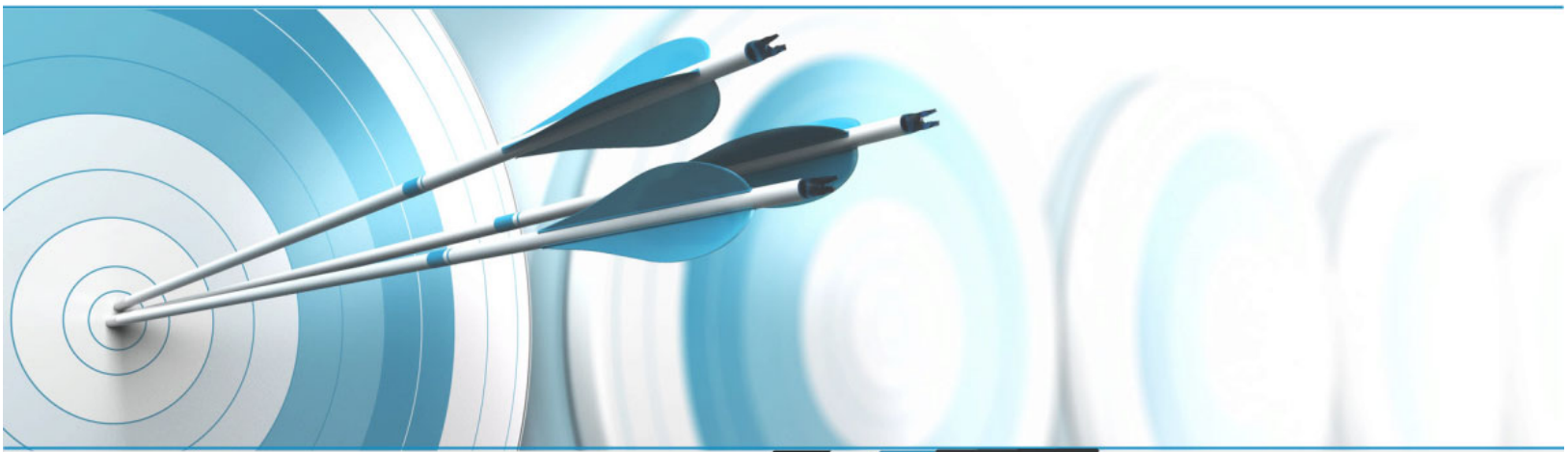

D50193408
Q50193407
Annual Security Refresher Briefing
D50193408 Q50193407

Annual Security Refresher Briefing

D50193408
Q50193407

Terminal Objective:

Upon completion of this course, attendees will identify basic classification policies and procedures, classified matter protection elements, personnel security elements, and counterintelligence awareness elements at Y-12 as outlined in this annual security briefing.



Page n of nn

Annual Security Refresher Briefing

D50193408
Q50193407

Enabling Objectives:

EO1: Identify basic classification security policies and procedures.

EO2: Identify classified information or matter protection elements.

EO3: Identify personnel security elements.

EO1: Identify basic classification security policies and procedures.

DOE O 475.2B, *Identifying Classified Information*

EO1: Identify basic classification security policies and procedures.

EO1: Identify basic classification security policies and procedures.

What is the purpose of the Y-12 Classification Program?

- The purpose of the classification program at Y-12 is to identify information that is classified under the Atomic Energy Act (AEA) or Executive Order 13526, Classified National Security Information, so it can be protected against unauthorized dissemination.

Y-12 Field Office Classification Officer – Jared Holas, 865-241-7209
Y-12 Classification Officer – Chris Poe, 865-241-0807
Classification Manager– Robbie Gamble, 865-574-1852

EO1: Identify basic classification security policies and procedures.

Classified Information

Classified information is classified by statute or executive order. It includes the following:

- Restricted Data (RD) or Formerly Restricted Data (FRD) classified by the AEA or by 10 CFR 1045, Nuclear Classification and Declassification
- Transclassified Foreign Nuclear Information (TFNI) classified by the AEA
- National Security Information (NSI) classified by Executive Order 13526 or prior executive orders

EO1: Identify basic classification security policies and procedures.

Classification Levels

The classification level indicates the level or degree of damage that could occur to national security should that information or matter be compromised.

Top Secret	Secret	Confidential
Information whose unauthorized disclosure could reasonably be expected to cause **EXCEPTIONALLY GRAVE** damage to national security that the appropriate official is able to identify or describe	Information whose unauthorized disclosure could reasonably be expected to cause **SERIOUS** damage to national security that the appropriate official is able to identify or describe	Information whose unauthorized disclosure could reasonably be expected to cause either **UNDUE RISK** to the common defense and security (if RD, FRD, or TFNI) or **DAMAGE** (if NSI) that the appropriate official is able to identify or describe

EO1: Identify basic classification security policies and procedures.

Classification Categories

RD	FRD	TFNI	NSI
Classified information concerning the design, manufacture, and use of atomic weapons; production of special nuclear material (SNM); or the use of SNM in the production of energy	Classified information concerning the military use of atomic weapons that has been removed from the RD category under Section 142d of the AEA	Classified information concerning foreign nuclear programs that has been removed from the RD category under Section 142e of the AEA	Classified information that has been determined under Executive Order 13526 or any predecessor executive order to require protection against unauthorized disclosure

EO1: Identify basic classification security policies and procedures.

Classified and UCNI Subject Areas

- Arms Control
- Fissile Isotope Separation
- Intelligence/Counterintelligence Information
- Weapon Research and Development or Technology Maturation
- Nuclear Weapon Disassembly and Reuse
- Improvised Nuclear Devices
- Safeguards, Security, and Nuclear Material Transportation
- Fissile Materials Disposition
- Nuclear Materials Control and Accountability Information
- Nuclear Materials Utilization/Production
- Special Materials Utilization/Production
- Nuclear/Radiological Incident Emergency Response and Consequence Management
- Uranium Processing
- Lithium Enrichment or Processing
- Naval Nuclear Propulsion Program
- Special Access Programs
- Technical Surveillance Countermeasures
- U.S./U.K. Mutual Defense
- Nuclear Assembly Systems
- Weapon Production and Military Use
- Nuclear Nonproliferation
- UCNI Utilization Facilities and Security Areas
- Additive Manufacturing
- Weapon Program Budget or Procurement Information
- Proliferant Enrichment Technology
- Securing International Materials

Identification of **ANY** Specified Weapon Programs

EO1: Identify basic classification security policies and procedures.

Required Classification Reviews

The following require a classification review:

- A newly generated document or material in a classified subject area that potentially contains classified information
- An existing, unmarked document or material that you believe may contain classified information
- An existing, marked document or material that you believe may contain information classified at a higher level or more restrictive category
- A document or material generated in a classified subject area and intended for public release (e.g., for a publicly available web page, for news organizations), including documents provided to or testimony given to Congress [Such information must be reviewed by the classification officer or a derivative classifier (DC) who has been delegated this authority in writing.]
- Printed output from a classified information system must be reviewed by a DC to determine the appropriate classification unless:
  - The output is a final document, has already been reviewed and marked
  - The output is a working paper marked at the highest potential level and category or marked and protected at the highest level and category of the information resident on the system.

EO1: Identify basic classification security policies and procedures.

Required Classification Reviews (cont.)

- An extract [i.e., a newly generated document that consists of a complete section (e.g., chapter, attachment, appendix)]
  - Extract from a classified document marked classified
    - If an extract is intended to be a stand-alone classified document, it must be reviewed by a DC.
    - If an extract is intended to be a stand-alone unclassified document, a declassification review is required.
  - Unclassified extract intended for public release
    - If an extract is unclassified and intended for public release, a classification officer review is required.
- Prepared text for a presentation in a classified subject area to be given in a classified setting

Contact the Y-12 Classification Office for assistance in extracting information or material from classified documents.

Any document or material intended for public release must be reviewed by and processed through the Y-12 Information Release Office (IRO).

EO1: Identify basic classification security policies and procedures.

Classification Challenges

- You are encouraged and expected to challenge the classification of information, documents, or materials that you believe are improperly marked.
- Challenges may be submitted to the Classification Office; however, any employee may submit a classification challenge directly to the DOE Office of Classification anytime. Information concerning contact with the DOE Office of Classification can be located in DOE O 475.2B, Attachment 4, par. 4.
- Under no circumstances are you subject to retribution for making a challenge.
- While the classification review is being processed, the information, document, or material that is the subject of the challenge must be protected at the current classification level and category or the classification level and category proposed by the challenge, whichever is higher, until a final decision is Information made.

For information on challenging a classification decision, please review **E-PROC-0031, *Identifying Classified***.

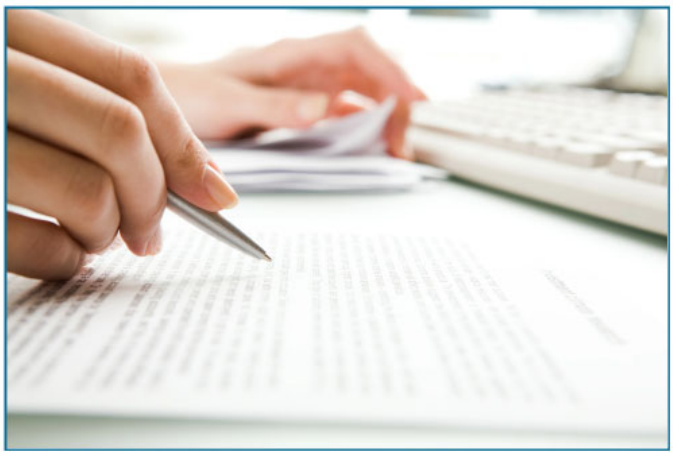
EO1: Identify basic classification security policies and procedures.

Declassification

Declassification is a determination by an appropriate authority that information no longer warrants classification or that documents or materials no longer contain classified information.

Who Performs Declassifications?

Derivative declassifiers—individuals authorized to declassify or downgrade documents or material in specified areas as allowed by his or her description of authority



EO1: Identify basic classification security policies and procedures.

Declassification

WHEN MUST A DOCUMENT OR MATERIAL BE REVIEWED FOR DECLASSIFICATION, AND WHO CAN REVIEW?

Classified documents ...	No. of reviews
being prepared for declassification in full	Two [first DC or derivative declassifier (DD); second must be DD]
being prepared for redacted versio	Two (first DC or DD; second must be DD)
requested under *Freedom of Infor* *and Mandatory Declassification R*	bracketing assification
NSI 1. With specific date or event c 2. With no specific date or ever 3. With obsolete declassificatio 4. Permanent historical records	second must be DD) table.
legacy markings 1. Official Use Only from 7/18/ 2. Restricted prior to 12/15/53	
referred to DOE by Other Govern containing or potentially containing RD, FRD, or TFNI	nd must be DD)

Executive Order	One Review	Two Reviews
13529	Date or event	25X1–9, 50X1–9
12958	Date or event	X1–X8 / 25X
12356	Date or event	OADR
12365	Date or event / D6	Review 20 Review 30
11652	Date or event / GDS	XGDS
10501 / 10964	Date or event / Group 4	Groups 1, 2, 3

- X1–X8 (different from the current 25X1–25X9)
- OADR = originating agency's determination required
- Group 1, Group 2, Group 3, Group 4
- GDS = general declassification schedule
- XGDS = exempt from general declassification schedule
- Review for declassification on (date)

Hover your mouse over the arrow to view the Obsolete Declassification table. You must view the table in order to proceed.

Annual Security Refresher Briefing

D50193408
Q50193407

EO1: Identify basic classification security policies and procedures.

Declassification

WHEN MUST A DOCUMENT OR MATERIAL BE REVIEWED FOR DECLASSIFICATION, AND WHO CAN REVIEW?

Classified documents ...	No. of reviews
being prepared for declassification in full	Two [first DC or derivative declassifier (DD); second must be DD]
being prepared for redacted version	Two (first DC or DD; second must be DD)
requested under *Freedom of Information Act/ Privacy Act and Mandatory Declassification Review Requirements*	First review – DC or DD performs bracketing Second review – DOE Office of Classification
NSI 1. With specific date or event declassification instructions 2. With no specific date or event for declassification 3. With obsolete declassification instructions 4. Permanent historical records 25 years old or older	1. One review by DD 2. Two reviews (first DC or DD; second must be DD) 3. See Obsolete Declassification table. 4. In accordance with 1, 2, or 3
legacy markings 1. Official Use Only from 7/18/49 to 10/22/51 2. Restricted prior to 12/15/53	One review by a DC or DD
referred to DOE by Other Government Agencies and containing or potentially containing RD, FRD, or TFNI	Two reviews (first DC or DD; second must be DD)

Hover your mouse over the arrow to view the Obsolete Declassification table. You must view the table in order to proceed.

Executive Order	One Review	Two Reviews
13529	Date or event	25X1–9, 50X1–9
12958	Date or event	X1–X8 / 25X
12356	Date or event	OADR
12365	Date or event / D6	Review 20 Review 30
11652	Date or event / GDS	XGDS
10501 / 10964	Date or event / Group 4	Groups 1, 2, 3

- X1–X8 (different from the current 25X1–25X9)
- OADR = originating agency's determination required
- Group 1, Group 2, Group 3, Group 4
- GDS = general declassification schedule
- XGDS = exempt from general declassification schedule
- Review for declassification on (date)

EO1: Identify basic classification security policies and procedures.

No Comment Policy

DOE has a no comment policy regarding classified information in the open literature or in the response to public inquiry on classified subjects.

A **comment** is any activity that could potentially allow an unauthorized individual to locate classified information or confirm the classified nature or technical accuracy of the information.

Commenting on classified information can result in greater damage to national security by confirming details such as its location, classified nature, or technical accuracy.

DO NOT comment on the classification status or technical accuracy of information.

For more information on the DOE no comment policy, please see Classification Bulletin GEN-16, *"No Comment" Policy on Classified Information in the Public Domain*.

EO2: Identify classified information or matter protection elements.

DOE O 471.6, *Information Security*

EO2: Identify classified information or matter protection elements.

EO2: Identify classified information or matter protection elements.

The protection and control of classified information is critical to our nation's security. At Y-12, classified information in all forms must be protected in accordance with all applicable laws, regulations, policies, directives, and other requirements.

Orders and procedures for protecting classified information or matter are as follows:

- DOE O 471.6, LtdChg 4
- E-PROC-3210, *Classified Matter Protection and Control*

Training

- Classified Matter Protection and Control (CMPC)
  - Introduces concepts of classified matter
  - Details how classified matter is protected
  - Identifies the controls in place to ensure classified matter is not compromised
- Who must complete CMPC?
  - Personnel whose job responsibilities include access (potential or actual) to classified information or matter (originating, handling, storing, using, accounting for, reproducing, transmitting, destroying, and/or emergency reporting)

EO2: Identify classified information or matter protection elements.

General Information Concerning the Protection of SNM

Some facilities at Y-12 may contain SNM. SNM is protected according to the material's category (i.e., quantity) and level of attractiveness (i.e., ease of turning it into a weapon) to an adversary.

Because SNM is an attractive adversary target, there are strict requirements regarding where it can be used or stored and who may have access to it.

If you will be working in an area that may contain SNM, you will be required to complete additional training.

EO2: Identify classified information or matter protection elements.

Access to Classified Information

Authorized access to classified information requires the following:

- Possession of the appropriate security clearance and access approvals
- Need to know
- Completion of required training
- Signing of the Classified Information Nondisclosure Agreement (SF 312)

EO2: Identify classified information or matter protection elements.

Purpose of the Classified Information Nondisclosure Agreement (SF 312)

As a condition of access, a cleared individual must complete an SF 312 before accessing classified information or matter or SNM. SF 312 is a legal, binding document between you and the U.S. government stating that you agree to protect classified information.

Any individual who refuses to execute SF 312 will be denied access to classified information or matter and SNM and reported to the cognizant security office.

The SF 312 informs you of the following:

- The trust that has been placed in you by providing you access to classified information
- Your responsibilities to protect classified information from unauthorized disclosure
- The consequences that may result from your failure to fulfill these responsibilities

Annual Security Refresher Briefing

D50193408
Q50193407

EO2: Identify classified information or matter protection elements.

Unauthorized Disclosures

Unauthorized disclosures are communication or physical transfers of classified information to an unauthorized recipient.

Penalties for Unauthorized Disclosure of Classified Information or Matter

- **Imprisonment**
- **Monetary fines**
- **Termination of security clearance (if applicable)**
- **Removal from any position of special confidence and trust that requires a security clearance**
- **Termination of employment**

EO2: Identify classified information or matter protection elements.

Administrative sanctions for the intentional disclosure of classified information may include the following:

- Formal reprimand
- Suspension of your security clearance
- Termination of employment

Legal sanctions for the intentional disclosure of classified information include the following:

- 18 U.S.C. 793, *Gathering, transmitting, or losing defense information*
- 18 U.S.C. 794, *Gathering or delivering defense information to aid foreign government*
- 18 U.S.C. 798, *Disclosure of classified information*
- 18 U.S.C. 1924, *Unauthorized removal and retention of classified documents or material*
- AEA, Section 224, *Communication of restricted data*

Annual Security Refresher Briefing

D50193408
Q50193407

EO2: Identify classified information or matter protection elements.

Protection

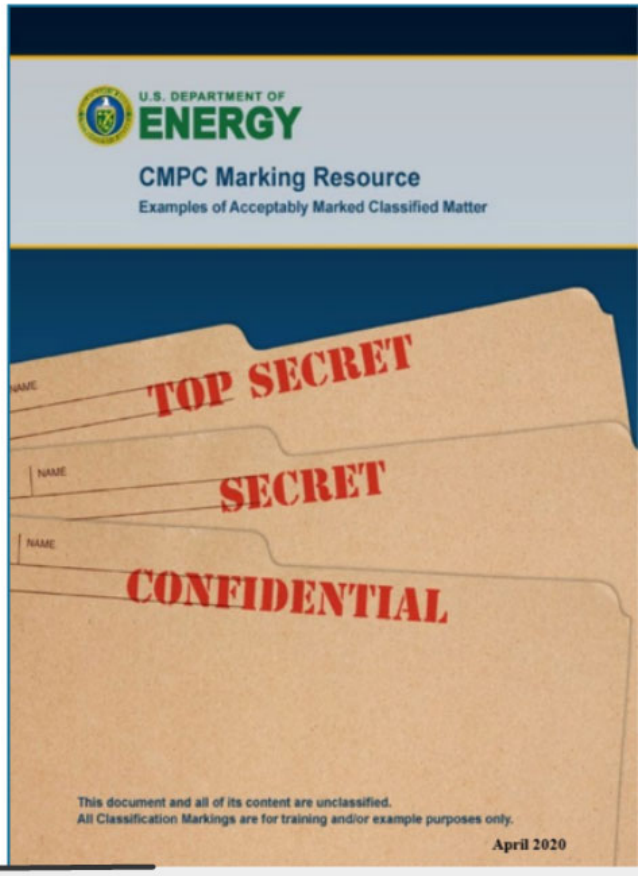
All members of the workforce are responsible for protecting classified information. Classified information or matter must be protected from release to those without the valid need to know or security clearance. Classified information must be under the direct control of an authorized holder responsible for its protection, or it must be stored appropriately. Classified matter should be kept within a limited area or higher. When not in use, classified matter must be locked in a repository, vault, or vault-type room that is approved by the General Services Administration.

EO2: Identify classified information or matter protection elements.

Marking

Ensure all classified matter is marked with the proper and complete classification markings. If the classified matter has not been reviewed by a DC, mark and protect the matter at the highest potential classification level the item is believed to contain until a DC reviews it.

For additional information on marking classified matter, please refer to CMPC Marking Resource – April 2020 (energy.gov).



EO2: Identify classified information or matter protection elements.

Dissemination

Protect classified matter from inadvertent or unauthorized release by ensuring classified work takes place only in a structure (not outside or in common areas) and, if electronic, on an approved system and network for the level and category the matter contains.

For assistance sending classified matter, please contact the Classification and CMPC offices.

EO2: Identify classified information or matter protection elements.

Disposal

- Classified matter may only be destroyed using a process and equipment approved by CMPC.
- Papers must be disposed of in appropriate Destruction and Recycle Facility bins located in a vault or vault-type room or shredded in an approved shredder.
- Classified matter intended for destruction must be protected until it is destroyed.

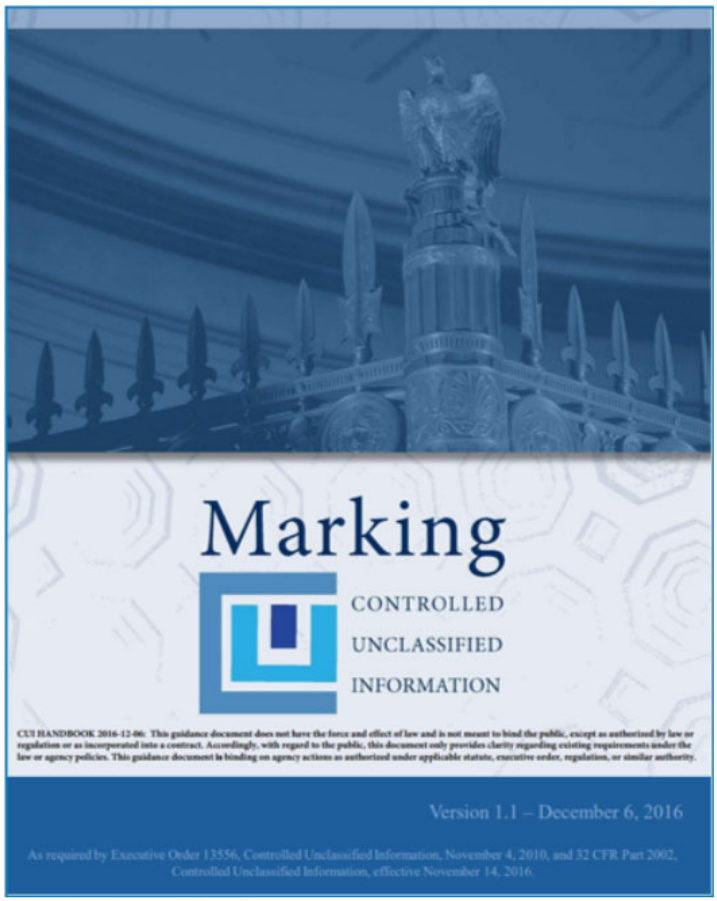
EO2: Identify classified information or matter protection elements.

Controlled Unclassified Information (CUI)

The CUI Program standardizes the way DOE NNSA handles information that requires protection under laws, regulations, or government-wide policies.

CUI Marking Handbook: *Marking Controlled Unclassified Information* (doe.gov)

DOE O 471.7, Controlled Unclassified Information



EO2: Identify classified information or matter protection elements.

Information Pertaining to Security Badges, Security Clearance Levels, and Access Controls

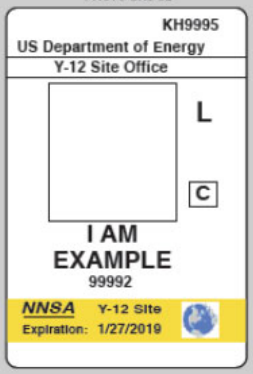
The following two types of badges are used at Y-12:

Local Site-Specific Only, or LSSO

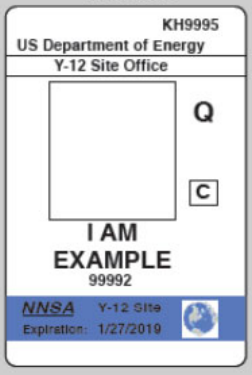
Y-12 LSSO BADGES

UNCLEARED PHOTO BADGE

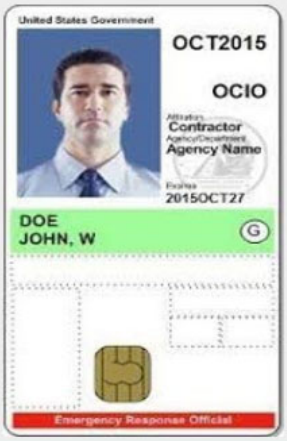
"L" CLEARED PHOTO BADGE



"Q" CLEARED PHOTO BADGE



DOE Security Badge (Homeland Security Presidential Directive-12, or HSPD-12)



EO2: Identify classified information or matter protection elements.

Badge Responsibilities

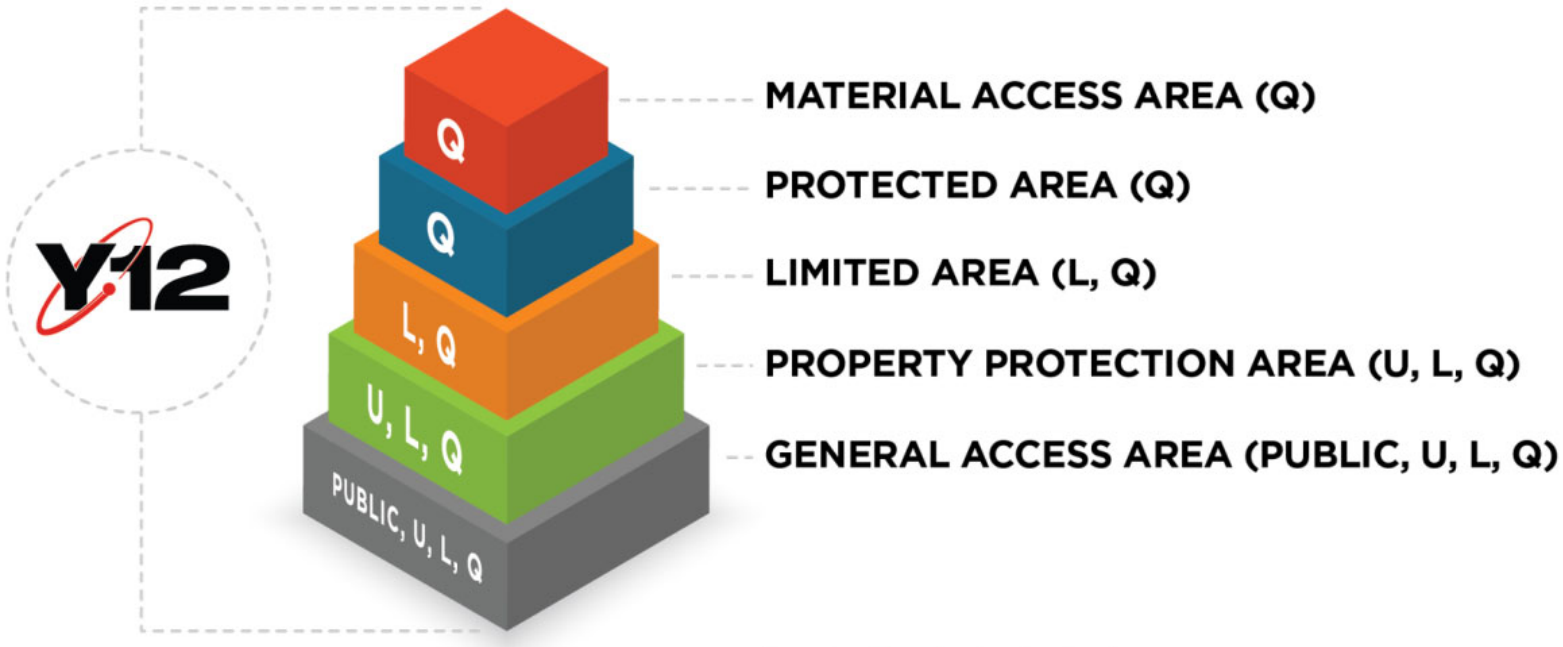
1. Protect your badge by using the holder provided to you when the badge was issued.
2. Protect your badge against loss, theft, or misuse.
3. Report a lost, stolen, or misused badge to the Y-12 Badge Office immediately (within 24 hours of discovery).
4. Protect the integrity of the badge by ensuring the badge is not altered, photocopied, counterfeited, reproduced, or photographed (other than for official government business).
5. Return the badge when it is no longer valid or required.
6. Surrender or return the badge when requested and according to Y-12 procedures.
7. Wear the badge conspicuously, photo side out, above the waist and on the front of the body while on-site.
8. Remove the badge, or obscure it from visual access, when not on federally controlled, owned, or leased property.

Annual Security Refresher Briefing

D50193408
Q50193407

EO2: Identify classified information or matter protection elements.

Controlling access to Y-12 is an essential part of everyone's responsibility for safeguarding classified information/matter and nuclear materials. The types of security areas at Y-12 are shown in the graphic.



EO2: Identify classified information or matter protection elements.

Responsibilities Associated with Escorting

Escorts must fulfill the following general requirements:

- Be L or Q cleared (as appropriate for the area).
- Be knowledgeable of security interests to be protected.
- Ensure measures are taken to prevent unauthorized access (physical, visual, or auditory) resulting in a compromise of classified information/matter.
- Ensure escorted personnel wear their badge in plain view above the waist and on outer clothing.
- Maintain visual contact with escorted personnel at all times. Remain in a position that will allow control of their movements/actions.
- Report any potential compromise of classified information/matter to the Y-12 Operations Center.

EO2: Identify classified information or matter protection elements.

Targeting and Recruitment Methods of Foreign Intelligence Services

The mission of the Y-12 Office of Counterintelligence is to protect and defend against hostile foreign intelligence activities and terrorism threats targeting Y-12.

Foreign Collection Methods/Indicators

According to the Defense Counterintelligence and Security Agency (DCSA), the following are the most common foreign collection methods and are used in over 80% of targeting cases:

- Unsolicited/unknown requests for information
- Inappropriate academic solicitation
- Suspicious network activity
- Targeting at conferences, conventions, and trade shows
- Solicitation and marketing/seeking employment or collaboration
- Foreign visits (one-time or long-term)
- Elicitation and recruitment

Note: These methods remain successful primarily because they can be hidden among legitimate business practices and plausible deniability.

EO2: Identify classified information or matter protection elements.

The Foreign Intelligence Services Targeting and Recruitment Process

1. **Spot and Assess**
   - Intelligence officers spot and assess an individual for potential recruitment. Adversaries are not necessarily looking for someone with a high level of access; sometimes the potential for future access or the ability of the recruit to lead to other high-value targets is enough to generate adversary interest.
   - Spotting and accessing can take place anywhere but is always approached in a nonthreatening, natural manner. Trade shows, business contacts, social events, or online venues such as chat rooms and social media are used for this process.
   - During this phase, the foreign intelligence services will often explore potential exploitable weaknesses that may be used as leverage against the recruit. These weaknesses could include the following:
     - Drugs or alcohol
     - Gambling
     - Adultery
     - Financial issues
     - Other weaknesses

EO2: Identify classified information or matter protection elements.

The Foreign Intelligence Services Targeting and Recruitment Process (cont.)

2. **Develop**
   Once a potential recruit has been identified, adversaries begin to cultivate a relationship with that individual. In the "development phase," meetings with the recruit become more private and less likely to be observable or reportable. By the time the "recruitment and handling phase" is initiated, the individual is likely emotionally tied to the adversary.

3. **Recruit**
   The actual recruitment may involve appeals to ideological leanings, financial gain, blackmail, coercion, or other motivators unique to that recruit. Some of these may manifest as observable and reportable behaviors.

4. **Witting or Unwitting Elicitation**
   Not all foreign intelligence services targeting ends in recruitment. Sophisticated social engineering efforts, including personal elicitation of information and targeted online phishing campaigns, can be used to gather information from an unwitting source.

If you suspect a member of a foreign intelligence service or a nonstate actor has approached you or anyone you know, please contact Y-12 Counterintelligence at CISTAFF@y12nsc.doe.gov.

EO3: Identify personnel security elements.

DOE O 472.2A, *Personnel Security*

EO3: Identify personnel security elements.

Adjudicative Guidelines:

The purpose of the Y-12 Personnel Security Program is to protect national security by ensuring only trustworthy and reliable individuals gain access to classified information and/or be assigned to national security–sensitive positions. A security clearance is an indication of this trust and confidence.

A security clearance is an administrative determination confirming an individual is eligible for access to classified information.

Sources of Legal Authority and Guidance

Legal authority and guidance for the Y-12 Personnel Security Program can be located in the following:

- 10 CFR 710, *Procedures for Determining Eligibility for Access to Classified Matter and Special Nuclear Material or Eligibility to Hold a Sensitive Position*
- Executive Order 12968, *Access to Classified Information*

EO3: Identify personnel security elements.

The Access Authorization Process

An individual's eligibility for a security clearance is based on the completion of a background investigation (SF 86, Questionnaire for National Security Positions) conducted for DOE NNSA by the primary investigative service provider (i.e., DCSA).

To conduct a background investigation, your Y-12 manager or subcontract technical representative will submit a clearance action request form to Personnel Security. Personnel Security will then initiate a request on your behalf in the electronic questionnaire (eAPP). You will complete all sections of the eAPP and sign certifications and releases. Should you have any questions while completing the eAPP, you may contact your clearance processor for assistance.

When completing the clearance request, you may also be required to provide supporting documentation. This documentation may include, but is not limited to, the following:

- Citizenship documentation
- Residence history
- Employment history
- Selective service number

EO3: Identify personnel security elements.

The Access Authorization Process (cont.)

Providing the information requested on the form is voluntary. However, not providing the information requested could impact your eligibility for the position or access to classified information. Withholding, misrepresenting, or falsifying information may also impact your eligibility and job status.

After you submit your eAPP, your Y-12 clearance processor will review it for accuracy and completeness. If the processor finds errors or missing information, you will be asked to correct the errors or provide the missing information.

After making any corrections to the eAPP, the Y-12 clearance processor will submit the completed clearance packet to DCSA to complete the background investigation.

During your background investigation, DCSA will examine criminal records (courts/law enforcement entities), employer history, educational history, and credit history. Investigators will also speak to your friends, coworkers, landlords, family, and neighbors. Additionally, your investigator may interview you to verify, expand upon, or clarify the information you provided in the eAPP.

EO3: Identify personnel security elements.

How Does the Adjudication Process Work?

The adjudicative process is in examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is also known as the whole-person concept. All available, reliable information about the individual—past and present, favorable and unfavorable—should be considered in determining national security eligibility.

The ultimate determination of whether the granting or continuing of national security eligibility is or is not clearly consistent with the interests of national security must be an overall common sense judgment based on careful consideration of the guidelines on the next slide. Each of the guidelines is to be evaluated in the context of the whole person.

EO3: Identify personnel security elements.

Adjudicative Guidelines:

- Guideline A – Allegiance to the United States
- Guideline B – Foreign Influence
- Guideline C – Foreign Preference
- Guideline D – Sexual Behavior
- Guideline E – Personal Conduct
- Guideline F – Financial Considerations
- Guideline G – Alcohol Consumption
- Guideline H – Drug Involvement and Substance Misuse
- Guideline I – Psychological Conditions
- Guideline J – Criminal Conduct
- Guideline K – Handling Protected Information
- Guideline L – Outside Activities
- Guideline M – Use of Information Technology

EO3: Identify personnel security elements.

When evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- The nature, extent, and seriousness of the conduct
- The circumstances surrounding the conduct, to include knowledgeable participation
- The frequency and recency of the conduct
- The individual's age and maturity at the time of the conduct
- The extent to which participation is voluntary
- The presence or absence of rehabilitation and other permanent behavioral changes
- The motivation for the conduct
- The potential for pressure, coercion, exploitation, or duress
- The likelihood of continuation or recurrence

EO3: Identify personnel security elements.

Due Process

If it is determined an individual is not eligible for a security clearance, administrative review procedures, as set forth in 10 CFR 710, are initiated to ensure the individual is afforded full due process in a manner consistent with traditional American concepts of justice and fairness.

Annual Security Refresher Briefing

D50193408
Q50193407

EO3: Identify personnel security elements.

Continuous Evaluation

Continuous evaluation is the review of the background of an individual who has been determined eligible for access to classified information. The purpose of the review, which can occur anytime during the period of eligibility, is to determine whether that individual does or does not continue to meet the requirements for eligibility to access classified information.

EO3: Identify personnel security elements.

Reporting Requirements for Clearance Holders and Applicants

Certain events and circumstances must be reported to Personnel Security immediately following the event or circumstance but no later than 3 working days after, unless otherwise indicated.

Personnel Security Reporting Contact:

clearancesy12@y12nsc.doe.gov or 865-574-7196

EO3: Identify personnel security elements.

What to Report:

- Arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by federal, state, or other law enforcement authorities for violations of law within or outside of the United States (Note: Traffic violations for which a fine of less than $300 was imposed need not be reported, unless the violation was alcohol or drug related.)
- Financial anomalies, including, but not limited to, the following:
  - Bankruptcy
  - Wage garnishment
  - Delinquency of more than 120 days on any debt
  - Unusual infusions of assets of more than $10,000 or greater, such as inheritance, winnings, or similar financial gain
- Action to legally change one's name
- Change in citizenship
- Use of any federally illegal drug (to include the abuse or misuse of any legal drug) and any drug- or alcohol-related treatment
- Relocation to a sensitive country of an immediate family member's residence
- Hospitalization for mental health reasons
- Marriage/cohabitation (***Note: The individual must complete DOE F 5631.34, Data Report on Spouse/ Cohabitant, within 45 days of marriage or cohabitation.***)

EO3: Identify personnel security elements.

What to Report (cont.):

- Foreign travel (official and unofficial) (***Note: Foreign travel must be reported via a completed DOE F 272.2, Personnel Security Information Reporting Form, 30 days before travel or as soon as possible.***)
- Contacts with foreign intelligence
- Elicitation
- Continuing association with foreign nationals
- Foreign activities:
- Direct involvement in a foreign business
- Opening of a foreign bank account
- Purchase of a foreign property
- Application for or receipt of a foreign citizenship
- Application for, possession of, or use of a foreign passport or identity card for travel
- Voting in a foreign election
- Adoption of a non-U.S.-citizen child

EO3: Identify personnel security elements.

Actions Reportable by Others:

Covered Y-12 personnel must notify Personnel Security of the following reportable activities/actions on the part of other covered individuals:

- An unwillingness to comply with rules and/or regulations or to cooperate with security requirements
- Unexplained affluence or excessive indebtedness
- Alcohol abuse
- Illegal use or misuse of drugs or drug activity
- Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified matter or other materials specifically prohibited by law from disclosure
- Criminal conduct
- Any activity that calls into question whether another covered individual's continued eligibility to access classified matter or hold a national security position is or is not clearly consistent with the interests of national security
- Misuse of U.S. government property or information systems

Annual Security Refresher Briefing

D50193408
Q50193407

You have completed this course. When you click **I Agree**, this window will close and you will receive credit in the LMS.

Acknowledgment

By submitting this statement, I acknowledge having been provided training or information.

I acknowledge that it is my responsibility to know and comply with the information presented. If I do not understand the information, it is my responsibility to ask for clarification.

I Agree | I Disagree