# Authorization Process for Classified Licensees

# Your role is critical…

## *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*

In one of the most sophisticated and perhaps largest ha
han five years, email systems were
ry and Commerce D
igation

DEFENSE

SHARE... E-MAIL THIS PAGE PRINTABLE FORMAT

## Defense contractors aren't securing sensitive inform watchdog finds

By Lauren C. Williams | Jul 26, 2019

Contractors routinely fail to secure the Defense Department's uncla
information from cyberthreats when it's housed on their systems an
according to a new report from the department's watchdog agency.

LAW

## Ex-Navy nuclear engineer and his wife are charged in an espionage plot

October 12, 2021 · 5:09 AM ET
Heard on Morning Edition

A MARTÍNEZ RYAN LUCAS

+ PLAYLIST

3-Minute Listen

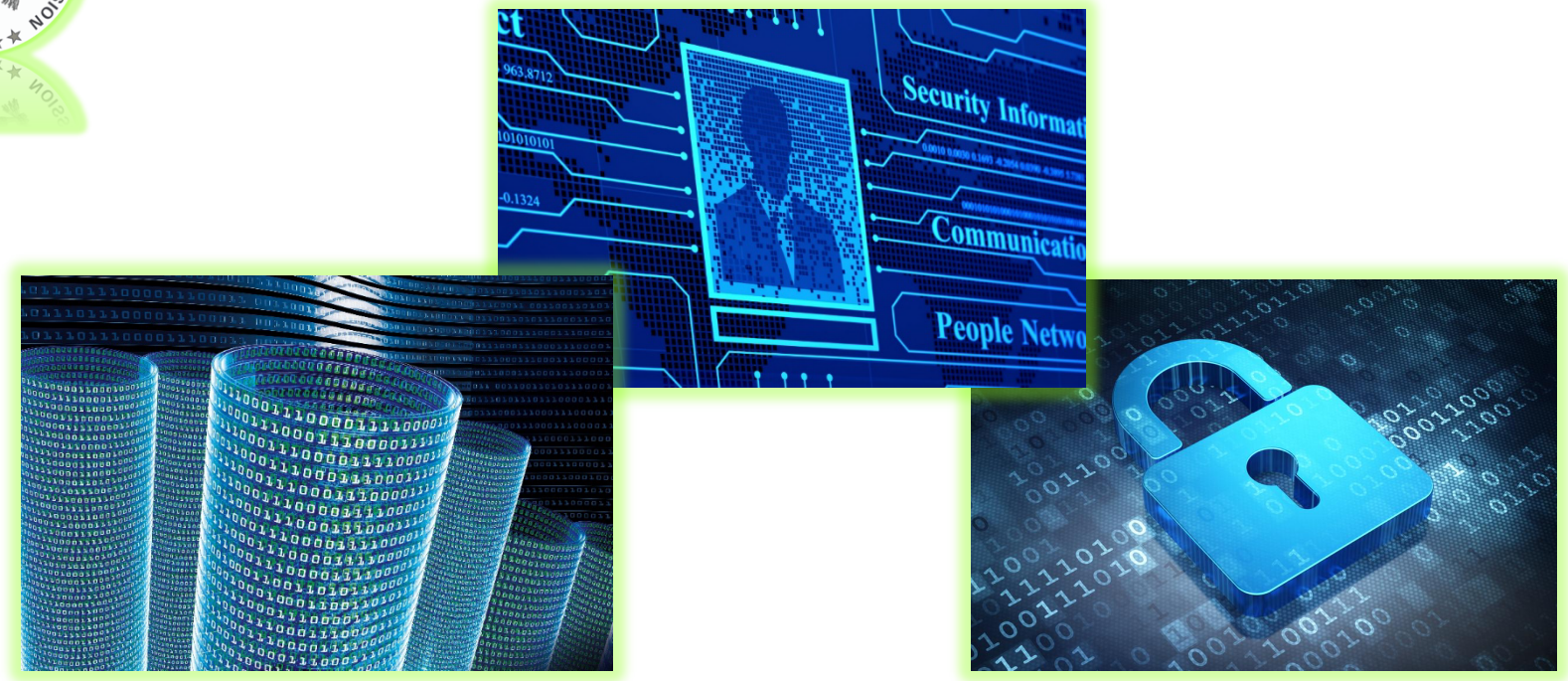
A former U.S. Navy engineer and his wife are due in federal court Tuesday. The Justice Department accuses them of trying to share secrets about nuclear submarine technology with another country.

Transcript

## ontractor pleads guilty to sharing info with person linked to Hezbollah

Associated Press March 28

# 3 Pillars of Cyber Security




Confidentiality – Integrity - Availability

# Key Goals of Cyber Security

**Ensuring that all computer-based equipment, systems, information and services are protected from:**

- unintended or unauthorized access,
- unauthorized activities
- unauthorized change or destruction
- untrustworthy individuals
- unplanned events and natural disasters

**Managing risks related to the use, processing, storage, and transmission of information and the systems and processes used for those purposes.**

# Who is the Authorizing Official for Licensee Classified Systems?

The Authorizing Official for Licensee Classified Systems (AOLCS) is fully responsible and accountable for the risks associated with operating classified networks and Information Technology (IT) systems located, for example, at NRC licensed enrichment facilities.

“The authorizing official has inherent U.S. government authority and, as such, must be a government employee.”*

Coordinates with the NRC Chief Information Security Officer (CISO), security control assessors, NRC inspectors, licensees, and other interested parties during the security authorization process.

*Reference- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems

# Authorizing Official for Licensee Classified Systems Overview

- Ensures systems are properly assessed and authorized based on the environment of operation, security impact levels, and required security controls
- Evaluates threats and vulnerabilities to determine if additional safeguards are needed and system security is an element of the life-cycle process
- Formally assumes responsibility for the risk associated with the operation of licensee classified information systems
- Issues security authorization

# Chief Information Security Officer Overview

The NRC Chief Information Security Officer (CISO) plans, directs, and oversees the Classified Authorization Program for Licensees, including standards, processes, and security requirements. The CISO has inherent U.S. government authority and, as such, must be a government employee.

- Provides cybersecurity requirements for classified networks and IT systems located at NRC licensed enrichment facilities
- Ensures the AOLCS is presented with a recommendation based on risk
- Provides technical expertise in the preparation for system validations

# Chief Information Security Officer Overview

- Coordinates the assessment and authorization activities based on the environment of operation, security impact levels, and required security controls
- Identifies the threats and vulnerabilities and provides recommendations of additional safeguards to the AOLCS
- Ensures the licensee information and cyber security programs include the national guidance, policies and procedures designed to protect the information and information systems
- Communicates and coordinates responses to applicable national level issuances (Statutes, Executive Orders, National Security Directives, etc.)

# Authority over National Security Systems

National Security Directive 42 “National Policy for the Security of National Security Telecommunications and Information Systems”

- Signed July 5, 1990, declassified November 22, 1996

Genesis of the Committee on National Security Systems (CNSS)

Policies (CNSSP) - Instructions (CNSSI) - Directives (CNSSD)

Leverages National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) guidance

***CNSS issuance shall not alter or supersede the authorities of the Director of National Intelligence.***

# National Security Systems Guidance


- Committee on National Security Systems (CNSS)

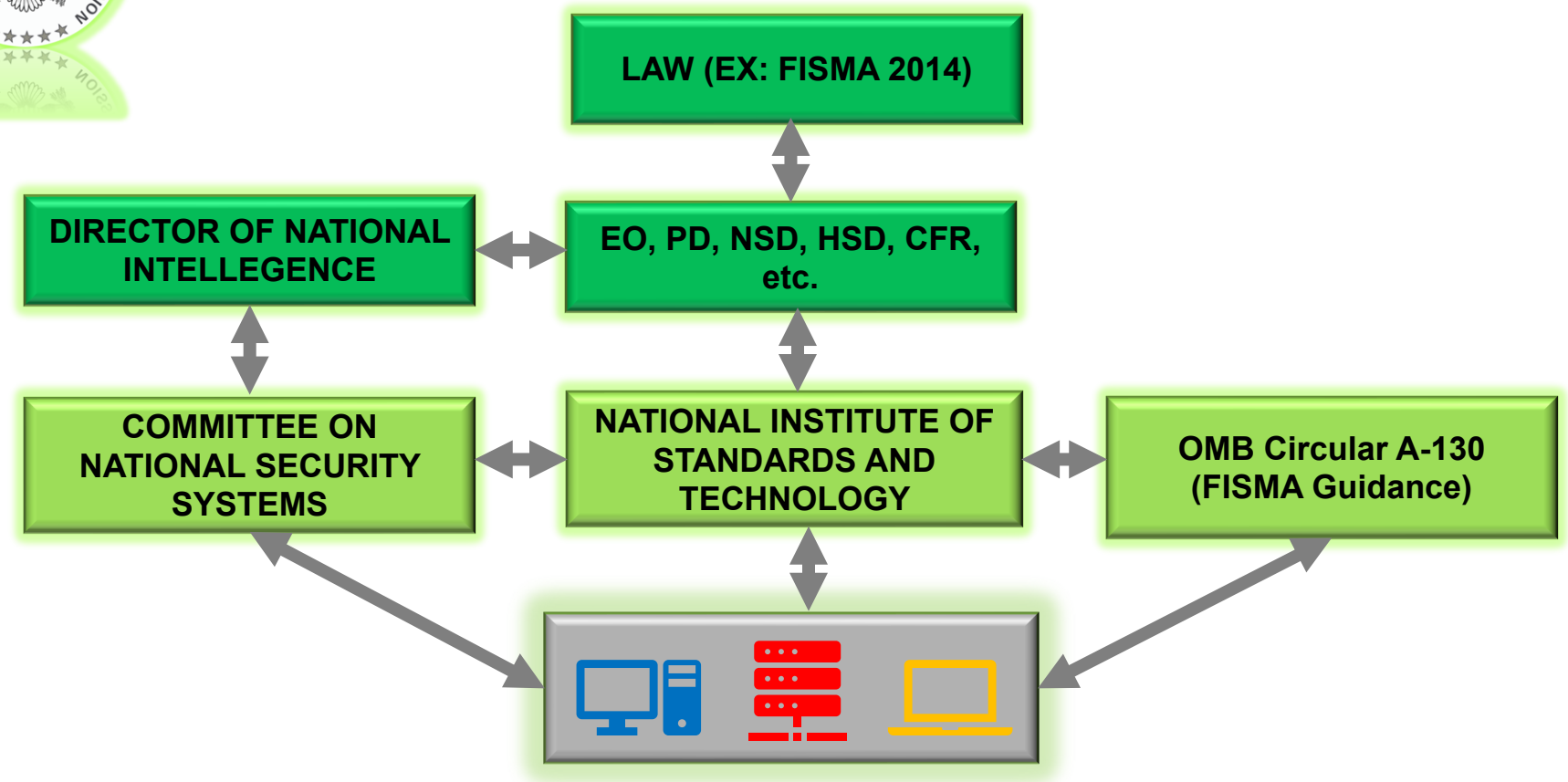
  Policies (CNSSP) - Instructions (CNSSI) - Directives (CNSSD)

- National Institute of Standards and Technology (NIST)

  Special Publications, Federal Information Processing Standards Publication

- ***CNSS and NIST developed most guidance together as a special joint Department of Defense, Intelligence Community, and NIST task force***
- ***CNSS guidance is used as an overlay in conjunction with the associated NIST guidance***

# Authority and Guidance Structure



# Risk Management Framework

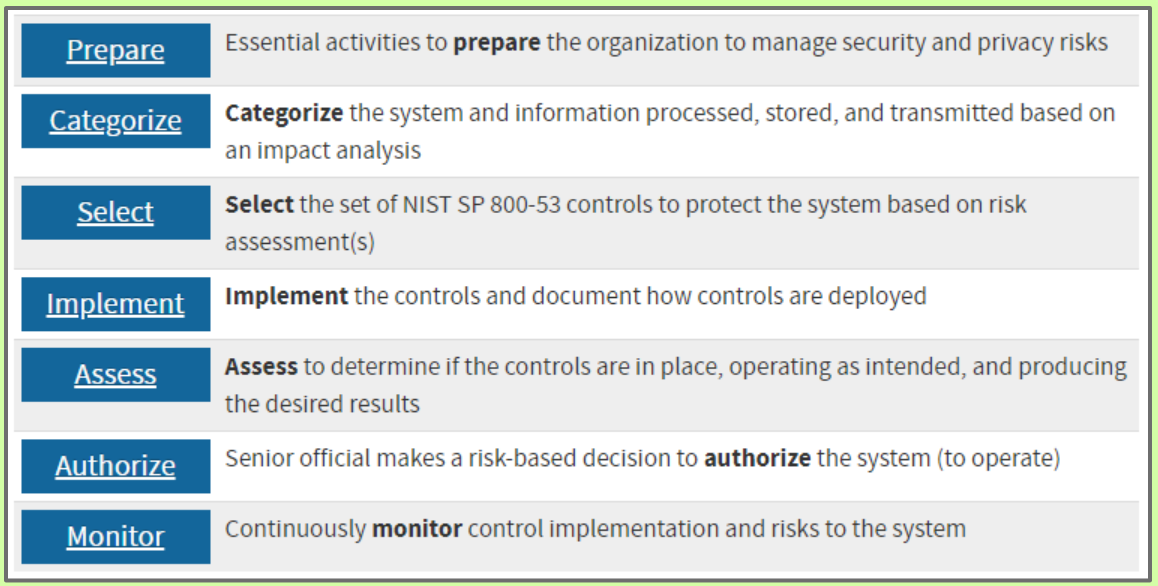
- CNSSP No. 22 “Policy on Information Assurance Risk Management for National Security Systems”
- NIST 800-37 “Risk Management Framework for Information Systems and Organizations”
- The Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.
- The RMF approach can be applied to new and legacy systems, any type of system or technology and within any type of organization regardless of size or sector.

# CNSSI Number 1253 & NIST 800-53 Revision 5

- CNSS collaborated with NIST to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS) and provides a common foundation for information security across the U.S. Federal Government.
  - CNSSI No. 1253 is a companion document to the NIST publications relevant to categorization and selection.
    - NIST 800-53, NIST 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories, and Federal Information Processing Standard (FIPS) 199 “Standards for Security Categorization of Federal Information Systems”
  - For NSS, where differences between the NIST documentation and CNSSI 1253 occur, CNSSI 1253 takes precedence.

# Risk Management Framework Resources

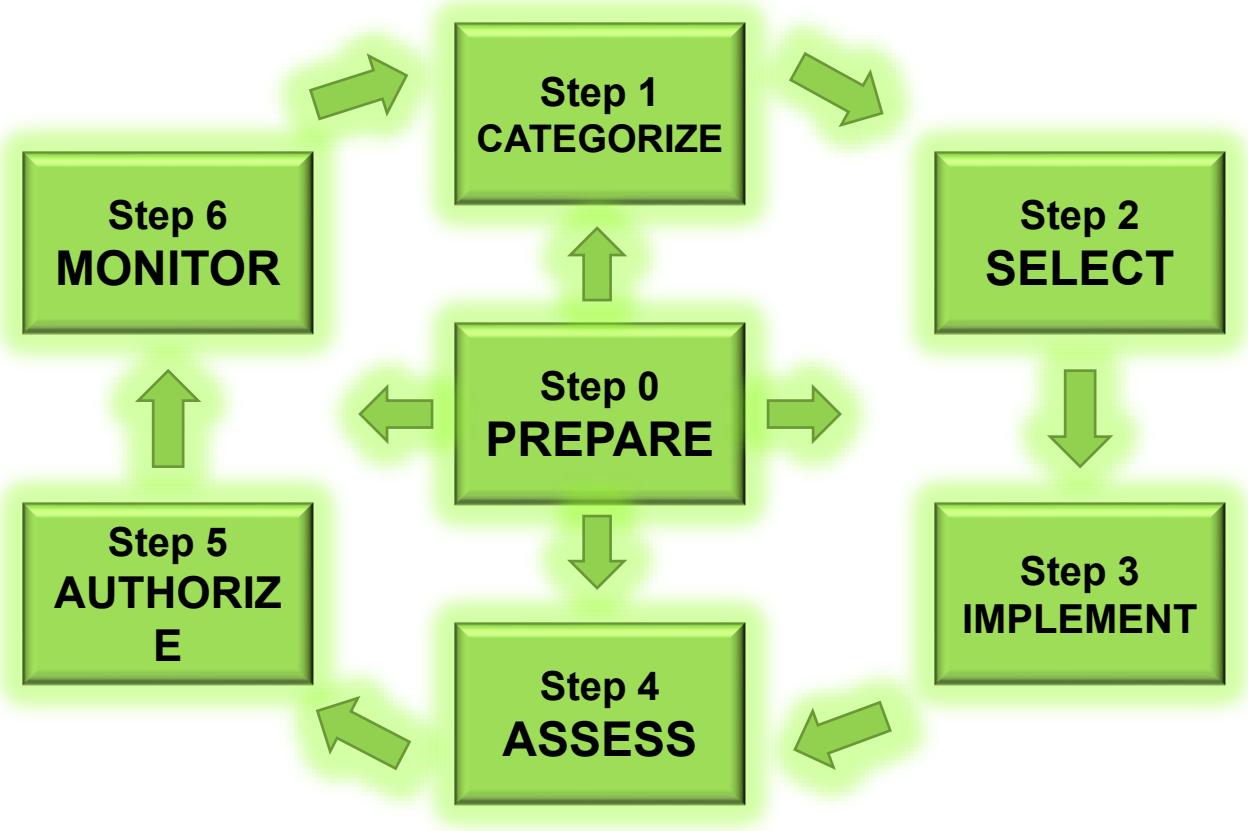
- NIST RMF project site – provides excellent resources on how to navigate through the process.



| | |
|---|---|
| Prepare | Essential activities to **prepare** the organization to manage security and privacy risks |
| Categorize | **Categorize** the system and information processed, stored, and transmitted based on an impact analysis |
| Select | **Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s) |
| Implement | **Implement** the controls and document how controls are deployed |
| Assess | **Assess** to determine if the controls are in place, operating as intended, and producing the desired results |
| Authorize | Senior official makes a risk-based decision to **authorize** the system (to operate) |
| Monitor | Continuously **monitor** control implementation and risks to the system |

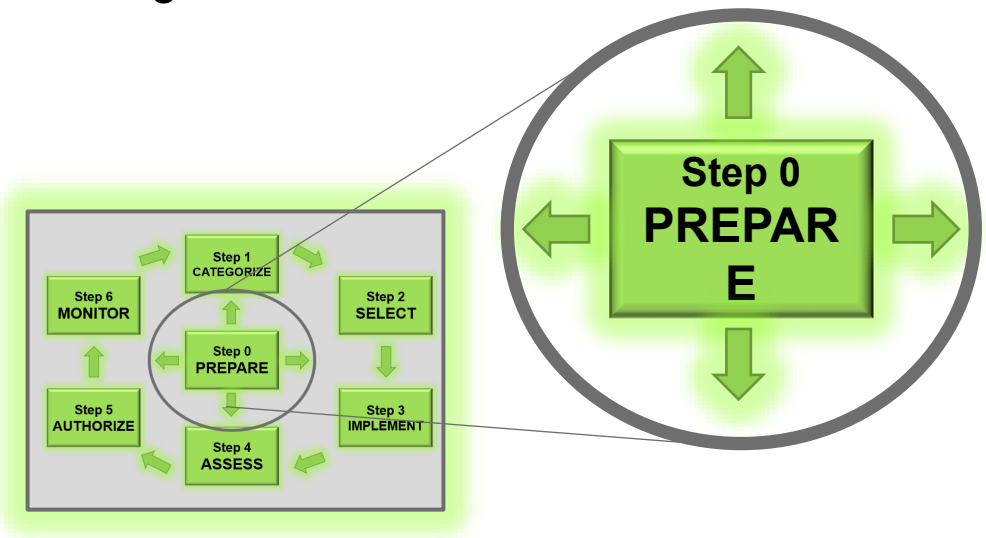
Site includes links to overviews and guidance for each of the seven steps of the RMF

# Risk Management Framework



# Risk Management Framework
# Step 0 PREPARE

- The purpose of the Prepare step is to carry out essential risk management tasks at the organization, mission and business process, and system levels to establish context and help prepare the organization to manage its security and privacy risks using the RMF.

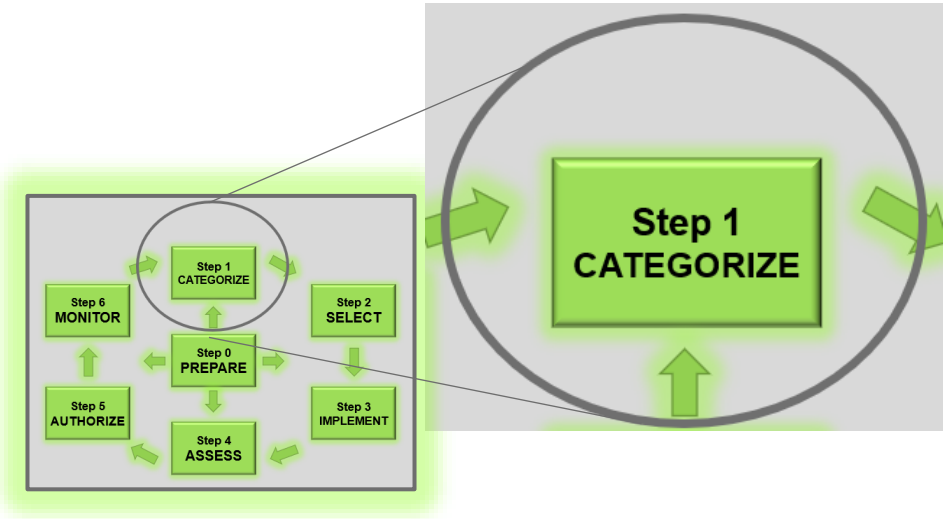



Prepare step tasks are completed before each of the RMF steps and tasks.

The intention is to provide the information and resources necessary to successfully manage information security risk to the organization and its missions from the operation and use of systems.

# Risk Management Framework
# Step 1 CATEGORIZE

- Security categorization provides a structured way to determine the criticality of the information being processed, stored, and transmitted by a system.

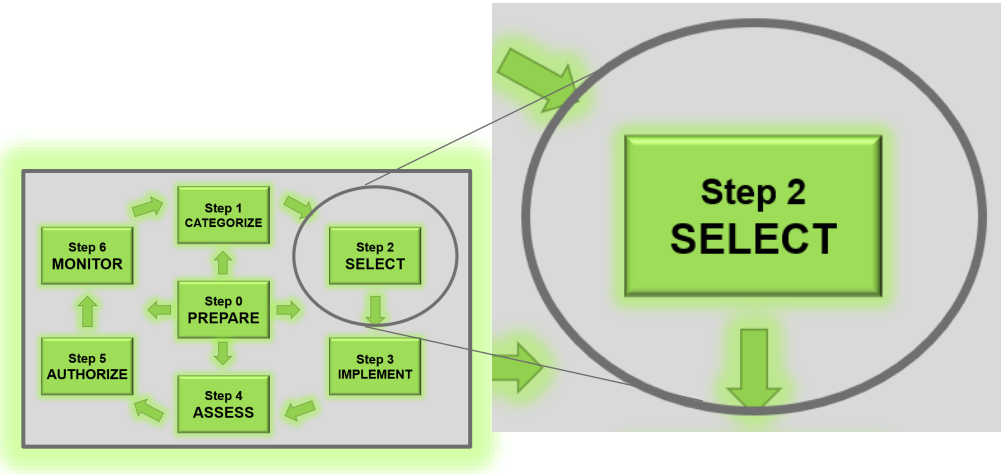



The information owner or system owner identifies the types of information processed, stored, and transmitted by the system and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type.

This is used to inform all subsequent risk management decisions regarding the security of the system.

# Risk Management Framework
# Step 2 SELECT

- Controls are selected according to security and privacy requirements allocated to the system, system elements, and environment of operation.

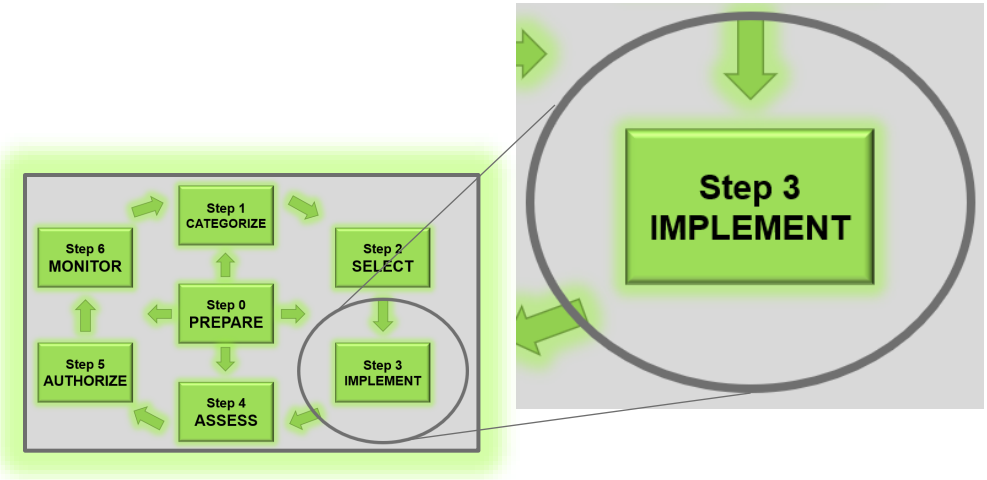



The control selection process helps to identify an initial set of controls, including common controls and baseline or organization-generated controls

Allows for tailoring the baseline controls by applying scoping, parameterization and compensating control guidance

# Risk Management Framework
# Step 3 IMPLEMENT

- The implementation of controls involves the establishment of new or the utilization of existing processes, procedures, products, and services to meet the intent of the controls selected in the RMF Select step. The system security plans serve as guides for implementing the controls and are updated, if necessary, as controls are implemented.

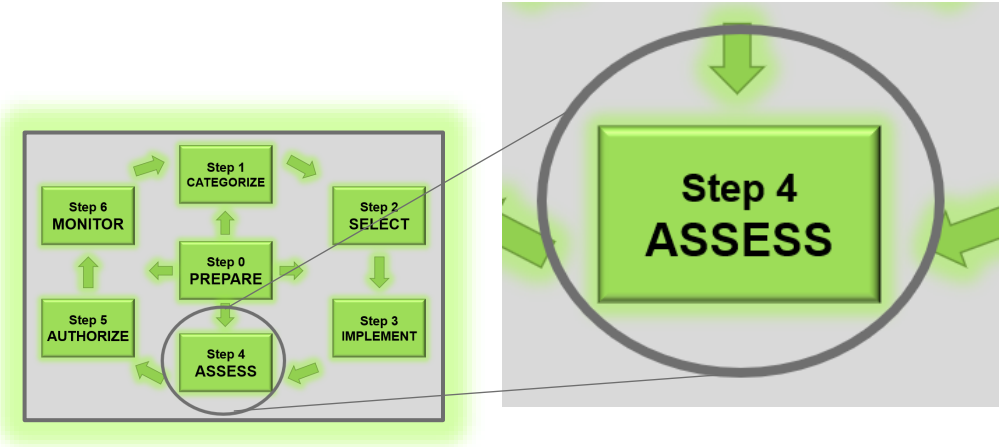



The selection and implementation of security controls reflect the objectives of information security programs and how those programs manage their respective risks.

The system owner and the common control provider have primary responsibilities for implementing controls.

# Risk Management Framework
# Step 4 ASSESS

- The purpose of the Assess step is to determine that selected security controls are implemented correctly, operate as intended, produce the desired outcome, and meet organizational or system security and privacy requirements. The Assessment identifies control deficiencies and remediation actions.




Assessments verify that selected controls are implemented correctly, operating as expected, and recorded appropriately in security plans.

The deficiencies in the implementation of controls should be prioritized by the potential risks they convey to the system, components, and organization.

# NRC Assessment Tasks

- Documentation and artifact review
  - Information System Security Plans, Standard Practice Procedures Plan, Security Test and Evaluations, Plan of Action & Milestones, Security Evaluation Reports, prior authorizations & conditions, policies, procedures, processes, inspection reports, inventory list, scanning results, NIST National Vulnerability Database, United States Computer Emergency Readiness Team (US-CERT) site, Cybersecurity & Infrastructure Security Agency site, etc.
- Other Activities
  - Plan assessment priorities, interview cyber & facility security teams, users, and leadership, observe processes and procedures, physically review systems and the operating environment, verify inventory, verify controls are implemented as described, etc.

# NRC Assessment Tasks

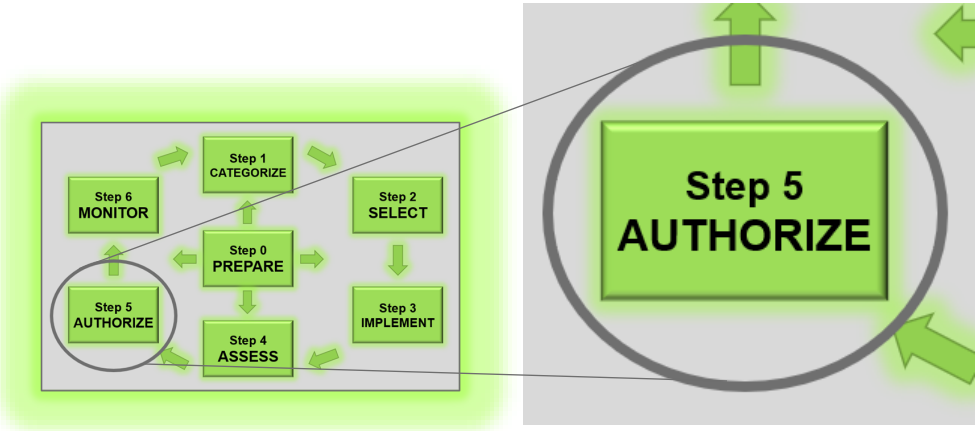
- Assessment collects the information used to provide a risk analysis that is used to:
  - Compare implementation against federal requirements and guidance
  - Understand operating environment
  - Understand the organizations security culture
  - Make a risk assessment used to inform the authorization decision
  - Define any conditions that will be part of the authorization
  - Define Plan of Action & Milestones

# Plan of Action & Milestones

- A Plan of Action & Milestones (POA&M) is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
- POA&Ms are used to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems in need of remediation identified during any assessment.
- A tool for documenting the remediation actions to address system risk.

# Risk Management Framework
# Step 5 AUTHORIZE

- The Authorize step provides organizational accountability by requiring a senior management official to determine if the security, privacy, and supply chain risk to organizational operations, assets, individuals, other organizations, or the Nation is acceptable based on the operation of a system or the use of common controls.




Authorization is the determination of risk since the decision to authorize (or not) a system to operate depends on the security posture of that system, as well as the risk from the operation and use of the system.

This risk is determined using the authorizing official review and analysis of the information and materials in the authorization package, as well as organizational-level and system-level risk information provided by the CISO.

# Types of System Authorizations (1 of 3)

- Interim Authorization
  - An authorization for a specific amount of time, usually six months. Usually granted when operations must continue but a full authorization effort is unable to be performed but a risk evaluation has been made.
- Periodic Authorization
  - An authorization granted for a period of usually three years at the end of which a full assessment is performed.
- Ongoing Authorization
  - Authorization continues over time based on ongoing monitoring and assessment of security control effectiveness with respect to changing threats, vulnerabilities, technologies, and missions/business processes.

# Types of System Authorizations (2 of 3)

- Authority to Test (ATT)
  - Temporary authorization to test an information system granted under a well-defined scope of time, tasks, and expected outcome. An interim authorization, no more than a few months in duration with the goal of converting to an IATO or ATO.
- Authority to Use (ATU)
  - An authorization for the use of an information system, service, or application granted based on an existing authorization package generated by another organization. Can be an interim, periodic, or ongoing authorization.

# Types of System Authorizations (3 of 3)

- Interim Authority to Operate (IATO)
  - Temporary authorization granted for an information system to process information based on preliminary results of a security evaluation of the system. Typically, up to six months in duration with the goal of converting to an ATO.
- Authority to Operate (ATO)
  - Authorization granted for an information system to process information based on a comprehensive security evaluation of the agreed-upon set of security controls. Can be a periodic or ongoing authorization.

# Authorization Summary

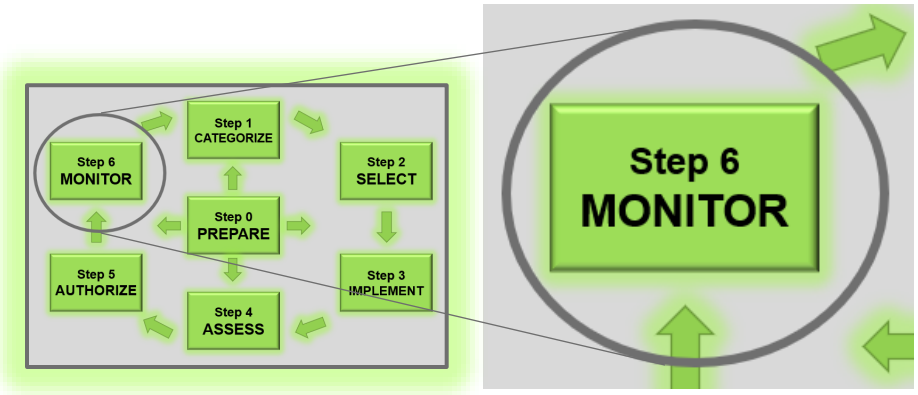
- The AOLCS, working with the CISO, takes on the risk and responsibility of an organizations information technology systems through the authorization of these systems.
- The authorization is based on how the organization manages risk.
  - A risk assessment is based on how the organization implements security controls commensurate with the severity level of risk to the confidentiality, integrity, and availability of the information and systems. This implementation is compared to national guidance, the mission, and operating environment.

# System Authorizations Artifacts and Documentation

- Authorization Assessment Report (ASR)
  - Documents the results of the assessor's risk analysis and any recommendations for the system.  Provided to the CISO for review.
- CISO Recommendation to the AOLCS
  - Formal document that provides the AOLCS with the CISO’s analysis and recommendation for authorization type and period to include any conditions or POA&Ms.
- AOLCS Authorization
  - Formal document that provides the system owner with the authority to operate with parameters to include conditions, POA&Ms, type of authorization and period.

# Risk Management Framework
# Step 6 MONITOR

- The objective of continuous monitoring is to determine if the security controls continue to be effective over time in light of the inevitable changes that occur in the system and the environment in which the system operates. Continuous monitoring also provides an effective mechanism to update security and privacy plans, assessment reports, and plans of action and milestones.




The authorizing official may need to reauthorize a system depending on the severity of an event; the impact of an event or change in organizational operations, organizational assets, or individuals; and the extent of the corrective actions required to fix the identified deficiencies in a system.

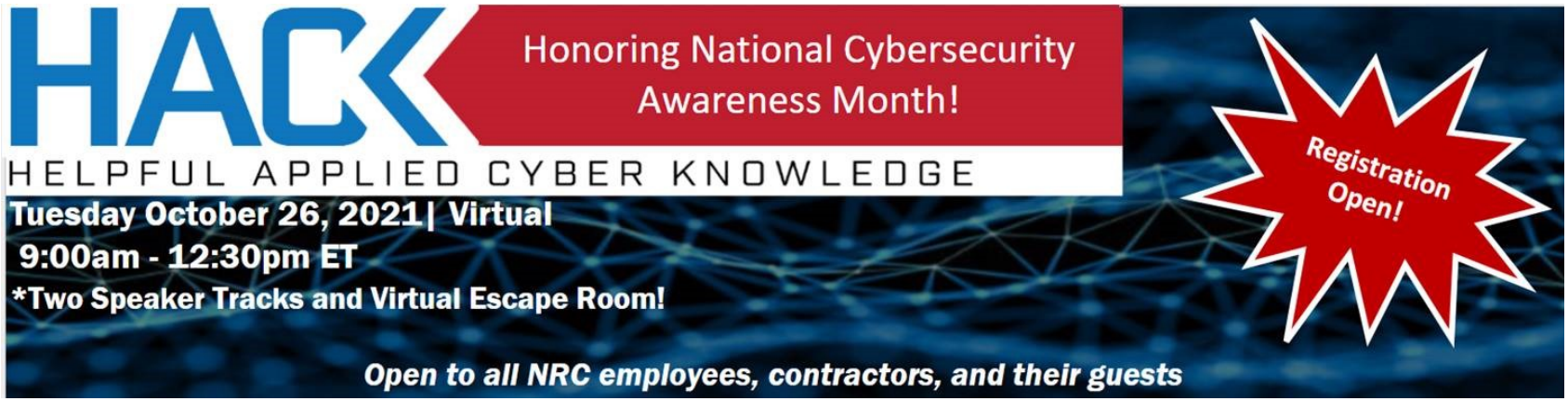
# Discussion Time

# Helpful Applied Cyber Knowledge
# HACK 2021

- On Tuesday October 26, 2021, the NRC and the Office of the Chief Information Officer will host a virtual version of their bi-annual Helpful Applied Cyber Knowledge (HACK) event.

- In its sixth year, HACK aims to increase the knowledge of all technology users to be aware of the impact of potential threats they may unknowingly face as a result of their activities and behaviors online and offline, at work and at home. This half-day seminar features dynamic speakers from government, education and industry discussing a wide range of current technologies and cybersecurity challenges. HACK will be held virtually and streamed live to select audiences

# Helpful Applied Cyber Knowledge
# HACK 2020




Register today!

# AUTHORIZING OFFICIAL WORKSHOP FOR NRC ENRICHMENT LICENSEES

32 CFR Part 117, “National Industrial Security Program Operating Manual" (NISPOM)

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# 32 CFR Part 117 NISPOM

- 32 CFR Part 117 was promulgated to codify the existing NISPOM into the Code of Federal Regulations.
- Prescribes industrial security procedures and practices to safeguard U.S. Government (USG) classified information developed by or disclosed to contractors (in this case licensees) of the NRC.

# 32 CFR Part 117 NISPOM - Applicability

- All industrial, educational, commercial, or other non-USG entities granted access to classified information by the USG executive branch departments and agencies or by foreign governments. (32 CFR 117.2(a)(3).
- The rule does not limit the authority of the USG to grant access to classified information under the cognizance of their department or agency to any individual designated by them.

# 32 CFR Part 117 NISPOM - Responsibilities

The Chairman of the NRC :

1. Prescribes procedures for the portions of this rule that pertain to information under NRC programs classified under the Atomic Energy Act, other federal statutes, and executive orders.
2. Retains authority over access to information under NRC programs classified under the AEA, other federal statutes, and executive orders.
3. Inspects and monitors licensee programs and facilities that involved access to information under NRC programs classified pursuant to the AEA, other federal statutes, and executive orders where appropriate.

# 32 CFR Part 117 NISPOM – Reporting Requirements

- Reporting requirements for infractions and violations regarding classified matter are already covered in 10 CFR 95.57.
- All enrichment licensees' SPPPs commit to reporting via NRC requirements.
- Reports to other agencies i.e., the FBI should be vetted with the NRC first.

# 32 CFR Part 117 NISPOM – SEAD 3 Reporting Requirements

- Licensees are required to report certain events that may affect the status of their employee's eligibility for access to classified information.
- Licensees must report potential counterintelligence concerns such as
  - Foreign activities involving application for foreign citizenship
  - Application for foreign passport
  - Elicitation to obtain classified information
  - Adoption of non-U.S. citizen children
- Cleared licensee employees must report foreign travel in accordance with NRC's SEAD 3 policy.

# 32 CFR Part 117 NISPOM - Procedures

- Licensees are required to establish and execute an insider threat program (ITP).
- Elements of the program include:

1. Formal appointment by the licensee of an ITP senior official (ITPSO) who is a U.S. citizen employee and a senior official of the company.
2. Annual licensee self-review including self-inspection of the ITP.
3. Initial and refresher insider threat training for the awareness of cleared program management and cleared individuals.
4. Requirements to report to the NRC any detection of an insider threat to the licensee.
5. Provide user activity monitoring on any classified IT system.

# 32 CFR Part 117 NISPOM – Exclusion Resolutions and Self-Inspections

- Any Exclusion Resolutions that have been previously executed by a licensee to exclude certain individuals from access to classified information will remain in effect even if the language in the resolution is not the exact wording in § 117.18.
- Licensees are now required to conduct at least an annual self-inspection of their security program and prepare a formal report for NRC review during inspections.
- Senior Management Official will annually certify to the NRC that a self-inspection has been conducted.

# 32 CFR Part 117 NISPOM – Hotlines, Rule Interpretations and Waivers to Part 117

- The NRC's Headquarters Operations Center phone number is an unconstrained avenue available to all licensees to report security incidents, irregularities and infractions with out reprisal.
- Licensees can request interpretations of Part 117 to address unique NRC mission requirements.
- Licensees can request waivers to provisions of Part 117 provided they supply written justification for the waiver.

# 32 CFR Part 117 NISPOM – Information System Security

- §117.18 codifies the requirements that must be met for a licensee to process classified information on a network system.
- The guidance provided is based on the Federal Information Security Modernization Act and associated guidance in NIST 800-37, CNSS Instruction 1253 and NIST 800-53, rev. 5.
- Information System Security Plans must address key components of the licensee's ITP such as:

1. User activity monitoring network activity
2. Information sharing procedures
3. A continuous monitoring program

# 32 CFR Part 117 NISPOM – Examples of requirements that do not apply to NRC licensees

- Requirements for the protection of TOP SECRET (TS) Information as NRC licensees are not permitted access to TS.
- Requirements for the protection of Critical Nuclear Weapon Design Information.
- COMSEC material is provided for and managed by the Department of Energy. Licensees protect and use COMSEC material but DOE accounts for it.

# Any Questions?

Please contact J. Keith Everly of the NRC's Information Security Branch at 301-717-0596.

# Discussion of INFOSEC and Counterintelligence (CI) Program Options for Commercial Uranium Enrichment Plants

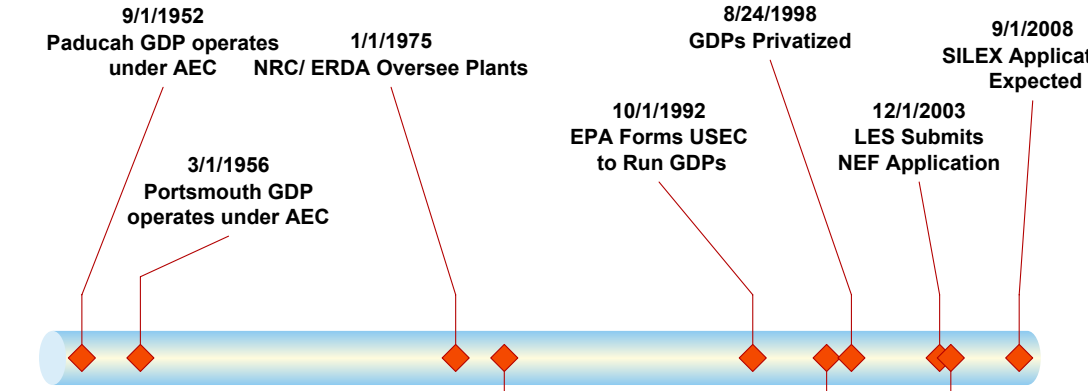
July 2008

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# Discussion Outline

- History of enrichment facilities
- Current NRC INFOSEC program
- Why additional programs may be required
- Additional INFOSEC programs under consideration
- Threat
- Statutory authority
- Privacy considerations
- Discussion of CI program options
- Path forward

# Timeline: History of Uranium Enrichment in the US




*Portsmouth Site*

# New Commercial Uranium Enrichment Plants

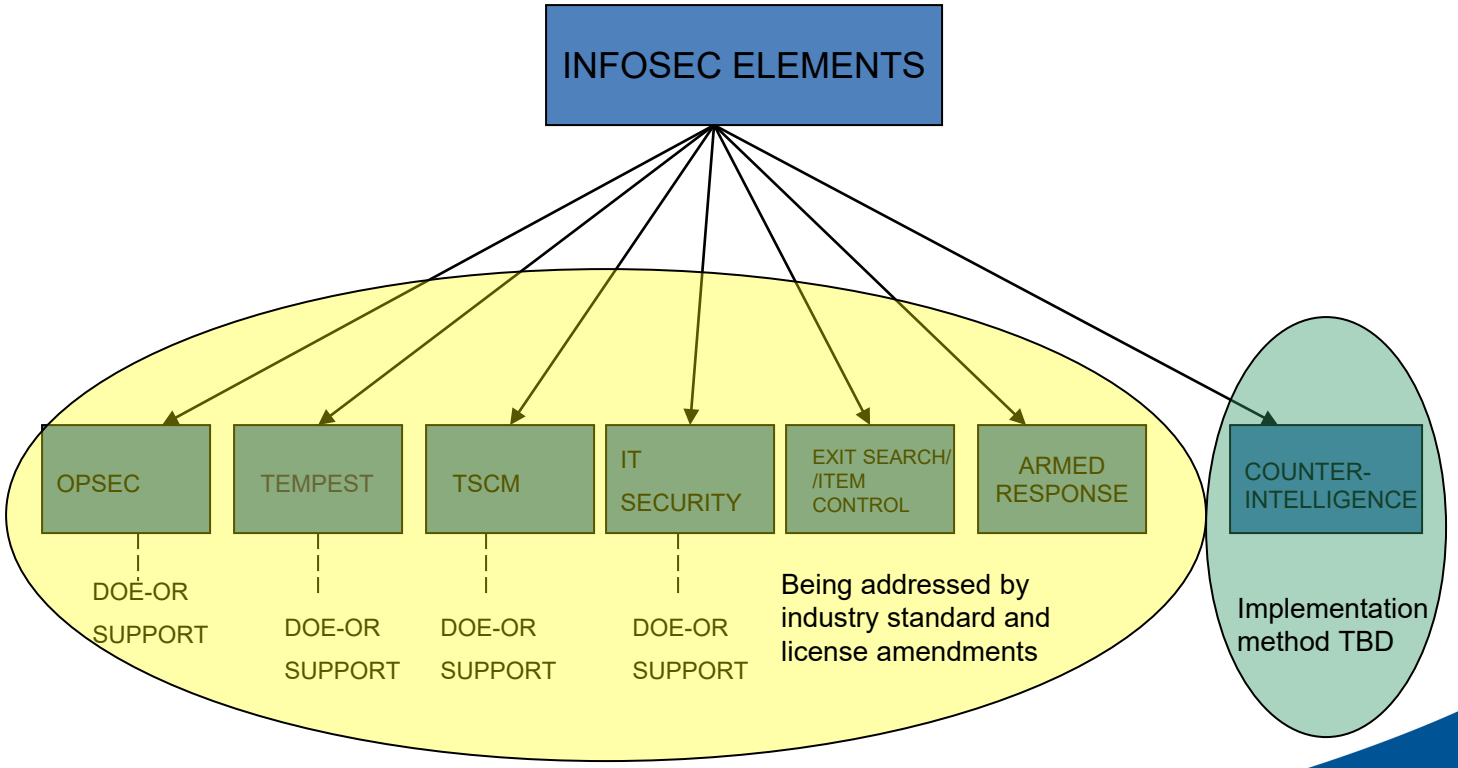
- Louisiana Energy Services National Enrichment Facility
- General Electric/Silex test loop,
- General Electric/Silex full-scale plant,
- AREVA
- USEC Lead Cascade
- USEC American Centrifuge Plant

# Existing NRC INFOSEC Measures for Commercial Uranium Enrichment Operations

- Addressed in 10CFR Parts 25 and 95:
  - Personnel clearance program
  - Classified document protection
  - Additional transportation requirements
  - Facility approval and FOCI
- Requirements track with National Industrial Security Program Operations Manual (NISPOM)

# Additional INFOSEC Measures for Enrichment Plants

- DOE has historically required a suite of special INFOSEC measures for enrichment sites under its purview, for counter-proliferation
- The US is bound by international agreements to protect classified enrichment technologies
- For the first time, enrichment activities are being undertaken by commercial entities in the U.S.
- The threat suggests the need for additional INFOSEC measures


INFOSEC ELEMENTS
OPSEC
TEMPEST
TSCM
IT SECURITY
EXIT SEARCH/ /ITEM CONTROL
ARMED RESPONSE
COUNTER-INTELLIGENCE
DOE-OR SUPPORT
DOE-OR SUPPORT
DOE-OR SUPPORT
DOE-OR SUPPORT
Being addressed by industry standard and license amendments
Implementation method TBD

# The Threat Associated with Proliferation of Enrichment Technologies

*(INCLUDE HIGHLIGHTS FROM DOE THREAT BRIEF HERE)*

# NRC Statutory Authority

- OGC affirms that the NRC has the statutory authority under the Atomic Energy Act to protect classified matter, including enrichment technologies. This would include the adoption of CI programs. CI programs are considered a logical extension of the INFOSEC requirements the NRC has previously promulgated in 10CFR Parts 25 and 95.

# Privacy Considerations

- OGC further advises that NRC-instituted CI programs should not include measures such as e-mail monitoring.
- This limitation would not restrict the FBI from employing duly authorized monitoring techniques when investigating a CI case, under DOJ procedures and guidelines

# Counterintelligence (CI)

- Capabilities of CI programs would include:
  - Awareness briefings
  - Sharing intelligence information relevant to the regulated facilities
  - Performing limited analysis of CI data
  - Obtaining intelligence community background checks for certain visitors
  - Foreign travel pre- and post- briefings
  - Cooperating with federal CI investigations, as appropriate

# Existing CI Programs

*(Other federal programs the NRC could utilize)*

- **FBI Domain Program**
  - Existing program to protect key infrastructure elements within the geographical region of FBI field offices
  - Provides awareness briefs, FBI name checks
  - Requires sharing of limited FBI resources with other interests
  - Requires MOA w/FBI
  - No cost to NRC or industry

- **DOE CI Program**
  - Existing 300+ person program focused on classified nuclear operations and technologies
  - Provides awareness briefs, DOE and Intelligence Community (IC) name checks
  - Requires MOA w/DOE, IC
  - Likely to be cost-reimbursable to DOE

*Note: The FBI has sole federal jurisdiction to investigate and prosecute CI cases, regardless of program selected*

# Requirement for In-House CI Staff

- FBI and DOE agree that an in-house NRC CI staff would be required
- Individuals should have bona fide CI backgrounds
- Activities would include:
  - CI policy/requirements
  - Program coordination
  - Liaison with other federal agencies
  - Data analysis
  - Processing of name checks through other agencies
  - Awareness support
  - Inspection guidance
  - Inspections and enforcement

# Options for CI Programs

1. Status Quo. No CI Program
2. Adopt FBI Domain Program with Licensee CI POCs
3. Adopt FBI Domain Program with on-site NRC CI POCs
4. Utilize DOE's CI Program with Licensee CI POCs
5. Utilize DOE's CI Program with on-site NRC CI POCs
6. Utilize DOE's CI Program with Licensee CI POCs, and NRC staff co-located with DOE CI staff
7. Utilize DOE's CI Program with on-site NRC CI POCs, and NRC staff co-located with DOE CI staff

# Comparison of CI Program Options

| CI PROGRAM OPTIONS | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Features/Requirements---> | FBI Awareness Briefs | DOE Awareness Briefs | CIA Awareness Briefs | FBI Name Checks | DOE Name Checks | CIA Name Checks | FBI MOU Required | DOE MOU Required | CIA MOU Required | FBI investigate cases | In-House NRC Staff Required | NRC Fed CI POC at Sites | NRC CI Fed located at DOE HQ |
| **OPTIONS** | | | | | | | | | | | | | |
| **1. Status Quo- no CI program** | | | | | | | | | | √ | | | |
| **2. FBI Domain Program- Licensee POCs** | √ | | | √ | | | √ | | | √ | √ | | |
| **3. FBI Domain Program with NRC POCs at Sites** | √ | | | √ | | | √ | | | √ | √ | √ | |
| **4. DOE Program-Licensee POCs** | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | |
| **5. DOE/Program with NRC POCs at Sites** | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | |
| **6. DOE Program-Licensee POCs, with NRC CI staff at DOE HQ** | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ |
| **7. DOE Program with NRC POCs at Sites and NRC CI staff at DOE HQ** | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |

# Path Forward

- Decision on NSIR organizational element to implement new INFOSEC-CI programs, and transfer of responsibility
- Develop resource estimates (in-house and industry impacts)
- Obtain Program Office concurrence in option paper
- Obtain Commission approval of CI program options

U.S.NRC

United States Nuclear Regulatory Commission

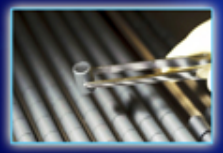
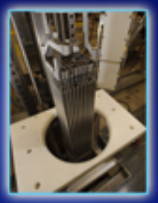
*Protecting People and the Environment*

# INFORMATION SECURITY (INFOSEC) Inspection Procedure (IP) Changes

October 13, 2021





Division of Fuel Facility Inspection

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# INFOSEC Resources Prior to NRC AO Activities

| NRC | DOE |
| --- | --- |
| NRC Region 2 inspectors | DOE Authorizing Official |
| NRC HQ inspectors | DOE Inspectors |
| | DOE Contract Subject Matter Experts (SMEs) |
| | DOE Classification Officer |

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# INFOSEC Resources After NRC AO Activities

| NRC | DOE |
| --- | --- |
| NRC Region 2 inspectors | |
| NRC HQ inspectors | |
| NRC Contract SMEs | |
| NRC Authorizing Official | |
| | DOE Classification Officer |

# IP 81820 – Physical Protection Facility Approval of National Security Information (NSI) and Restricted Data (RD)

Previous Areas Specifically Identified:

- security plan
- protection of classified matter while in use
- storage of classified matter
- keys
- protective personnel
- lock combinations
- unlocked security containers

# IP 81820 – Physical Protection Facility Approval of National Security Information (NSI) and Restricted Data (RD)

Previous Areas Specifically Identified (continued):

- reproduction/destruction
- marking of documents
- external transmission
- revocation of access authorization
- automated data processing (ADP)
- education
- establishment of restricted/closed areas

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# IP 81820 – Physical Protection Facility Approval of National Security Information (NSI) and Restricted Data (RD)

Previous Areas Specifically Identified (continued):

- access to NSI/RD
- termination of facility approval
- reports
- records

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# IP 81820 – Physical Protection Facility Approval of National Security Information (NSI) and Restricted Data (RD)

Areas Specifically Added:

- NEI 08-11 Areas
  - Operational Security (OPSEC)
  - TEMPEST
  - Technical Surveillance Countermeasures (TCM)
  - Counterintelligence
  - Classified Item Control and Inventory (CICI)
  - Armed Response to Information Compromise (ARTIC)

- Reports
- Records

# IP 81820 – Physical Protection Facility Approval of National Security Information (NSI) and Restricted Data (RD)

Areas Specifically Added (continued):

- ADP Areas
  - Review of all classified network critical controls
  - Review of select classified network non-critical controls
  - Review of authorized equipment type and configuration
  - Classified network system walkdowns
  - Interviews with classified network administrators and SMEs
- 32CFR117 vs. 10CFR95 gaps (TBD)

- Reports

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# Impact to Licensees

- Estimated hours 48 to 160 direct inspection effort (DIE)
  - Comparable hours, just shifted from DOE/DOE contract support to NRC direct activities except DOE classification officer
- Activities added and previously inspected
  - NEI 08-11
  - Classified network reviews
  - AO authorization
- Activities not previously inspected and under evaluation
  - 32 CFR 117 (NISPOM) vs. 10 CFR 95 requirements

# Impact to Licensees

- IP 81820 used to focus on 10CFR95/32CFR117 requirements
  - Licensee will be inspected against 10CFR95/32CFR117 requirements and associated commitments contained within approved licensing documents
  - Licensee will be inspected against commitments contained within approved licensing documents associated with NEI 08-11, NIST, etc.

U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

# Questions?