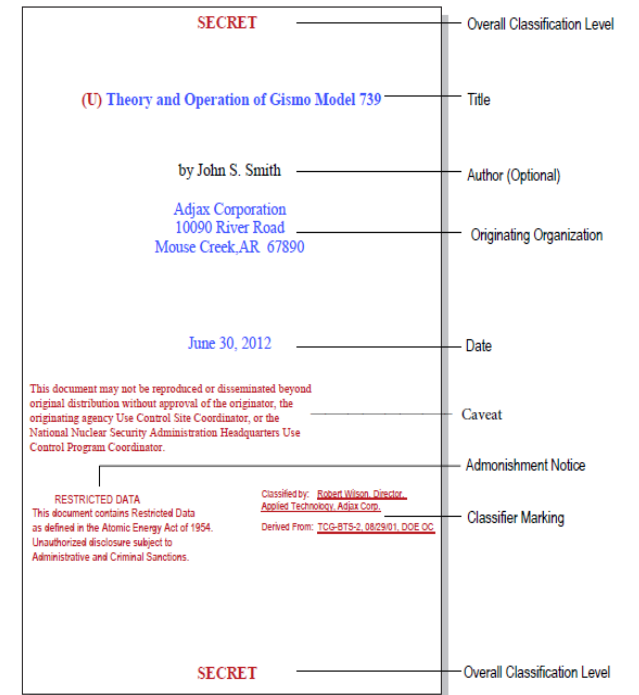
Before releasing or accepting classified information in any form; it is YOUR responsibility to ensure classified assets are properly marked (to prevent inadvertent disclosure). Additionally, ensure

- electronic files and documents are marked through the electronic Derivative Classifier/Reviewing Official (eDC/RO) system;
- CM is marked to leave no doubt at first glance that it is classified;
- CM is marked to current marking standards when released by the current holder (individual, specific office, or ad-hoc working group);
- written notification of the classification is provided to all recipients when marking level and category are not practical; and
- the Marking Handbook is referred to for specific Transclassified Foreign Nuclear Information (TFNI), SIGMA and electronic environment requirements.

CMPC Essentials (Cleared Subcontractors)

All Documents:

- Mark classified documents with the following items:
- Classification level on the top and bottom of the title/cover/first page
- Restricted data (RD)/formerly restricted data (FRD) admonishment on title/cover/first page
- Originating organization, date, and mailing address (if removed from site)
- Derivative classifier marking
- Level and category on the top and the bottom of interior pages
- Level on the back page (a cover sheet may be used as the back page)
- Caveats (if any) -- Acronyms that are typically placed at bottom left of page; they are used to denote special handling requirements, such as the following:
 - SIGMA 14, 15, 18, and 20
 - FGI
 - No Foreign Government (NOFORN)
 - Originator Controlled (ORCON)
 - ATOMAL [Atomic information that has been released to the North Atlantic Treaty Organization (NATO)]
- Subjects and titles must be marked with the appropriate classification [i.e., level, category (if RD or FRD); and other applicable caveats] or “U” if unclassified; the marking must be placed immediately preceding the item.



CMPC Essentials (Cleared Subcontractors)

Documents with Mixed Levels and Categories:

- You may use a marking matrix (optional) when CM contains a mix of information and various levels and categories. If the marking matrix is used, the following marking (in addition to other required markings) must be placed on the first page of text:

This document contains:

Restricted Data at the (*e.g.*, *Confidential*) level.
Formerly Restricted Data at the (*e.g.*, *Secret*) level.
National Security Information at the (*e.g.*, *Secret*) level.

Classified by: *Name and Title*

Transmittal Documents:

- The first page of a transmittal document must be marked with the highest level and other applicable caveats of classified information being transmitted, and an appropriate notation must be given to indicate its classification when the enclosures are removed.

SECRET

Department of Energy
Office of Security
1000 Independence Avenue S. W.
Washington, D.C. 20585

October 12, 2011

MEMORANDUM FOR: Bill Brown, Director
Office of Administration Services

FROM: Bruce Black, Director
Office of Nuclear Energy

SUBJECT: (U) Special Nuclear Materials Inventory

Transmittal Memo

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

Document transmitted herewith contains (U) **SECRET RESTRICTED DATA**

When separated from attachment, handle this document as (U) **UNCLASSIFIED**

Classified by: **Siam**
Derived From: **00-58-4, 09-12-09, DOE/OC**

SECRET

CMPC Essentials (Cleared Subcontractors)

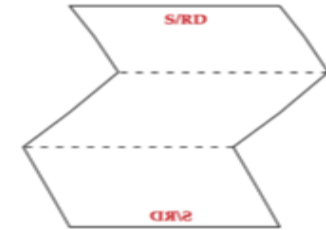
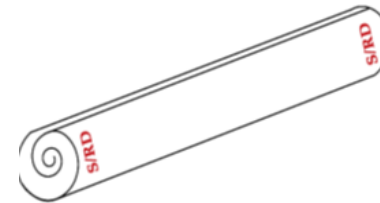
Unclassified Transmittal Documents:

An unclassified transmittal document that is attached to a classified document must contain all of the required first-page markings of its classified attachment (in addition to the proper markings when it is separated from the attachment).

Example: In this case, the transmittal becomes the first page of the attachment, which, in turn, becomes a new document. Once the new document reaches its final destination and becomes separated, the transmittal must be re-marked to reflect its original classification.

More Documents:

Charts, maps, drawings, and X-rays are also documents and must be visibly marked with the same required markings as a regular RD or FRD document.



CMPC Essentials (Cleared Subcontractors)

National Security Information:

National Security Information (NSI) documents dated after April 1, 1997, must be portion-marked by a derivative classifier. Portion markings must include any applicable caveats. Each section, part, paragraph, graphic, figure, subject/title, or a similar portion of any such document must be accurately marked to show the level and categories. NSI documents must contain the marking requirements as designated by a derivative classifier when obtaining a DC review.

UNCLASSIFIED

Chapter 3

(U) Portion Marking

1. (U) This is paragraph 1 and contains unclassified information. This portion will be marked with the designation "U" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. This portion will be marked with the designation "U" in parentheses.

Page 42

UNCLASSIFIED

**UNCLASSIFIED CONTROLLED
NUCLEAR INFORMATION**

3. (U) This is paragraph 3 and contains unclassified information. This portion will be marked with the designation "U" in parentheses.

4. (UCNI) This is paragraph 4 and contains information determined to be UCNI. It is marked "UCNI" in parentheses.

5. (U) This is paragraph 5 and contains unclassified information. This portion will be marked with the designation "U" in parentheses.

Page 43

**UNCLASSIFIED CONTROLLED
NUCLEAR INFORMATION**

Overall Classification Level

Originator Information
(name of organization and address)

Date

(Classification Level/Caveat*) Title/Subject
Classification level and caveat (if applicable) must always be identified; the use of classified titles is strongly discouraged.

(Classification Level/Caveat*) Paragraph 1
(Classification Level/Caveat*) Paragraph 2

Caveat (if applicable)
NSI Classifier Marking

Overall Classification Level

CMPC Essentials (Cleared Subcontractors)

Cover Sheets and Media Labels:

Place coversheets/labels on all classified documents when they are removed from a safe, vault, or vault-type room (VTR).



SF 708 (1-87)



SF 710 (1-87)



SF 706 (1-87)

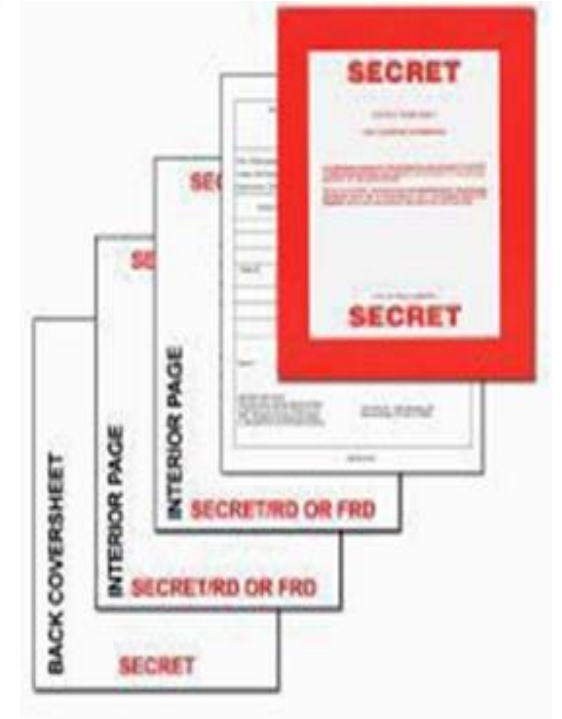
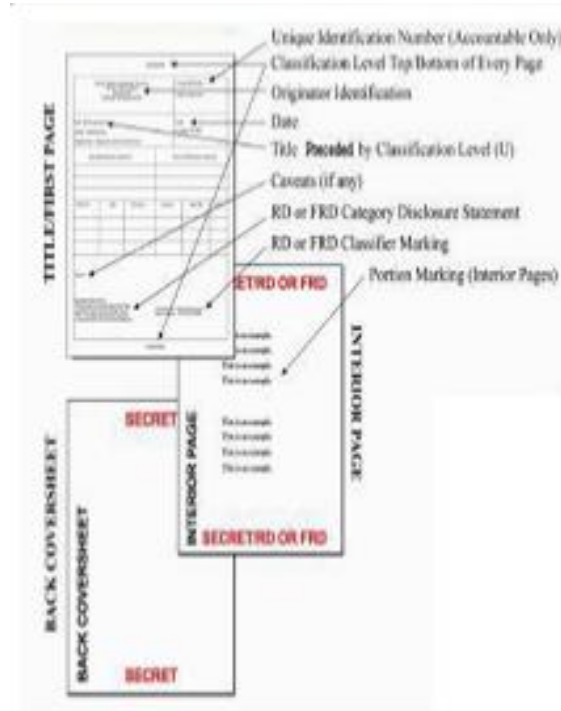


SF 707 (1-87)

CMPC Essentials (Cleared Subcontractors)

Media/Hard Copy Documents:

When information is prepared on classified information systems, the hard-copy output (this includes microfiche, film, labels, travelers, maps, drawings, etc.) must be correctly marked either according to its classification, per review of the output, or as a working paper.



CMPC Essentials (Cleared Subcontractors)

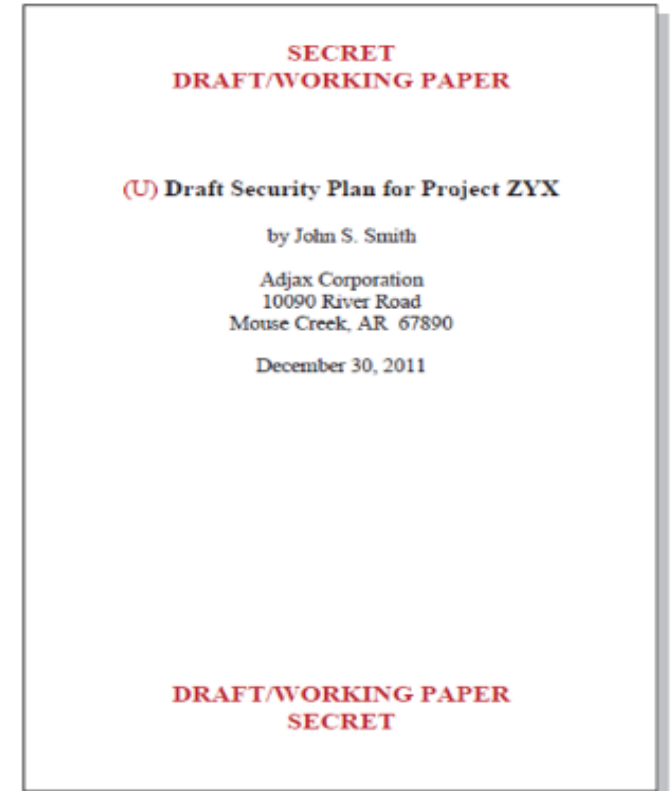
“Working Papers” and “Drafts”:

Classified working papers and drafts are considered to be temporary and must be:

- marked to leave no doubt at first glance that it is classified,
- marked with the annotation “Working Papers” or “Draft”,
- marked with the creation date,
- marked with their overall classification level [this includes the category (if RD or FRD) on the interior pages and the classification text is clearly distinguishable from the document text], and
- destroyed when no longer needed

Working papers and drafts must be marked in the same manner as a finished document and at the same classification level and category of the finalized documents when

- transmitted from Pantex,
- retained more than 180 days from the date of origin, or
- filed permanently.

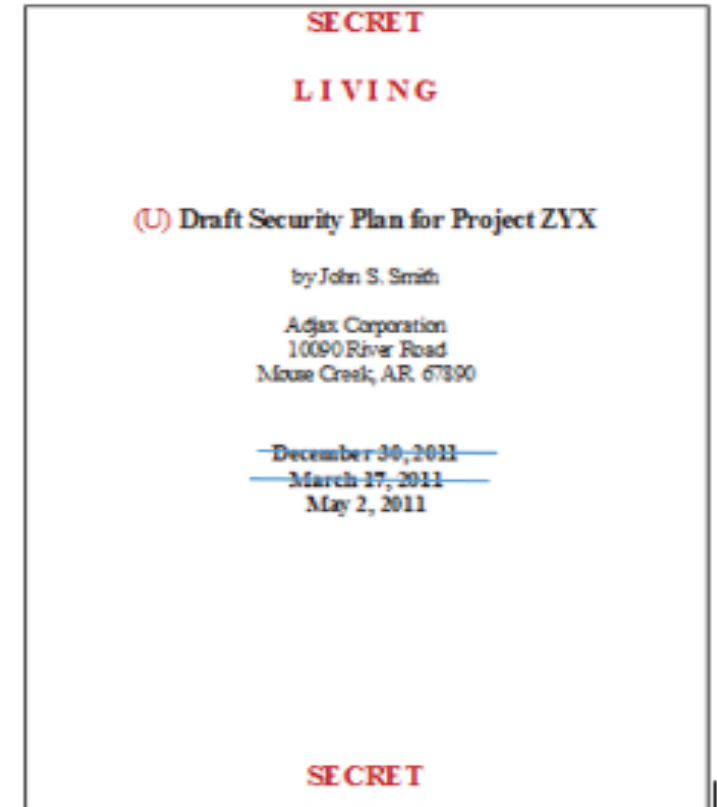


CMPC Essentials (Cleared Subcontractors)

Working paper and draft documents updated on a frequent basis are referred to as “living” documents. Ongoing experiments, studies, etc., are considered living documents. These types of documents originate on each date they are changed and must be

- marked with a new originating date
- marked with the annotation “Living,”
- marked in the same manner as working papers or drafts, and
- marked as finalized when
 - transmitted from Pantex,
 - retained more than 180 days from date of origin or
 - filed permanently.

NOTE: As a best business practice, it is a good idea to place a bright-colored folder labeled as “Working Papers/Drafts/Living Documents” in the very front of the top drawer. This will draw attention to living documents and will help with reminding you to check the dates and statuses of them.



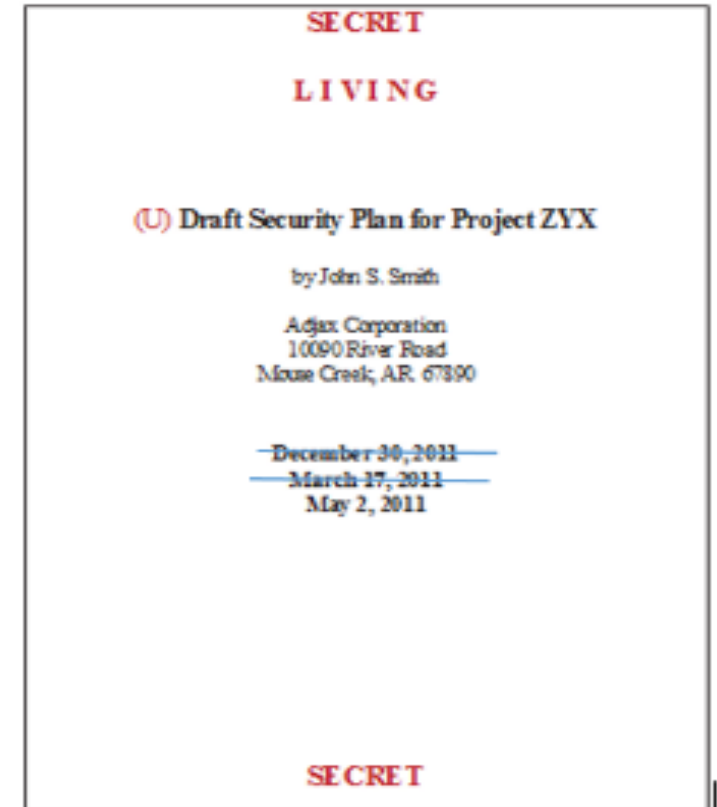
CMPC Essentials (Cleared Subcontractors)

“Living” Documents:

Working paper and draft documents updated on a frequent basis are referred to as “living” documents. Ongoing experiments, studies, etc., are considered living documents. These types of documents originate on each date they are changed and must be

- marked with a new originating date
- marked with the annotation “Living,”
- marked in the same manner as working papers or drafts, and
- marked as finalized when
 - transmitted from Pantex,
 - retained more than 180 days from date of origin or
 - filed permanently.

NOTE: As a best business practice, it is a good idea to place a bright-colored folder labeled as “Working Papers/Drafts/Living Documents” in the very front of the top drawer. This will draw attention to living documents and will help with reminding you to check the dates and statuses of them.



CMPC Essentials (Cleared Subcontractors)

File Folders and Other Containers:

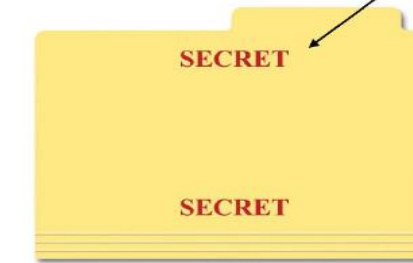
Containers include boxes, bags, envelopes, notebooks, attaché cases, video jackets, disk covers/sleeves, boxes, crates, barrels, carts etc. File folders and other containers must be

- marked when CM is in-use,
- marked to leave no doubt at first glance that it is classified, and
- marked on the top and bottom of all visible sides with the highest
- level of its contents once it is removed from an approved repository.
 - A cover sheet may be used for this purpose.

Containers must be clearly marked when documents or parts are unable to be marked.



Front



Back

Folders containing classified matter, when removed from secure storage repositories, are conspicuously marked to indicate the highest level of classified information contained in the folder. A coversheet could also be affixed to the folder.

The folder is unclassified when it no longer contains classified material.

CMPC Essentials (Cleared Subcontractors)

Classified Material (parts, equipment, tools, components, material):





The classification level and category (if RD or FRD) must be clearly marked on all non-document classified material (parts, equipment, tools, components, materials), if possible. Otherwise, alternative marking methods must be used to identify the overall classification level and category (if RD or FRD). When marking the level or category is not practical, written notification must be furnished to all recipients. The originator—when creating, generating, or printing—is responsible for ensuring that CM is marked (i.e., obtaining a DC review).

Overall markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material other than documents and on containers of such material, if possible. If marking the material or container is not practical, written notification of the markings shall be furnished to recipients.



CMPC Essentials (Cleared Subcontractors)

Containers must be clearly marked when the parts are unable to be marked.

<p>Bagged</p>		<p>Decal/Labeled</p>	
<p>Tagged</p>		<p>Labeled</p>	

CMPC Essentials (Cleared Subcontractors)

Containers must be clearly marked when the parts are unable to be marked.

Below are additional CM marking examples; these examples are not all inclusive:



CMPC Essentials (Cleared Subcontractors)

Missing Markings:

If documents originated by others are missing markings that cannot be corrected (i.e., missing DC or portion marking), the recipient must inform the sender of any missing standard markings and request correction and/or re-transmittal of the document, if possible.

Other Government Agencies (OGAs) and Foreign Government Documents:

Documents received from OGAs and foreign governments that have not been marked to conform to DOE requirements do not need to be re-marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD) or TFNI identifiers, when applicable.

CAUTION

Consult production engineers prior to marking classified materials. War reserve and configuration control requirements mandate strict control over what is done to specific materials - markings cannot violate these rules. Any alternative markings under consideration must be compatible with the matter being marked.

CMPC Essentials (Cleared Subcontractors)

Exceptions:

Do not place any classified markings on the following items:

- Repositories (safes/vaults/VTRs,)
- Outer containers or packages used to transmit CM off-site

NOTE: Refer to the DOE CMPC Marking Resource, April 2020, for more marking examples. This resource has a long list of examples, which also includes email markings.

CMPC Essentials (Cleared Subcontractors)

Classified matter in-use

Be aware that handling classified information (i.e., the origination, classification, marking, accountability, reproduction, transmission, and destruction of classified information) while conducting daily activities at Pantex signifies CM in-use. Additionally, hand carrying ON SITE is CM in-use; therefore, the hand transfers of classified information, no matter the method of transfer or transmission, must be

- constantly attended by an authorized person having proper clearance, authorization, and need to know or
- properly stored in a safe/vault/VTR.

Classified Computer Use

Any classified computer use, whether it is a network or a stand-alone computer, is considered classified in-use. To ensure proper protection of this classified system, you **MUST** sign off or lock the computer when you leave the work station, and you **MUST** sign off before you leave the site for the day.

CMPC Essentials (Cleared Subcontractors)

Discussion of Classified Information

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 the greatest vulnerabilities to the protection of classified resources. Classified information must never be discussed on a conventional telephone. Secure telephones (e.g. STEs or Vipers) have been placed in various locations around the plant and must be used for classified telephone discussions.

Unauthorized disclosure is a communication or physical transfer of classified information to an unauthorized recipient.

CMPC Essentials (Cleared Subcontractors)

Penalties for Unauthorized Disclosure

Unauthorized disclosure of classified information is subject to criminal and/or civil penalties, as directed by the Atomic Energy Act of 1954, the Espionage Act, and other security directives. Whoever knowingly and willfully communicates, furnishes, transmits, publishes, or otherwise makes available **ANY** classified information to an unauthorized person or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States shall be fined under U.S. Title Code 18, Subsection 798, *Disclosure of Classified Information*, imprisoned up to 10 years, or both (imprisonment and fines).

Conditions and restrictions for access to classified information or matter:

Personnel requiring access to classified information and/or matter must meet the following requirements:

- Possess a DOE access authorization/security clearance (L or Q)
- Have the need to know
- Sign SF-312, *Classified Information Nondisclosure Agreement*
- Complete the appropriate training

CMPC Essentials (Cleared Subcontractors)

The following table delineates minimum clearance levels for access to CM:

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

CMPC Essentials (Cleared Subcontractors)

Hand Carrying Classified Matter On-Site

Hand Carrying of classified matter is **not allowed** for subcontractors. Hand carrying must be performed by a federal employee (DOE, NNSA, DoD, etc.), or a Management & Operating employee (Pantex, Sandia, Los Alamos, etc.).

NOTE: If you have any questions pertaining to the Hand Carry process please contact the CMPC Hotline at 806-477-6000.

CMPC Essentials (Cleared Subcontractors)

Types of matter associated with control systems and accountability

Accountable matter includes the following:

- Top Secret matter
- Secret-RD stored outside the LA – (**must be approved by the information security manager**)
- Any matter designated as accountable by national, international, or programmatic requirements. Examples include, but are not limited to, SIGMA 14 and North Atlantic Treaty Organization (NATO) ATOMAL.

Accountability applies regardless of the physical form of the matter (i.e., electronic, paper, or parts). Accountable classified documents are tracked through PDM-Link in conjunction with the PX-925-1, *Classified Matter Receipt/Chain of Custody* form and DESKAID-936, *Processing Accountable Items into CRIS*. Appropriate control stations manage accountable matter by maintaining accountability systems for the matter. As such, accountability requirements are as follows:

- A chain of custody must be established, verified and documented from origination to destruction or transfer.
- Each accountable item can be located at any given time.
- An annual inventory must be conducted.
- All discrepancies regarding inventories are detected and reported to PFO.
- Two persons, the individual destroying the CM and the witness, must sign the destruction certificate, PX-925-1.
- Accountable matter can only be stored at an authorized control station.

The control systems and accountability make an audit trail, which helps to deter and detect unauthorized access or removal of CM.

CMPC Essentials (Cleared Subcontractors)

Reproduction requirements for classified documents

Reproduction equipment includes, but is not limited to, copiers, tooling machinery, printers, cameras, telephones, scanners, dry-erase and electronic boards, verbal (voice) technologies, and some cyber technologies. As part of your classified responsibilities, please do the following:

- Use only Reproduction equipment/methods (copiers, dimensional, printers, video teleconferences, scanners, prototype, synthesize, etc.) approved by CMPC. Additional requirements may be needed from TSCM, IT Communications/network administrators and Cyber.

Note: Copy machines used for the reproduction of CM must be designated and labeled as approved.

CMPC Essentials (Cleared Subcontractors)

- Limit reproducing CM to a minimum consistent with operational requirements or reproduction limitations.
- Ensure a PST-0004, *Reproduction Sign for Classified Equipment*, is conspicuously posted at copiers that are approved for classified reproduction.
- Copy machines must be cleared after classified documents have been reproduced. To clear a copy machine, three blank sheets must be run through the copier at the end of the process to ensure no images remain. The blank sheets that were run through the copier must be placed into the proper waste stream shred box.
- Double-check all of the reproduction paths before departing the area to ensure no trace of classified information is left behind on the equipment (e.g., on trays, screens, lids), floor, etc.
- Place all unacceptable or excess documents in the proper classified waste stream shred box.

Note: Only reproduce classified documents or matter in the presence of those who have the proper clearance level, and be conscious of need to know when others are in the area.

CMPC Essentials (Cleared Subcontractors)

Transmission requirements for classified matter

Note: Cleared subcontractors must contact Information Security to mail or ship classified matter on the CMPC Hotline at 806-477-6000

You must always use equipment/methods approved by CMPC for classified transmissions. Following are some examples of transmissions:

- Computers
- Mail
- Telephones
- Shipping
- Facsimiles (DeskAid-0205)
- Commercial express organization (i.e., Federal Express)
- Visual Teleconference Communication
- Hand carry off-site

CMPC Essentials (Cleared Subcontractors)

Hand Carrying Classified Matter:

Hand Carrying of classified matter is not allowed for subcontractors. Hand carrying must be performed by a federal employee (DOE, NNSA, DoD, etc.), or a Management & Operating employee (Pantex, Sandia, Los Alamos, etc.).

NOTE: If you have any questions pertaining to the Hand Carry process please contact the CMPC Hotline at 806-477-6000.

CMPC Essentials (Cleared Subcontractors)

Electronic Transmission of Classified Matter

Classified electronic transmissions must NOT take place over unclassified, non-secure telephone lines, computer lines, facsimile machines, or other similar electronic means. Approved methods of classified electronic transmission are as follows:

- Approved, secure telephone systems,
- Classified facsimile
- SecureNet

Individuals transmitting classified information via facsimile systems must confirm receipt (verbally or in writing) with the intended recipient. A log of incoming and outgoing classified facsimile activity is required. A classified document transmitted by an approved classified facsimile machine must be marked as a final document before transmission.

When classified drafts are transmitted by facsimile, they must be marked at the highest potential overall classification level and category.

CMPC Essentials (Cleared Subcontractors)

Destruction requirements for classified matter

All CM must be destroyed by approved equipment/methods and must be destroyed beyond recognition or reconstruction. CM is to be constantly attended to by authorized personnel or secured in a safe, vault, or VTR until it is properly sanitized and/or destroyed beyond recognition. Destroy CM in accordance with the current version of E-PROC-3210.

Only use destruction methods that are approved to ensure CM is physically altered, demolished, or reduced to a useless form in such a way that no classified information can be obtained from it.

Review Holdings:

All users must review classified holdings (e.g., parts, components, tooling, paper, media, etc.) on an ongoing basis to reduce CM to the minimum necessary and per Records Series (RS) guidance.

CMPC Essentials (Cleared Subcontractors)

Approved Equipment:

Only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be used to destroy classified information using any method covered by an EPL. Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be used for the destruction of classified information up to 5 years from the date of its removal from an EPL. In all cases, if any such previously approved equipment needs to be replaced or requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for the destruction.

Approved Methods:

The following are approved methods for classified destruction:

- Burning (excludes paper)
- Mutilating
- Shredding
- Pulverizing
- Pulping
- Chemical decomposition
- Melting

CMPC Essentials (Cleared Subcontractors)

Approved Methods (Cont.):

All excess classified documents must be placed into a classified destruction box and controlled as CM until Waste Operations (WasteOps) picks up the classified destruction boxes.

NOTE: Ensure no classified or Controlled Unclassified Information (CUI) paper enters our off-site waste stream. Do not put any kind of paper into the trash cans, (e.g. sticky notes, grocery lists, personal receipts)—all paper needs to be placed into its proper waste stream (either Classified or Sensitive shred boxes). The only thing that is acceptable for trash cans is food waste, cafeteria to-go boxes, used facial tissues, etc.

This also applies to all cardboard that is being sent off-site for recycling. Employees must remove or cover all address labels that may show employee names, badge numbers, building numbers, and other information that an outsider could use to complete their Operations Security (OPSEC) puzzle.

CMPC Essentials (Cleared Subcontractors)

Approved Methods (Cont.):

All business-related data gathering mediums that are no longer needed must be placed in the appropriate shred box (either Classified Data shred boxes or Sensitive Unclassified Data shred boxes). Examples of these mediums include documents containing Personal Identification Information (PII), Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), classified information, and meeting notes. In other words, no business-related paper should be thrown away in waste streams (e.g., trash containers, dumpsters, roll-off bins, receptacles, etc.), and shred boxes should be located away from trash containers.

Note: Shredders not producing the appropriate residue must be immediately taken out of service and have all residue removed and stored as CM, and notification must be made to the CMPC Office. The shredder must be unplugged, and a dated sign must be placed on the shredder that states it is out of service, to prevent further use.

NOTE: If you have any questions pertaining to the destruction process, please contact the CMPC Office.

CMPC Essentials (Cleared Subcontractors)

Destroy Nonaccountable Classified Documents:

- Place items for destruction in classified destruction boxes or approved receptacles.
- Maintain control of or properly store classified destruction boxes.
- Place an order via WOD Home Page (doe.gov) to arrange for Waste Ops to pick up classified documents for disintegration.
 - Waste Ops destroys classified documents in accordance with P6-2063.
 - Contact Cyber for media destruction requirements (see WI 02.02.04.05.18).

Destroy Accountable Classified Documents:

- Contact Cybersecurity for media destruction requirements (WI 02.02.04.05.18).
- Complete a PX-925-1.
- Destruction of accountable matter must be witnessed by an appropriately cleared individual, in addition to the person destroying the classified item; all individuals must have the appropriate clearance (including caveats).

CMPC Essentials (Cleared Subcontractors)

Destroy Classified Parts:

Destruction of classified parts, components, tooling, material, etc., are conducted according to the organizational procedures by the following facilities:

- Waste Ops
- Burning Ground
- Firing Site Complex
- HE Manufacturing

CMPC Essentials (Cleared Subcontractors)

Storage requirements for classified matter

CM must be under the direct control of an authorized person or secured in an approved safe, vault, or VTR.

Items of value susceptible to theft, such as funds, firearms, medical items, controlled substances, or precious metals, are NOT stored in security containers used to store CM.

Storage and Document Markings:

- Classified and unclassified documents that are commingled are marked at the highest level and category for each document.
- Cover sheets must be placed/applied to documents when taken out of a safe, vault, or a VTR.

Storage Repositories Include:

- Security Container/Safe – a filing cabinet-type safe that bears a test certification on the inside of the locking drawer/door and is marked “General Services Administration-Approved Security container (safe)” on the top or on a control drawer/door
- Vaults - Windowless enclosures with walls, floors, roofs, and doors designed and constructed to significantly delay penetration from forced entry and equipped with intrusion detection system devices on openings that would allow access
- Vault-Type Rooms (VTRs) - Department-approved rooms having combination-locked doors and protection provided by a department-approved intrusion alarm system that is activated by any penetration of walls, floors, ceilings, openings, or by motion in the room

CMPC Essentials (Cleared Subcontractors)

Initiate Classified Storage:

- Contact the repository administrator in CMPC for approval to place a safe/vault/VTR into use.
- Repositories must not be used to store items that may be a substantial target for theft.
- Repositories must conform to U.S. General Services Administration (GSA) standards and specifications.

Combinations:

Combinations must be managed by the repository administrator (RA) in CMPC and the lock and key administrator (LKA) in Physical Systems. The following guidelines apply to combinations:

- A record of granted access to storage repositories is maintained by the RA.
- Combinations are set by the LKA.
- Combinations must be available for authorized use.
- Combinations are changed by the LKA as soon as practical but no later than 6 months for
 - initial use of repository,
 - persons who do not possess the requisite access authorization,
 - formal access approvals, or
 - need to know for the information stored in the container.

CMPC Essentials (Cleared Subcontractors)

Standard Forms

The U.S. Department of Energy (DOE) has standard forms (SFs) associated with security repositories: (These forms may be obtained from the repository administrator in the CMPC Office.)

- SF-700 – Completed for each security repository and includes the names of who has access, or may be granted access to, combination(s). It must be affixed to the inside of the drawer/door.
- SF-702 – Completed to record each day in which a container may have been accessed. It is used to record the opening, closing, and checking of repositories.
- SF-701 – Use an SF-701, or an optional form, for a systematic means of checking end-of-day activities.
- OF 89 – This form, or a similar document, is used to record the maintenance history for each security container and must be placed inside the repository.

CMPC Essentials (Cleared Subcontractors)

Open and Secure Dial-Type Repository:

When walking up to the safe, ensure it is clear of any articles on top of the safe (only the SF702 should be on top).

To Open a Repository:

- Enter your information on the SF 702.
- Change the Open/Closed magnet to OPEN.
- First, open the safe by turning the dial to the LEFT until numbers appear. Continue turning until you reach your first number.
- Second, once you stop on the first number, turn the dial to the RIGHT until your second number appears.
- Third, once you stop on your second number, turn the dial to the LEFT until your last number appears.
- Finally, once you stop on your third number, turn the dial to the RIGHT until the word OPEN appears on the dial or it stops and then depress the handle on the drawer for it to open.

CMPC Essentials (Cleared Subcontractors)

When walking up to the safe, ensure it is clear of any articles on top of the safe (only the SF702 should be on top).

To Close a Repository:

- First, to close the safe, ensure that all doors or drawers are completely closed.
- Second, turn the dial to the left, counterclockwise, a minimum of one complete rotation. (a click sound can be heard within the dial)
- Third, spin the dial to the right, clockwise, a minimum of one complete rotation.
- Fourth, ensure that the safe is closed by trying to depress the handle and open the drawer.
- Change the Open/Closed magnet to CLOSED
- Enter the information on the SF 702.
- Ensure no Classified articles were left on top of the safe before leaving.

CMPC Essentials (Cleared Subcontractors)

Secure and Check a Dial-Type Repository:

YOU must take care to stay focused on the task at hand by minimizing interruptions; performing all necessary steps; and using deliberate, slow, and non-erratic movements while securing or checking a repository (safe, vault, VTR).

To secure and check a security container (safe), you should do the following:

- Visually check the immediate area and/or top of the container for any CM, and put it in the appropriate storage location.
- Close all safe drawers, and lock the XO-series combination lock by spinning the dial at least one full revolution/turn/rotation in the counterclockwise direction and then turning the dial at least one full revolution/turn/rotation in the opposite (clockwise) direction.
- Verify that all the container drawers are locked by attempting to turn the handle and simultaneously attempting to pull the drawer open. Then, check each auxiliary drawer by activating its thumb release and attempting to pull the drawer open.
- Record the closing/checking action on the SF-702 form.

CMPC Essentials (Cleared Subcontractors)

REMINDERS

Contact the LKA at extension 7413 for any technical questions regarding the security systems or in the case of a malfunction.

Additionally, the lightning bolt has **NO** relation to securing safes, vaults, or VTRs.

NOTE: Do NOT call a security police officer to check a safe, vault, or VTR.

Additional Repository Training for Custodians and Representatives:

Custodians and representatives must take training 564.44, Custodian/Representative Training.

CMPC Essentials (Cleared Subcontractors)

Report an Unsecured and Unattended Repository:

- You must take control of the CM (and continuously observe it).
- Immediately call the OC at extension 5000.
- The OC will contact the appropriate personnel, including the inquiry officials.
- The contents are checked as soon as practical for any evidence of discrepancies. These checks are done by the individuals listed on the SF-700 who serve as points of contact for call-outs.

CMPC Essentials (Cleared Subcontractors)

Nonconforming Storage

Nonconforming storage may only be used for CM that cannot be protected by the established standards and requirements. Organizations must submit a security plan to the CMPC Office (for PFO approval) with the following storage criteria:

- Results in protection effectiveness are equivalent to that provided to same level/category of CM standard configurations.
- Documentation must include an explanation as to why exercising this option is necessary.
- An analysis is performed to demonstrate the means by which equivalent security is to be provided.

CMPC Essentials (Cleared Subcontractors)

Permanent Burial

This option may be approved by PFO for the permanent placement of CM. It is not a form of CM destruction. The documentation must include the following:

- For active burial operations, a description of the entire placement process, including protection of CM prior to final burial
- Configuration of CM to be buried
- Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried CM
- Explanation of the current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the CM

Accountable CM is considered to meet accountability requirements when it is permanently placed into an approved burial configuration.

CMPC Essentials (Cleared Subcontractors)

Storage Inventory Anomalies

Inventory anomalies for classified parts or components must be reported to the Information Security manager within two business days by the owning organization.

- Inventory reconciliation evidence packages will be reviewed and approved by the Information Security manager.
- The Information Security manager will determine if the anomaly will be forwarded to IOSC.

CMPC Essentials (Cleared Subcontractors)

Protection measures given to classified matter during an emergency

In the event of a life-threatening emergency, plant personnel must conduct general guidance for the protection of CM:

- Follow instructions given by the OC or any on-scene emergency responders.
- Secure CM in an approved classified safe/vault/VTR if the situation allows time to take action.
- Leave CM behind if the situation does not allow time to secure it.
- Inspect classified holdings (i.e., safes, vaults, VTRs) upon return to the facility.
- Contact the OC at extension 5000 to report that CM was left unsecured and unattended.
- Notification of release: A notification of emergency release of classified information must be made to the Information Security manager, who will notify PFO.

CMPC Essentials (Cleared Subcontractors)

Criteria to handle Foreign Government Information (FGI) and Confidential FGI-Modified Handling Authorized (C/FGI-MOD)

The protection of FGI requires the same due diligence for the protection and control of CM. Although few individuals handle a small amount of FGI and C/FGI-MOD, it carries basic handling requirements with established international agreements, some of which are provided in the sections below.

Release Classified Information to Foreign Governments:

- Protect classified information at the highest restrictive level.
- Obtain approval from PFO by coordinating through the CMPC and Export Control offices.

Protection and Control Measures for Foreign Government Information:

- Protect FGI under the classification designated by the governing organization.
- Portion marking is not required.
- Involve a DC for any marking questions and re-mark with the U.S. equivalency.
- Maintain records for Confidential FGI (when designated by originating government).
- Secret FGI is accountable when designated by international agreements.
- When necessary, conceal FGI by marking it as if it were wholly of U.S. origin.

CMPC Essentials (Cleared Subcontractors)

Protection and Control Measures for Confidential FGI-Modified Handling Authorized:

Follow the requirements below when C/FGI-Mod requirements fall lower than those of U.S. Confidential information:

- Access requires only an established need to know when required for official duties and when authorized by originating countries.
- Include all fundamental markings and DC markings, unless foreign markings identify as such.
- Add “This document contains (name of country), (classification level) information to be treated as U.S. Confidential-Modified Handling Authorized.”
- Apply C/FGI-Mod cover sheet.
- Maintain physical control while it is in-use, and store it as required by foreign government.
- Reproduce as necessary to carry out official duties.
- Destroy it as CM.
- Transmit it as CM, unless waived by the originating government.

CMPC Essentials (Cleared Subcontractors)

Contacts

If you have any questions pertaining to the protection of classified matter, please contact the Information Security Hotline at 806-477-6000.