FACILITY SECURITY OFFICER WORKSHOP

Sandia National Laboratories

DAY 2 AGENDA | February 23rd, 2022 | Virtual Event

8:00 a.m. (MST)

Welcome Statement & Overview
Presented by: Samantha Flores, *Sandia Safeguards & Security Director and Facility Security Officer*

8:10 a.m. (MST)

Facility Clearance Requirements
Presented by: Jennifer Mahkee and Alexsea Montoya
Safeguards & Security Program: Contract Security Management
Review and discussion of facility clearance, Key Management Personnel clearances and Contract Security Classification Specification requirements.

8:35 a.m. (MST)

Non-Possessor Periodic Security Reviews
Presented by: Irene Nordquist
Safeguards & Security Program: Contract Security Management
Review of periodic security review requirements for non-possessing subcontractor facilities.

9:00 a.m. (MST)

Uncleared Personnel Identity Verification (UPIV)
Presented by: Gracie Raney
Safeguards & Security Program: Personnel Security Badge Office
UPIV requirements for Sandia subcontractor personnel.

9:20 a.m. (MST)

Subcontractor Security "Background" Reviews
Presented by: Joe Maruffi
Safeguards & Security Program: Personnel Security Clearance Office
FSO responsibilities for conducting security "background" reviews on applicable Sandia subcontractor personnel.

9:35 a.m. (MST)

Subcontractor DOE Personnel Clearances
Presented by: Lisa Lucero
Safeguards & Security Program: Personnel Security Clearance Office
Review of personnel clearance requirements for Sandia subcontractor personnel.

9:50 a.m. (MST)

Critical Information Lists
Presented by: Lauren McAuley
Safeguards & Security Program: Operations Security
Review of critical information lists and requirements for Sandia subcontractor personnel.

10:15 a.m. (MST) 10 MIN BREAK

FACILITY SECURITY OFFICER WORKSHOP

Sandia National Laboratories

DAY 2 AGENDA | February 23rd, 2022 | Virtual Event

10:25 a.m. (MST)

Security Incident Management Program Reporting Tools
Presented by: Zachary Aragon
Safeguards & Security Program: Security Incident Management Program
Guidance on when, what and how to report incidents of security concern to Sandia's Security Incident Management Program.

10:50 a.m. (MST)

Security Training & Resources
Presented by: Sylvia M. Chavez
Safeguards & Security Program: Security Awareness
Review of required security training and briefings. Review of Sandia Security Tools available to Sandia subcontractor personnel and FSOs.

11:20 a.m. (MST)

LUNCH BREAK

12:30 p.m. (MST)

Foreign Travel Requirements
Presented by: Veronica Robles
Safeguards & Security Program: International Security Operations
Review of Sandia official and unofficial foreign travel requirements and travel related training requirements for Sandia subcontractor personnel.

12:55 p.m. (MST)

Information Security
Presented by: Jeremy Pacheco
Safeguards & Security Program: Classified Matter Protection & Control
Review of information security requirements for Sandia subcontractor personnel.

1:25-1:30 p.m. (MST)

Workshop Wrap-Up
Presented by: Delvin Wood
Safeguards & Security Program: Contract Security Management Program
Workshop feedback and Sandia presentations.

Sandia National Laboratories | U.S. Department of Energy | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

Exceptional service in the national interest

FDAR/Significant Changes

For Subcontractor Facility Clearances

Merry Tidwell

Sandia National Laboratories

New Mexico Site

Security+ YOU

Think. Assess. Protect.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Who Needs to Report Changes?

- Any entity that holds or is in process for a DOE facility clearance
  - Includes entities with suspended facility clearances
- The designated Facility Security Officer (FSO)

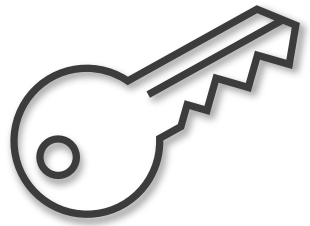
Key Terms: EED and FOCI

EED

- Entity Eligibility Determination
- Facility Clearance

FOCI

- Foreign Ownership, Control, or Influence
- Everything Together



What Changes Need to be Reported?

Anything pertaining to the Facility Data and Approval Record/Facility Clearance

Business Structure

- (ie: Privately Held Corporation to Publicly Held Corporation; Sole Proprietorship to LLC)

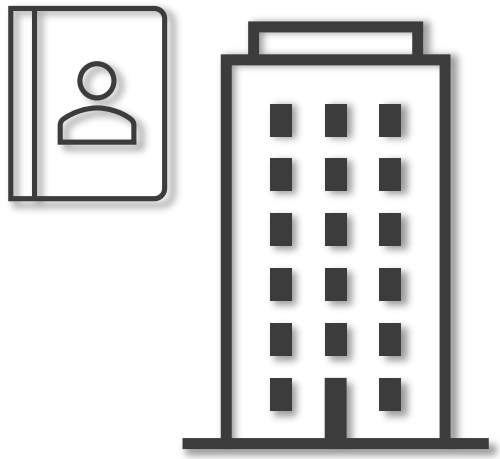
Company Name

- “Blocks and More” to “Building Innovations”
- “CB Services” to “Charlie Brown Services”
- “Smith Consulting” to “Smith Consulting Inc”

Tax ID Number

Address

- Even if its just adding/removing a suite #



What Changes Need to be Reported?

Anything pertaining to the Facility Data and Approval Record/Facility Clearance:

- **FSO (including FSO contact info)**
- **Board of Director structure or position titles**
- **KMP (owners, officers, directors, executive personnel)**
- **Ownership or Organizational Structure**
  - Stocks
  - Parents/Partners/Mergers/Buyouts
  - % of Ownership between KMP
  - Transferring a part of your business or assets to another entity
  - Negotiations

What Changes Need to be Reported?

Anything pertaining to the Facility Data and Approval Record/Facility Clearance:

- **Foreign Interactions**
  - Foreign contracts/business/interest/representatives
  - Adjudication or consultation with foreign persons
- **Bylaws/Operating Agreement/Articles of Incorporation, etc.**
- **Significant changes in financial information**
- **Termination of Facility Clearance with another agency**

What Changes DO NOT Require Reporting?

- **Hiring a new receptionist**
- **Changing the wording of a position title – examples:**
  - Our company is now calling all “Supervisors” “Team Leads”
  - Our sole owner’s title is now listed as CEO, but it is the same person as before

When to Report Changes?

- As soon as possible
- During Negotiations for a potential change
- Prior to executing the change if possible
- Takes time to update all systems

Where and How to Report Changes?

Under DOD Cognizance

- Report in NISS first
- Report via email to DOE sites you have subcontracts with

Under DOE Cognizance

- Report in eFOCI system
- Report via email to each DOE site you have subcontracts with

Where and How to Report Changes

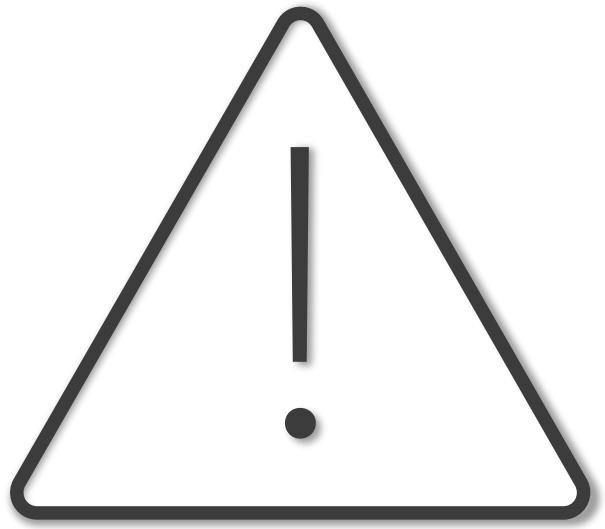
DRO Sites

- DOE Site that has responsibility to handle the significant change being reported
- Listed on your FDAR

Departments/Organizations at each site (Procurement, Clearance Office, Managers, etc.)

What if I choose not to report (Why?)

- Entity will be considered Out of Compliance
- Facility Clearance may be suspended or terminated
- Personnel clearances may no longer be available
- Future subcontracts may not be rewarded



Questions

Sandia National Laboratories

Exceptional service in the national interest

DOE Reporting Requirements Overview

Corey Munson

Personnel Security Department

Sandia National Laboratories

New Mexico Site

Security+ YOU

Think. Assess. Protect.

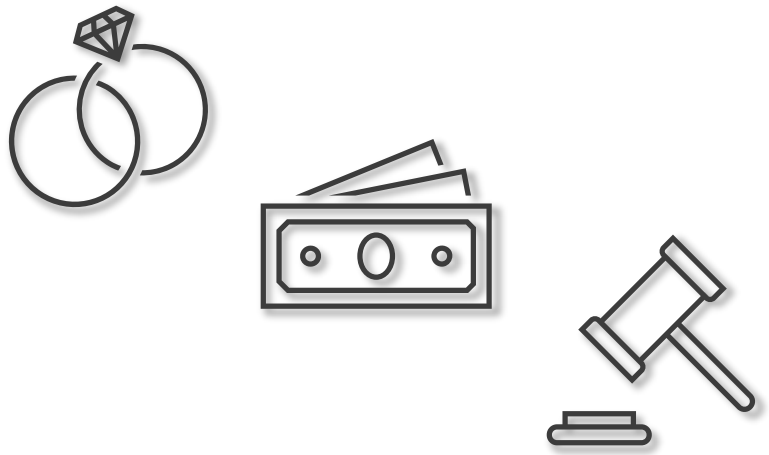
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Reporting Responsibilities and Requirements

- **DRIVERS**
  - DOE Order 472.2, *Personnel Security*
- **APPLICABILITY**
  - All individuals applying for (applicants) or in possession (holders) of a DOE security clearance
- **CATEGORIES**
  - Life circumstances
  - Law enforcement
  - Financial Matters
  - Drug/Alcohol Use
  - Foreign Interaction
  - Citizenship



General Reporting Roles & Methods

REPORTING ROLES

- Prime Contractor serves as the subcontractor reporting resource
- DOE/NNSA is the exclusive evaluating authority
- Reporting must occur immediately or as soon as possible, but no later than 2 working days after the event

HOW TO REPORT?

- Follow guidance from your Prime Contractor:
  - Kansas City National Security Campus
  - Sandia National Laboratories
  - Lawrence Livermore National Laboratory
  - Los Alamos National Laboratory

Sandia Reporting Roles, Methods, and Impact

REPORTING ROLES

- Sandia National Laboratories (SNL) serves as the reporting resource
- DOE/NNSA is the exclusive evaluating authority

HOW TO REPORT?

- Reporting Guide as an initial reference
- Security Connection: (505) 845-1321 | security@sandia.gov
- Personnel Security: (505) 844-8902 | persecreporting@sandia.gov

IMPACT

- Dependent on the nature of the item reported
- DOE/NNSA
  - May or may not choose to inquire further (e.g., LOI)
  - Their determination based on 'whole person concept'
- Don't jump to conclusions and bear in mind that reporting itself is a positive factor!

DOE and SNL
REPORTING REQUIREMENTS OF SECURITY INTEREST

Revised: April 28, 2021

Instructions

- The events and circumstances described below are reportable by the individuals specified in the spanning subheadings.
- All reporting must occur immediately or as soon as possible, but no later than two (2) working days after the event or circumstance.
- To begin the reporting process, contact Security Connection at 321 from a Sandia landline, 505-845-1321 from any phone, or security@sandia.gov.

Members of the Workforce (MOWs)

All MOWs are required to report the events/circumstances specified below, when applicable. However, the red highlighted items are applicable only to clearance holders and clearance applicants.

GENERAL REQUIREMENTS

1. Become aware of information that raises concerns of personnel security interest* about others who are applying for or in possession of a DOE security clearance.
   *"Concerns of personnel security interest" include but are not limited to the reportable circumstances cited in this guide. Note: Individuals who report circumstances about others may be asked to provide additional, corroborative information.
2. Approached or contacted by any individual seeking unauthorized access to classified matter or special nuclear material (SNM).

LIFE CIRCUMSTANCES

3. Marry or cohabitate.
   Note: A cohabitant is a person who lives in a spouse-like relationship or with a similar bond of affection or obligation, but is not a legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).
4. Legal action taken for a name change.

LAW ENFORCEMENT

5. Arrested or subject to criminal charges (including dismissed charges), citations, tickets, summonses, or detentions by federal, state, or other law-enforcement for violations of law within or outside the U.S.
   Exception: Traffic violations for which a fine of up to $300 was imposed need not be reported, unless the violation was alcohol- or drug-related.*
   **"Imposed" means agreeing to pay the fine, or a court ruling to pay, exclusive of court fees or other administrative costs.*

FINANCIAL MATTERS

6. Personal or business-related filing for bankruptcy.
7. Garnishment of wages (e.g., for debts, divorce, child support).

CITIZENSHIP

8. Change in citizenship (i.e., U.S. or foreign) or acquisition of another country citizenship(s).

DRUG USE

9. Use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction.
10. Treatment for drug abuse.
11. Positive (i.e., unfavorable) drug test regardless of source (e.g., court-ordered, military, employment).

ALCOHOL USE

12. Treatment for alcohol abuse.

MENTAL HEALTH

13. Hospitalization for mental-health reasons.

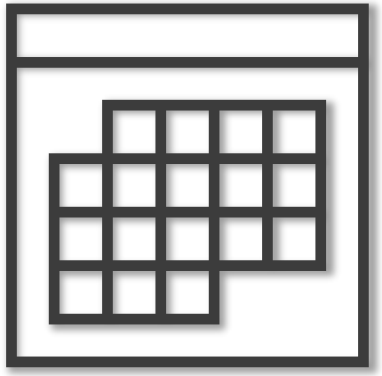
FOREIGN TRAVEL

14. Travel to a sensitive country for personal reasons.
    Note: Reporting prior to travel is preferred. A list of sensitive countries is available at the Counterintelligence (CI) website. Keeping a record of all personal foreign travel is recommended as a reference for future clearance (re)investigations.
15. Travel to any country where discussions with sensitive-country foreign nationals regarding sensitive subjects are anticipated or have already occurred.
    Note: This includes chance meetings where sensitive-country foreign nationals are in attendance.
16. Travel to any country where sensitive subjects will be discussed.

Forthcoming Changes to Reporting Requirements

Revision of DOE O 472.2 to comply with Security Executive Agent Directive (SEAD) 3

- Expected year 2022
- Notable changes include:
  - Unofficial Personal Foreign Travel
  - Additional Foreign Activity items
  - Financial Anomalies



Items to Remember/Keep in Mind

- ✓ Review/understand your reporting requirements
- ✓ Be honest & truthful
- ✓ Be timely & available
- ✓ Know your references

Questions

Sandia National Laboratories

Exceptional service in the national interest

Contract Security Management

Facility Clearances, CSCSs, DOE KMP Clearances

Jennifer Mahkee and Alexsea Stringfellow

Sandia National Laboratories

New Mexico Site

Security+ YOU

Think. Assess. Protect.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Facility Clearances

Facility Clearance Components

- Subcontract requiring personnel clearances (contains Clause 610- FO, *Security Requirements*)
- Contract Security Classification Specification (CSCS)
- Favorable Foreign Ownership, Control or Influence (FOCI) determination
- Facility Security Officer (FSO) designation and training
- Key Management Personnel (KMP) security clearances (executives, FSO etc.)
- Security Requirements Plan
- Ongoing Assessments
  - Periodic Security Review

Facility Clearances

What is it?

- DOE/National Nuclear Security Administration's approval of a subcontractor entity's eligibility to access, receive, generate, reproduce, store, transmit, or destroy:
  - Classified matter
  - Special Nuclear Material (SNM)
  - Other hazardous material presenting a potential radiological, chemical, or biological sabotage threat
  - DOE property of significant monetary value, exclusive of facilities and land values

FSO Responsibilities - Facility Clearance

Report Significant Changes

- All circumstances that would change any answer on the SF 328 from “No” to “Yes,” which must be reported by submitting a changed condition SF 328
- When contracting with a Foreign Entity
- If there is any change in the Foreign Ownership, control or influence of your company

Report Anticipated Actions

- Action to terminate business or operations of subcontractor or parent
- Legal actions to initiate bankruptcy
- Entering into negotiations with non-U.S. Citizens

Other Changes

- Changes in name or address
- Any changes in Key Management Personnel

Contract Security Classification Specification (CSCS)

What is a CSCS?

- A contractually binding form between SNL and the subcontractor entity outlining security and classification guidance for the classified information disclosed during the performance of the subcontract.
- CSCS forms are used to register each subcontract and begin the facility clearance process if the subcontract is for a company that does not yet hold a clearance interest with SNL
- Approved CSCS forms individually register each security interest/contract with DOE/NNSA
- Subcontractor personnel clearances can be processed once a CSCS is active
- A CSCS form identifies the classification level of work and classification guidance of the work to be performed

Contract Security Classification Specification (CSCS)

When is a CSCS required?

- When an SNL subcontract requires personnel clearances in the performance of work.
- When a company that holds an SNL subcontract needs to further subcontract work to other companies that will require personnel clearances in the performance of their work.
- When a parent or partner company of a subcontract company requires clearances.
- When any information on an approved CSCS changes, a revised CSCS is required.

FSO Responsibilities - CSCS

You will receive an updated CSCS every time you:

- Have a new cleared contract approved
- Have an existing contract renewed or revised (updating level and category of information)

You will need to Verify information on CSCS form is correct. Most commonly, you will need to verify these particular blocks:

- 4b/c – Verify the contract # and end date
- 7 – Name and address
- 6 - General Statement of work identified
- 9b (DOE) & 9b (Non-DOE) - Actual Place of Performance of Contract
- 10 - Clearance and Storage (level and category).
  Note: 10b indicates storage level at the contractor facility. If a category/level (other than "U") is in this block, SNL/DOE classified is at the contractor's facility.
- 12 – Classified matter location

FSO Responsibilities – CSCS (cont)

- Notify Facilities Approval Team of needed corrections
- Provide copies of CSCS forms to auditors upon request and notify remote sites coordinator of auditor request

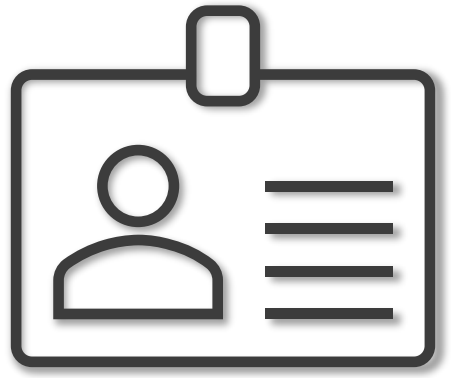
Key Management Personnel Clearances

New requirement from Department of Energy

- All Key Management Personnel (KMP) must receive a DOE personnel clearance regardless if their facility clearance is under DOE Cognizance in order to maintain or obtain a DOE facility clearance.

KMP are identified by DOE and DCSA

- KMP must obtain and maintain DOE personnel clearances at the same level of the highest subcontract that the company holds at a DOE facility.



Resources Available

Security Toolcart https://www.sandia.gov/security/home/facility-clearance/

You will find:

- FSO Foreign Ownership Control and Influence (FOCI) Responsibilities & Facility Clearance Reporting Requirements
- S&S PLN-120, Non-Possessing Subcontractor Security Requirements Plan (NPSSRP)
- PHY-210DE, Facility Security Officer Overview
- Flow Down of Requirements
- Other Security-Related information

Contract Security Management Team

You can reach us at farateam@sandia.gov

Questions

Sandia National Laboratories

Exceptional service in the national interest

Contract Security Management

Periodic Security Reviews

Presented by:

Irene Nordquist

Sandia National Laboratories

New Mexico

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Background - *DOE O 470.4B, Safeguards & Security Program*

As part of this DOE order, CSM is required to verify that Sandia subcontractors follow DOE security requirements.

DOE Order 470.4B, Chg. 3, Safeguards and Security Program, Attachment 2, Section 2. Survey, Review and Self-Assessment Programs,

> **5. REQUIREMENTS:** Contractors are responsible for ensuring that the following activities related to program reviews and self-assessments are conducted at facilities and sites under their cognizance, and for ensuring that assistance and data are provided as directed to Federal security personnel during survey activities. Procedures applicable to these activities must be documented in facility or site security plans.
>
> **a.** Review security programs on a continuing basis.
> **b.** Conduct formal self-assessments at intervals consistent with DOE direction and risk management principles
> **c.** Prepare and submit to the DOE cognizant security office formal reports of self-assessments and related findings and corrective actions.

- This requirement has been included in the S&S-PLN-120, *Non-Possessing Subcontractor Security Requirements Plan* (NPSSRP).

- This process is a recent implementation of a long-term requirement. Though some Periodic Security Reviews may have been conducted for your facility historically, this is a new implementation of the requirement found in DOE O 470.4B.

What's required of you?

Self-Assessment

- You will be required to documentation of a self-assessment of your Safeguards & Security Program
- If you do not currently have a self-assessment process, CSM provides an inclusive checklist to fulfill the requirement

CSM Review

- A member of the CSM team will review your results with you and go over any provided documentation

Report

- Following your self-assessment and meeting with CSM, a report will be drafted and sent for your concurrence
- If there are any areas of concern, additional follow-up may be required

Finalizations

- After completing the review, the CSM team will not require the documentation of your company's self-assessment for another five years
- CSM may require your company to provide documentation of your self-assessment more frequently if extenuating circumstances exist

Process

Engagement Letter

- CSM will notify you of your upcoming Periodic Security Review through an engagement letter

Self-Assessment

- You will need to provide documentation of your completed Self-Assessment of your Security program.
- CSM provides a self-assessment checklist if you do not currently have a self-assessment process

Review

- CSM team member will go over results from self-assessment and identify any questions, areas of good practice, and areas of concern

Report

- A member of the CSM team will draft and provide you a report summarizing the discussion at the Review session.
- You will be asked to provide your concurrence on this report.

Finalizations

- Once report is complete, the CSM team uploads the report and results from self-assessment into your company's folder
- You will not require a Periodic security review for another 5 years (unless extenuating circumstances exist)

Moving Forward

Contract Security Management is not assessing your company through this process.
We are verifying:

- You are completing self-assessments of your security program
- You are aware of the requirements of your security program
- You are fulfilling those requirements

Resources

- We have developed a self-assessment checklist that covers all the requirements of your security program
  - You are not required to complete our checklist if you can provide other documentation of a self-assessment conducted for your security program

- The Contract Security Management team is happy to help and guide you through the Periodic Security Review process. You can reach us at farateam@sandia.gov.

Questions?

Sandia National Laboratories

Exceptional service in the national interest

Personal Identity Verification for Uncleared Subcontractors (UPIV)

Gracie Raney

Sandia National Laboratories

New Mexico Site

Security+ Think. Assess. Protect. YOU

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

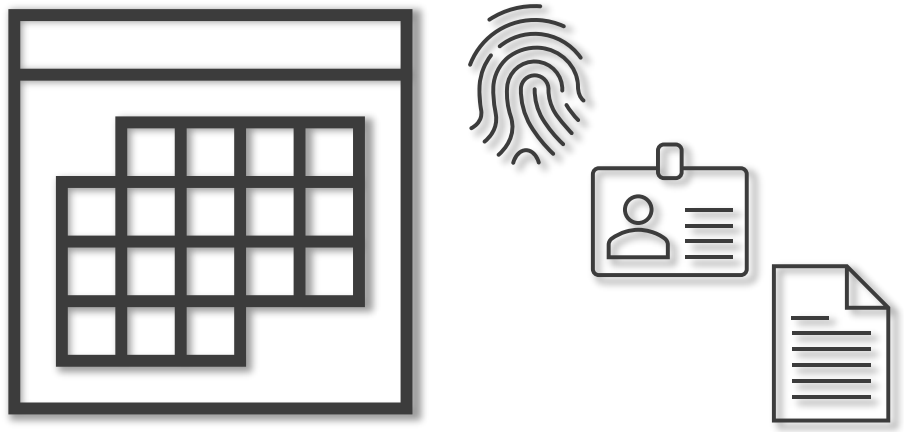
What is NNSA SD 206.2?

- NNSA SD 206.2 *Implementation of Personal Identity Verification for Uncleared Contractors* is a Homeland Security Presidential Directive (HSPD)-12 mandating the development and implementation of a Government wide standard to identity proof all subcontractors.
- Uncleared subcontractor and lower-tier subcontractors requiring physical access to SNL and DOE/NNSA owned or leased facilities and/or cyber access (logical access) greater than 179 calendar days must be processed for PIV.

*For Sandia National Labs and all remote sites, we have lowered the threshold to 120 days to ensure compliance with 179 calendar days per DOE.

What does UPIV Consist of?

- Sandia Total Access Request Tool (START) request must be submitted for any subcontractor who requires physical and/or cyber (logical) access greater than 120 calendar days.
- Completion of Questionnaire for Non-Sensitive Positions (SF-85) and Declaration for Federal Employment (OF-306) – This will enable DOE/NNSA to start a Tier 1 background investigation.
- Enrollment in USAccess – 2 forms of identification, photo and fingerprints

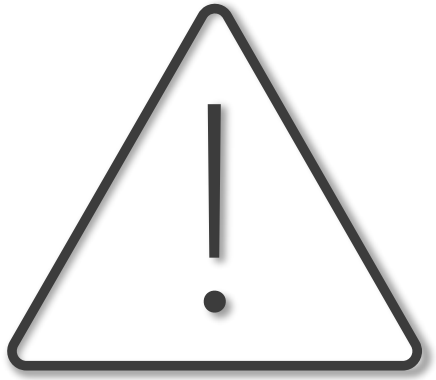


Important Notes to Complete UPIV

- Contractors will be expected to complete a UPIV Intake Sheet so we can ensure we have your current information.
- Must have a valid email address. This is how subcontractors will receive notifications to complete their SF-85, OF-306 and enrollment appointment.
- Valid forms of identification for Enrollment (Driver's License, Passport, Birth Certificate, Social Security Card, Voter's Registration Card).
- Failure to comply with the UPIV process within time requirements will result in badge deactivation and not being able to work until the actions are completed.
- Subcontractor companies are responsible for providing personnel with computer resources to schedule enrollment appointment and complete the background investigation paperwork for the PIV process.

What happens if I fail UPIV?

- If you have an Unfavorable UPIV, you will no longer be able to access the site physically and/or logically.
- The process can be appealed, but you cannot work at Sandia while going through this process.
- If the appeal fails, you can reapply to go through the UPIV process one (1) year after the failed date.



UPIV Contact Information

PROGRAM LEAD – Gracie Raney

Questions on UPIV process – Email upiv@sandia.gov

Questions on eQIP/OF306 – Email clearance-nm@sandia.gov

Questions

Sandia National Laboratories

Exceptional service in the national interest

Subcontractor Security Background Reviews

Personnel Security Background Review Office

Joe Maruffi

Sandia National Laboratories

New Mexico Site

Security+ YOU

Think. Assess. Protect.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Subcontractor Background Reviews

DRIVER:

Per the Department of Energy (DOE) DEAR 952.204-2 Security Clause the following is required:

- All contractors and subcontractors **must** conduct a thorough background review as defined in 48 CFR 904.401(Federal Acquisition Regulations System)

- This background review is not required for personnel possessing a current clearance from DOE or another federal agency

Background Review Requirements

Background reviews must include:

1. Testing for illegal drugs for all uncleared employees prior to selecting individuals for any position requiring a DOE clearance
2. Verifying educational background:
    - Any high school diploma or equivalent obtained in the past five years
    - All degrees or diplomas granted by an institution of higher learning
3. Contacting listed employers for the last three years and listed personal references
4. Conducting law enforcement checks
5. Conducting a credit check

Background Review Requirements (cont.)

All requests for initial access authorization must include a record and certification of the following information concerning each uncleared applicant or employee who is selected for a position requiring a DOE clearance:

- The date the review was conducted
- Each entity that provided the information concerning the individual
- A certification that all information collected during the review was reviewed in accordance with the Subontractor's personnel policies
- A certification that the review was conducted in accordance with all applicable laws, regulations, and executive orders

Risks of not conducting Subcontractor Personnel Reviews

Failure to complete a subcontractor background review can lead to adverse actions, to include:

- Denial of a DOE security clearance
- Employee being removed from the subcontract
- Denied physical access to Sandia sites
- Delayed times in onsite work or project
- Subcontractor failing to meet official deadlines

Questions and Answers

Sandia National Laboratories

Exceptional service in the national interest

Personnel Security
Clearance Processing

Lisa Lucero, Clearance Office Program Lead

Sandia National Laboratories

New Mexico Site

Security+ YOU

Think. Assess. Protect.

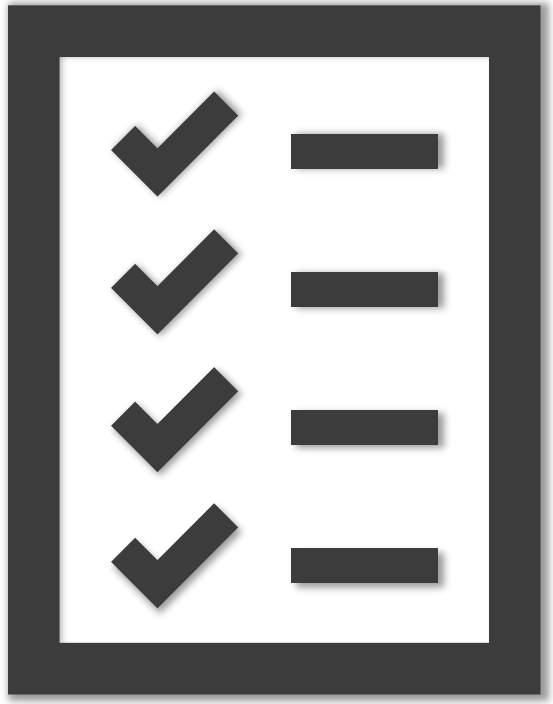
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Goals & Objectives

- Clearance Process
- How can you help?
- Periodic Clearance Reconciliation
- Clearance Termination Process
- Clearance Processing times



Clearance Process

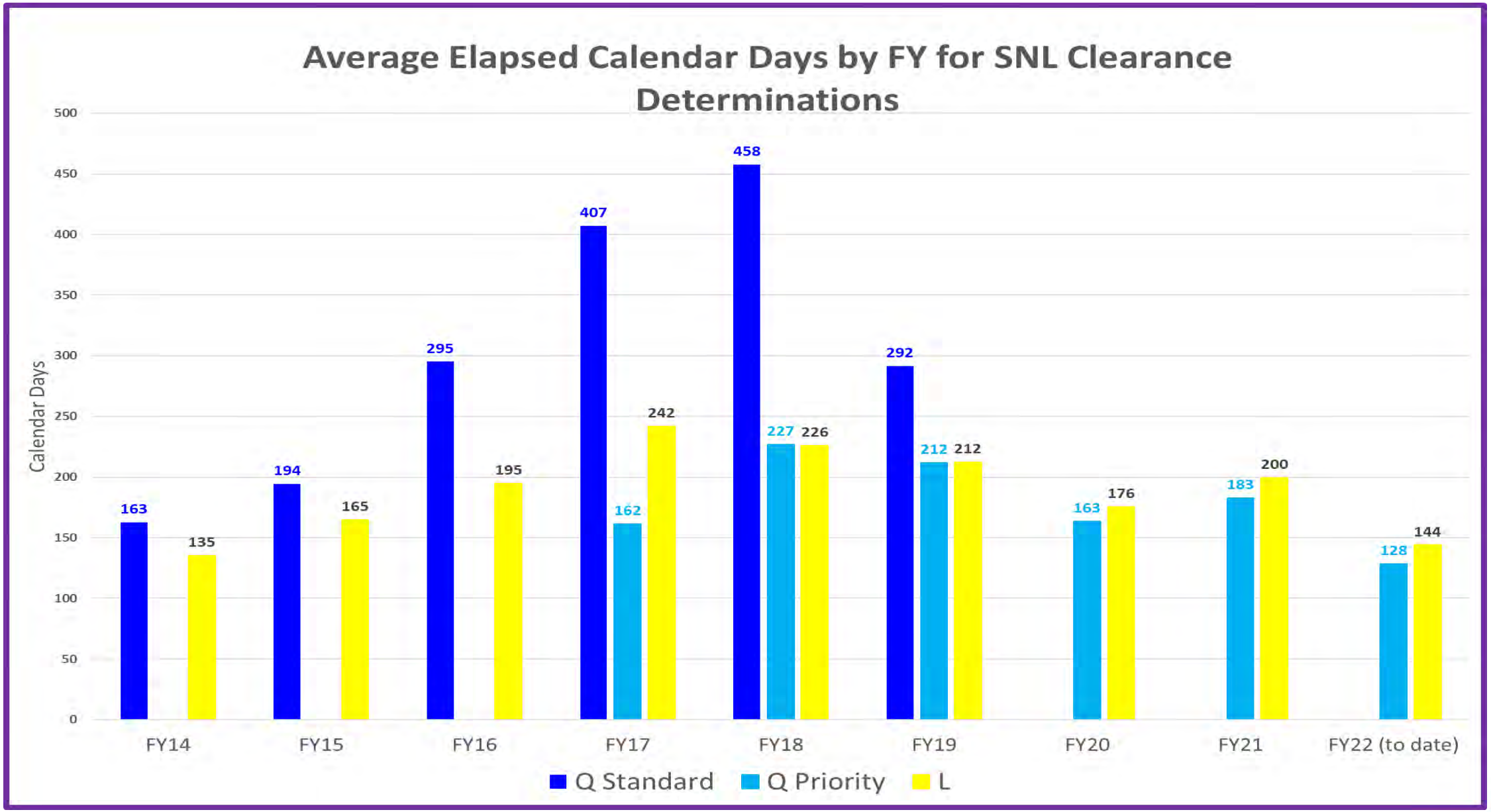
Stages

- Application/Initiation (SNL)
  - Favorable Drug Test
  - Personnel Identity Verification (PIV) i.e. Fingerprints
  - DOE Security Acknowledgement Form
  - Completion of the e-QIP
- Investigation (DCSA & FBI)
  - Tier 3/3R (L) & Tier 5/5R (Q)
- Adjudication (DOE)
  - DOE is the sole determining authority
  - Favorable: Grant, Reinstate, Extend, Reciprocity
  - Unfavorable: Deny, Suspend, Revoke
- Reinvestigation/Continuous Evaluation

How Can You Help?

- Email Notices
  - Clearance Processing/Tasks
  - Periodic Clearance Reconciliation
  - Delinquent notices
- Security Clearance Termination
  - Timely submission of forms
  - Badge retrieval

Clearance Processing Times



Questions

Sandia National Laboratories

Exceptional service in the national interest

Security Training & Resources

Sandia Security Toolcart

Sylvia M. Chavez

Sandia National Laboratories

New Mexico Site

Security+ YOU

Think. Assess. Protect.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Security Toolcart

Provides current security forms, briefings, trainings, and security topics, such as:

- Security News and Updates
- How to obtain/maintain a clearance
- Security Termination Information
- DOE & Sandia Reporting Requirements

Security+ Think. Assess. Protect. YOU

If you have questions, contact Security Connection 505-845-1321

Security Toolcart

Export/Import Control

Helpline: (505) 845-7000

Email: eico@sandia.gov

Facility Clearance

FSO Responsibilities

Flowdown of Requirements

Email: farateam@sandia.gov

Frequently Used Forms

Data Report on Spouse/Cohabitant (DOE F 5631.34)

Request for Visits or Access Approval (DOE F 5631.20)

International Travel

Process for Official International Travel Approval

Required Training for Official International Travel

Email: CIHelp@sandia.gov

Official Use Only (OUO)

Freedom Of Information Act Exemption List
Protection of OUO
Dissemination of OUO

Prohibited/Controlled Items

Explosives, personally-owned bladed weapons
KAFB Firearms Policy
Visitor-owned Computer Devices & Media
Mobile devices
Medically Necessary devices

Uncleared Foreign Nationals

Time Requirements
Required Documentation
Badging and KAFB Pass

Security+ YOU
Think. Assess. Protect.

If you have questions, contact Security Connection 505-845-1321

Security News

Security+ YOU News
Think. Assess. Protect.
April 7, 2021

- Security News Announcements that may impact contractors
- Security News Archive back to 2015 for reference and links
- COVID-19 Work Practices for Subcontractors

If you have questions, contact Security Connection 505-845-1321

Security Clearances & Badges

Badge Office

- Request Access (Cleared or Uncleared) for a Visitor
- Request Access for a Member of the Workforce
- DOE Personal Identity Verification (PIV) Credential Process
- Reporting Lost, Stolen, or Forgotten Badges
- Defense Biometric Identification System (DBIDS) at KAFB
- Uncleared Personal Identity Verification (UPIV) Process

Drug Testing

- Initial
- Random
- Failure to Report
- Verified Positive Drug Test Procedure
- Use of Medical Marijuana/Another person's prescription drugs

Clearance Office

- Request Access (Cleared or Uncleared) for a Member of the Workforce
- The DOE Personnel Clearance Process
- Application Criteria
- Sequence of Events
- DOE Adjudication
- DOE Due Process of Adverse Determinations
- DOE Clearance Topics of Interest
  - Background Investigations & Reinvestigations
- DOE Applicant Tracking System (ATS)

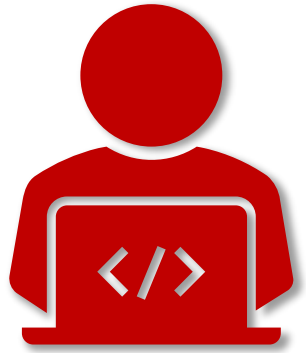
Reporting Requirements

- Current Reporting Requirements handout

If you have questions, contact Security Connection 505-845-1321

Security Briefings & Trainings

- **SEC050,** Initial Security Briefing (pdf)
- **SEC150,** Comprehensive Security Briefing (securityed@sandia.gov)
- **SEC100,** Annual Security Refresher Briefing (SON & pdf)
- **SEC180,** Vault & Vault Type Room (VTR) Training (SON)
- **SEC225,** Security Termination Briefing (pdf)
- **SEC301,** Classified Matter Training (SON)
- **SEC303,** Classified Marking Training (SON)
- **OUO101,** Understanding Official Use Only (OUO) (SON)



If you have questions, contact Security Connection 505-845-1321

Visitors

Visiting Sandia/New Mexico (NM)

- Directions, Map and Mail & Delivery address
- Access Requirements
- Visitor Badges
- Entering Kirtland Air Force Base (KAFB)
- Commercial Deliveries
- Controlled Items
- Prohibited articles
- Where to Stay

Visiting Sandia/California (CA)

- Visiting the Site
- Life in Livermore
- Livermore Valley Open Campus (LVOC)

Tonopah Test Range

Kauai Test Facility

If you have questions, contact Security Connection 505-845-1321

Mobile Devices and You

It's not about the WHO it's about the WHAT

Mobile Devices of any type, whether Sandia-, Government- or personally-owned are **prohibited** from entering any location designated as **Secure Space.**

A **mobile device** is a portable computing device that:

- can easily be carried by a single individual
- is designed to operate without a physical connection (e.g., wirelessly transmit or receive information)
- possesses local, non-removable data storage
- is powered-on for extended periods of time with a self-contained power source

Secure Space is any location where ***classified processing occurs***, is exclusively located within a Limited or more restrictive area, and is conspicuously denoted by **red, white and blue** signs at its boundaries within the Limited Area. Any devices brought into the limited area must be stored at approved **designated storage areas.**

If you have questions, contact Security Connection 505-845-1321

Mobile Devices and You

It's not about the WHO it's about the WHAT

Prior to bringing a **mobile device** into the Limited Area:

- Turn off Bluetooth and leave it off while in the Limited Area.
- Turn off Wi-Fi and leave it off while in the Limited Area.

Do not introduce an item or an electronic function (e.g., wireless) to an area where a sign says it is not allowed.

Approved storage locations are normally found throughout Sandia-controlled premises, but may not always be located near to where your business is to be conducted.

Plan ahead to determine whether your device will be allowed into these areas, and if not, where approved storage is located.

Devices may not enter, or be carried through, an unapproved area to reach a device storage location.

If in doubt, leave it outside any Sandia controlled premises.

If you have questions, contact Security Connection 505-845-1321

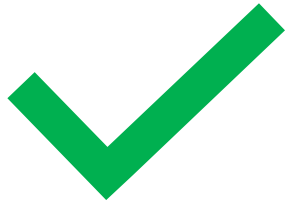
No Vouching, Tailgating, or Piggybacking

Everyone ***must*** swipe or present their badge to gain access.

No Vouching/Piggybacking - Do not vouch other individuals through **pedestrian** access-control points (gates, turnstiles, doors, etc.) at a **security area boundary**.

No Tailgating - Do not follow another individual into a security area without that individual's knowledge.

System overlapping
Entering an area via an automated access-control device while another person holds the door open, thereby ensuring that each person entering the area is both authorized and appropriately recorded by the automated access-control system.



Escorting - Action taken by an authorized individual to oversee and control people within a security area who do not have the proper need to know or access authorization for that area.

If you have questions, contact Security Connection 505-845-1321

Questions

Security+
Think.
Assess.
Protect.
YOU

If you have questions, contact Security Connection 505-845-1321

Sandia National Laboratories

Exceptional service in the national interest

Information Security

Jeremy Pacheco

Classified Matter Protection & Control

Sandia National Laboratories

New Mexico Site

Security+ Think. Assess. Protect. YOU

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Information Security

Discussion Topics:

1. Increase in Virtual Work Environment

2. CMPC Training

3. CMPC Resource Website

4. Upcoming major change to unclassified controlled information

Evolving Work Environment

Due to pandemic, higher % of workforce working virtually.

Reminders for FSOs to emphasize with their staff:

- Reminder, any work in potentially classified subject area must occur onsite within a building/structure within a Limited Area.
  Note: Staff unsure of information sensitivities? They can contact their SNL manager and/or derivative classifier (DC).
- Classified information, including computing password, combination to safe or VTR, can only be communicated using an approved secure method of transmission.
- Reminder, SNL no-vouching policy (effective April 2020) into limited areas.

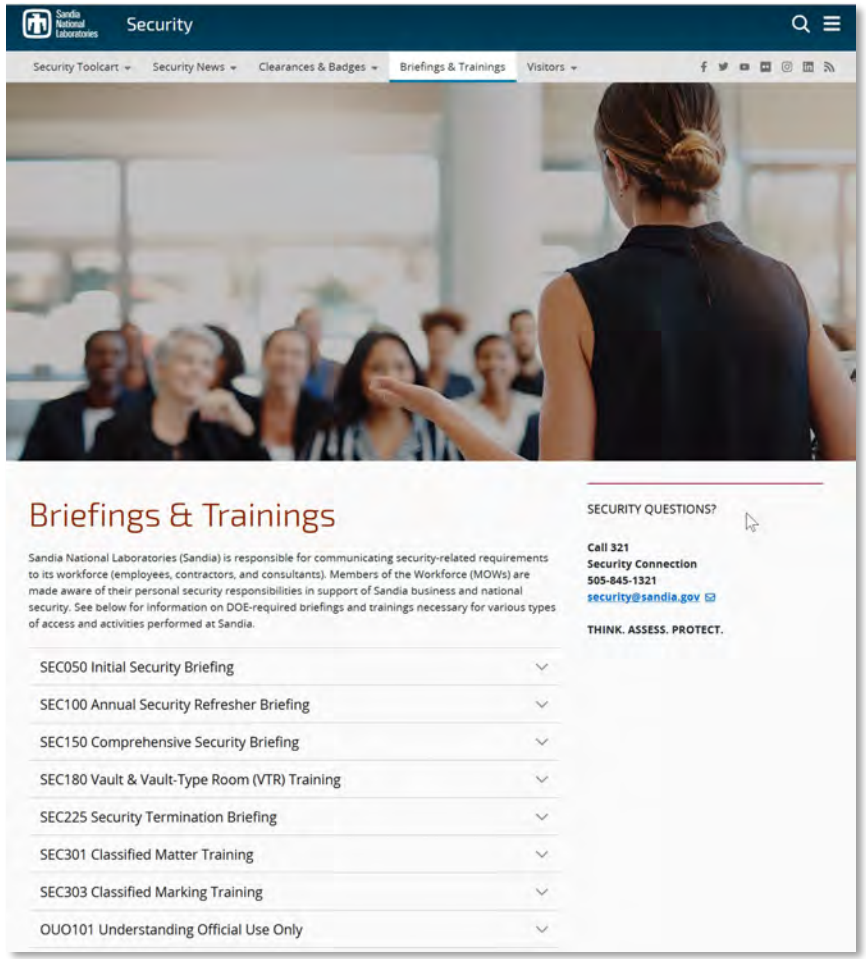
Sandia CMPC Primary Training Classes

1. SEC301, *Classified Matter Training*
   - Auto-assigned, online training required for all Q-cleared individuals

     Change Coming- will be auto-assigned to PO Contractors with active badges only (~March 2021).
   - 24 month refresher requirement
   - Fundamental basics for working with classified (e.g., protect, control, move, store, destroy)

2. SEC303, *Classified Marking Training*
   - Online training required for all individuals who have the potential to create classified
   - Required and auto-assigned for all individuals with Sandia Classified Network (SCN) accounts
   - 24-month refresher requirement

https://www.sandia.gov/security/briefings-trainings/



CMPC Resource Website

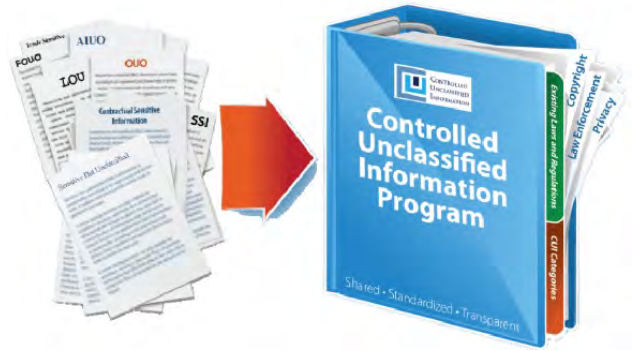
https://wp.sandia.gov/cmpc - CMPC's resource website on the Sandia Restricted Network (SRN)

What is Controlled Unclassified Information (CUI)?

- The 9/11 Commission recommended (2004) “horizontal sharing of intelligence information, transcending individual agencies” and stressed improved consistency in terminology, policy and markings of sensitive unclassified info **agency-wide**.

- Executive Order 13556 (Nov 2010) mandated consistency and management of CUI across executive branch agencies. Responsibility for implementation assigned to Information Security Oversight Office (ISOO).

- 32 CFR 2002, Controlled Unclassified Information created (Nov 2016) established unified policy for CUI for federal agencies and contractors.



Controlled Unclassified Information

Summary:

1. DOE and NNSA are the last federal agencies to publish guidance to align with 32 CFR 2002. Policy owned by CIO office at DOE HQ.

2. DOE CUI Directive expected to be finalized by end of CY2021.

4. SNL mission partners are already encountering CUI via external customers from agencies who have implemented.

5. At SNL, the CIO Office will own and implement CUI related policies. Implementation plan (IP) will be created to outline needed resources and schedule.

Summary of Impacts from draft CUI directive

Notable impacts:

1. New language for unclassified controlled information. Will require major updates to most all applicable lab policies, manuals, training classes and applications.
   Note: No longer OUO, would be "CUI-Basic" or "CUI-Specified"

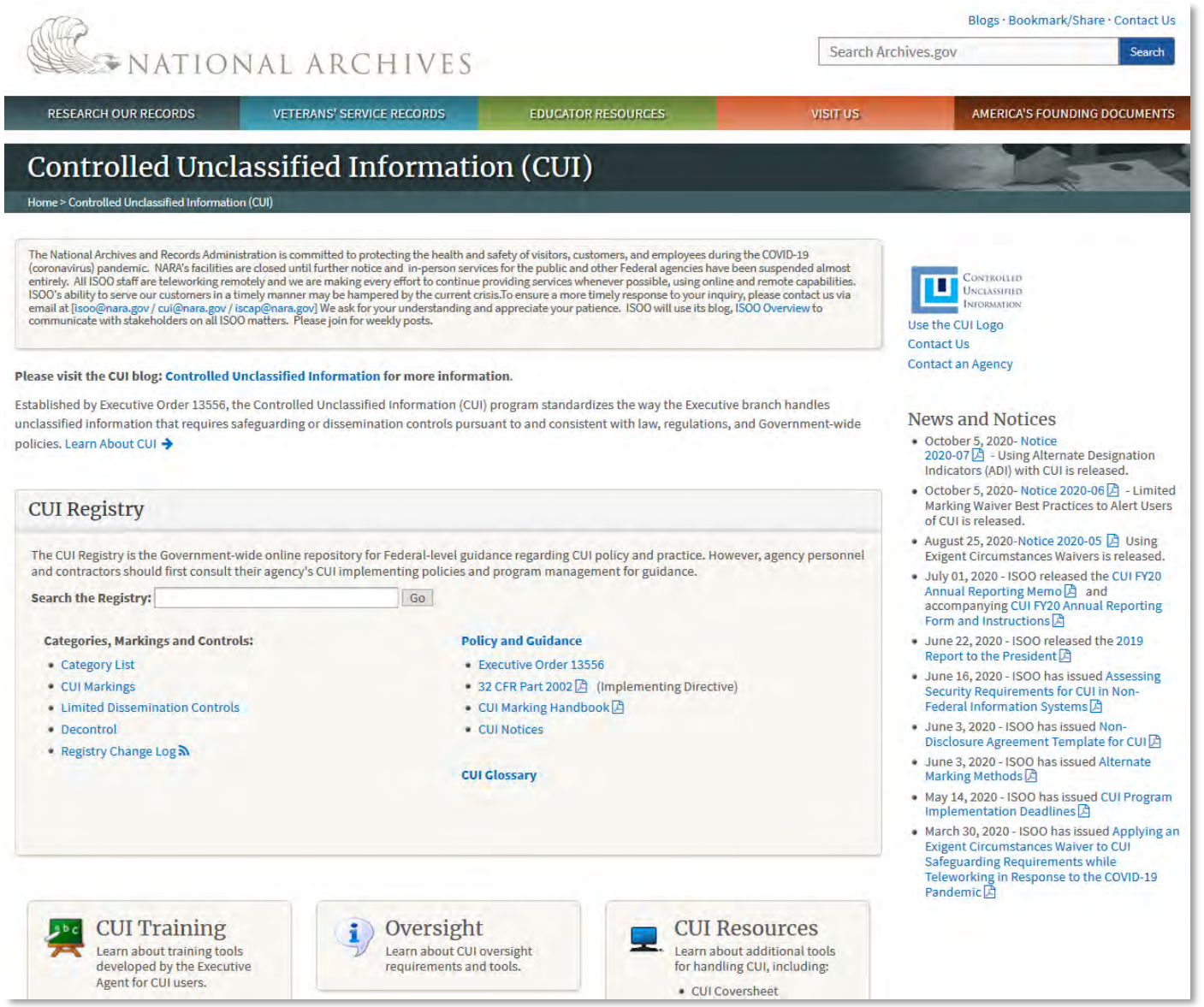
2. Destruction requirements align with destruction of classified.

Controlled Unclassified Information - CUI

Timeline:

1. DOE CUI Directive scheduled to be finalized by end of CY2021
2. Sandia will construct an implementation plan identifying resources needed to come into compliance. Implementation plan is provided to the local NNSA Field Office, Sandia Field Office (SFO)
3. SNL's CIO Office will serve a owning entity of new CUI requirements.

https://www.archives.gov/cui



NATIONAL ARCHIVES

Blogs · Bookmark/Share · Contact Us

Search Archives.gov Search

RESEARCH OUR RECORDS | VETERANS' SERVICE RECORDS | EDUCATOR RESOURCES | VISIT US | AMERICA'S FOUNDING DOCUMENTS

Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI)

The National Archives and Records Administration is committed to protecting the health and safety of visitors, customers, and employees during the COVID-19 (coronavirus) pandemic. NARA's facilities are closed until further notice and in-person services for the public and other Federal agencies have been suspended almost entirely. All ISOO staff are teleworking remotely and we are making every effort to continue providing services whenever possible, using online and remote capabilities. ISOO's ability to serve our customers in a timely manner may be hampered by the current crisis.To ensure a more timely response to your inquiry, please contact us via email at [isoo@nara.gov / cui@nara.gov / iscap@nara.gov] We ask for your understanding and appreciate your patience. ISOO will use its blog, ISOO Overview to communicate with stakeholders on all ISOO matters. Please join for weekly posts.

Please visit the CUI blog: Controlled Unclassified Information for more information.

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Learn About CUI

CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

Search the Registry: Go

Categories, Markings and Controls:

- Category List
- CUI Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log

Policy and Guidance

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Directive)
- CUI Marking Handbook
- CUI Notices

CUI Glossary

Controlled Unclassified Information

Use the CUI Logo
Contact Us
Contact an Agency

News and Notices

- October 5, 2020- Notice 2020-07 - Using Alternate Designation Indicators (ADI) with CUI is released.
- October 5, 2020- Notice 2020-06 - Limited Marking Waiver Best Practices to Alert Users of CUI is released.
- August 25, 2020-Notice 2020-05 Using Exigent Circumstances Waivers is released.
- July 01, 2020 - ISOO released the CUI FY20 Annual Reporting Memo and accompanying CUI FY20 Annual Reporting Form and Instructions
- June 22, 2020 - ISOO released the 2019 Report to the President
- June 16, 2020 - ISOO has issued Assessing Security Requirements for CUI in Non-Federal Information Systems
- June 3, 2020 - ISOO has issued Non-Disclosure Agreement Template for CUI
- June 3, 2020 - ISOO has issued Alternate Marking Methods
- May 14, 2020 - ISOO has issued CUI Program Implementation Deadlines
- March 30, 2020 - ISOO has issued Applying an Exigent Circumstances Waiver to CUI Safeguarding Requirements while Teleworking in Response to the COVID-19 Pandemic

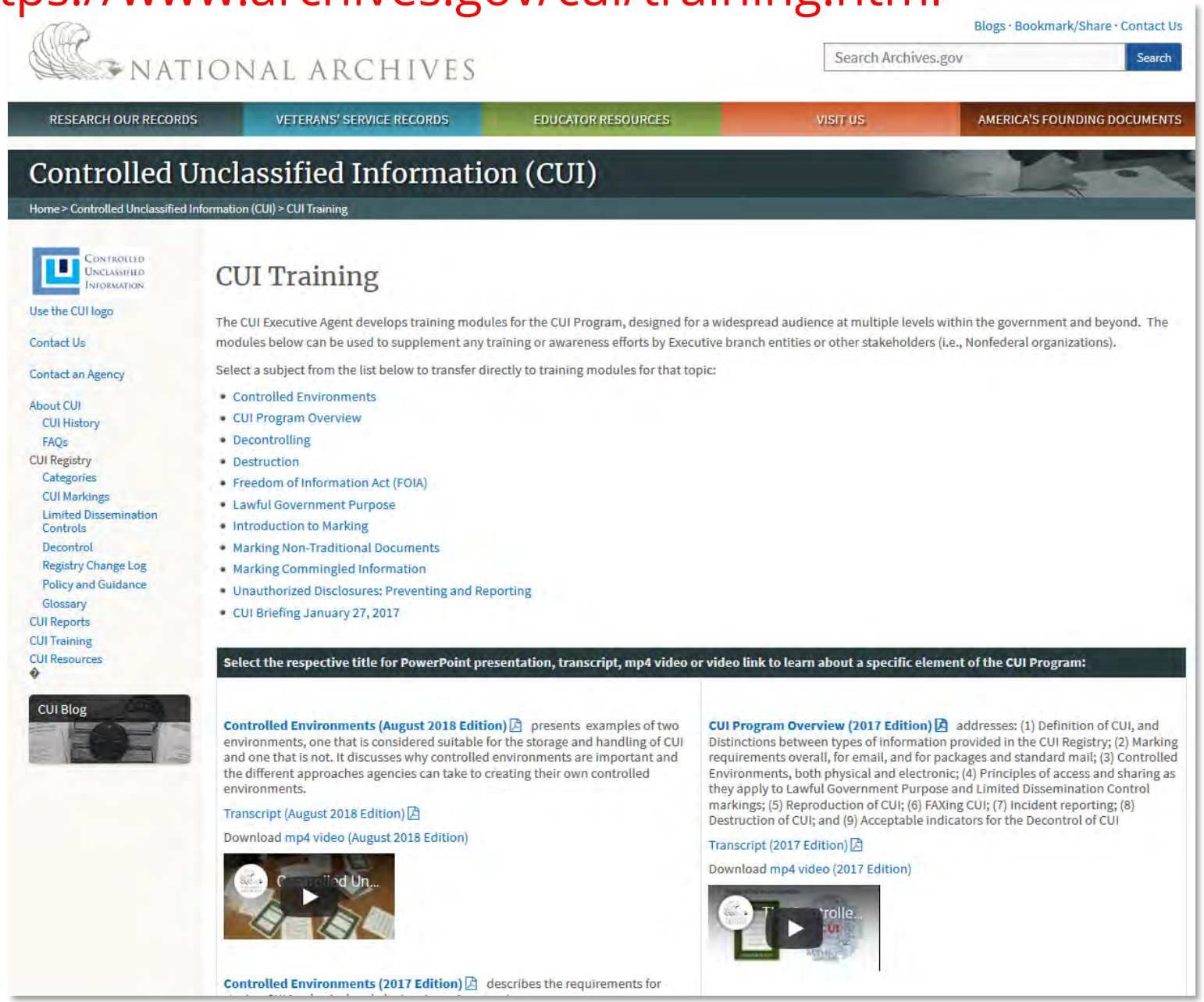
CUI Training
Learn about training tools developed by the Executive Agent for CUI users.

Oversight
Learn about CUI oversight requirements and tools.

CUI Resources
Learn about additional tools for handling CUI, including:

- CUI Coversheet

https://www.archives.gov/cui/training.html



Blogs · Bookmark/Share · Contact Us

NATIONAL ARCHIVES

Search Archives.gov Search

RESEARCH OUR RECORDS | VETERANS' SERVICE RECORDS | EDUCATOR RESOURCES | VISIT US | AMERICA'S FOUNDING DOCUMENTS

Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI) > CUI Training

Controlled Unclassified Information

Use the CUI logo

Contact Us

Contact an Agency

About CUI
- CUI History
- FAQs

CUI Registry
- Categories
- CUI Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log
- Policy and Guidance
- Glossary

CUI Reports

CUI Training

CUI Resources

CUI Blog

CUI Training

The CUI Executive Agent develops training modules for the CUI Program, designed for a widespread audience at multiple levels within the government and beyond. The modules below can be used to supplement any training or awareness efforts by Executive branch entities or other stakeholders (i.e., Nonfederal organizations).

Select a subject from the list below to transfer directly to training modules for that topic:

- Controlled Environments
- CUI Program Overview
- Decontrolling
- Destruction
- Freedom of Information Act (FOIA)
- Lawful Government Purpose
- Introduction to Marking
- Marking Non-Traditional Documents
- Marking Commingled Information
- Unauthorized Disclosures: Preventing and Reporting
- CUI Briefing January 27, 2017

Select the respective title for PowerPoint presentation, transcript, mp4 video or video link to learn about a specific element of the CUI Program:

Controlled Environments (August 2018 Edition) presents examples of two environments, one that is considered suitable for the storage and handling of CUI and one that is not. It discusses why controlled environments are important and the different approaches agencies can take to creating their own controlled environments.

Transcript (August 2018 Edition)

Download mp4 video (August 2018 Edition)

Controlled Environments (2017 Edition) describes the requirements for

CUI Program Overview (2017 Edition) addresses: (1) Definition of CUI, and Distinctions between types of information provided in the CUI Registry; (2) Marking requirements overall, for email, and for packages and standard mail; (3) Controlled Environments, both physical and electronic; (4) Principles of access and sharing as they apply to Lawful Government Purpose and Limited Dissemination Control markings; (5) Reproduction of CUI; (6) FAXing CUI; (7) Incident reporting; (8) Destruction of CUI; and (9) Acceptable indicators for the Decontrol of CUI

Transcript (2017 Edition)

Download mp4 video (2017 Edition)

Questions