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

Insider Threat Program and Security Executive Agent Directive 3 for NRC-Licensed Facilities

US NRC Public Meeting

21 February 2018

Office of Nuclear Security and Incident Response

9:00 am

Introductions

- Darryl Parsons, Branch Chief

  Information Security Branch

  Division of Security Operations

  Office of Nuclear Security and Incident Response

  Darryl.Parsons@nrc.gov

9:10 am – 10:00 am

Information on SEAD 3 and Insider Threat Programs

Insider Threat Program

- Executive Order 13587 was adopted by National Industrial Security Program to cover all contractors and licensees who have exposure to classified information. https://www.gpo.gov/fdsys/granule/CFR-2012-title3-vol1/CFR-2012-title3-vol1-eo13587

- The National Industrial Security Program Operating Manual (NISPOM) Change 2 incorporated May 2016 covers the implementation of an Insider Threat Program (ITP)
  http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf

Non-Possessing Facility Security Clearance

- Any facility which has cleared individuals (those with personnel security clearances) and does not possess classified material onsite is considered a non-possessing facility.

- The majority of NRC's contractors and licensees are non-possessing entities.

Possessing Facility Security Clearance

- The NRC issues possessing facility clearances and associated personnel security clearances to licensees and licensee contractors that meet the requirements of 10 CFR Part 95, Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," and 10 CFR Part 25, "Access Authorization," and possess a demonstrable need to store classified information at their facility.

- Only two facilities have possessing facility clearances issued by the NRC as the Cognizant Security Agency.

- These facilities need access to classified information in order to maintain their license.

NISPOM ITP for Non-Possessing Licensees
Four Minimum Requirements

- Appointment by the licensee of an ITP Senior Official who is a U.S. citizen and a senior official of the company.
  - This can be the Facility Security Officer (FSO) as defined by the NISPOM.

- Annual self-review or self inspection of the ITP.

- Insider Threat training for cleared program management and cleared individual awareness.

- Reporting to the NRC of any detection of an insider threat to the licensee. (This program is designed for threats to the protection of classified information, and does not have in its scope any other detection of insider threats at a power plant).

NISPOM ITP for Possessing Licensees
Five Minimum Requirements

- Appointment by the licensee of an ITP Senior Official who is a U.S. citizen and a senior official of the company. (same as non-possessors)
  - This can be the Facility Security Officer (FSO) as defined by the NISPOM.
- Annual self-review or self inspection of the ITP. (same as non-possessors)
- Insider Threat training for cleared program management and cleared individual awareness. (same as non-possessors)
- Reporting to the NRC of any detection of an insider threat to the licensee. (This program is designed for threats to the protection of classified information, and does not have in its scope any other detection of insider threats at a power plant). (same as non-possessors)
- Provide User Activity Monitoring on any classified IT system.

Implementation of NISPOM ITP

- The NRC staff are recommending to the Commission that we pursue a license commitment by incorporating the requirements into the Standard Practice Procedures Plan in accordance with 10 CFR Part 95.

- ITP requirements planned implementation by **June 2018**. The staff are seeking input from licensees throughout this process.

- By modifying the SPPP, which is already committed to in each license, the licensee makes the ITP requirements a license commitment without having to do an amendment to the license itself.

Security Executive Agent Directive (SEAD) 3

- In December 2016, the Office of the Director of National Intelligence (ODNI) issued SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position," to executive branch agencies and covered individuals; these individuals include NRC employees, contractors, licensees, licensees' contractors, and other individuals such as members of the Nuclear Energy Institute whom NRC has granted national security clearances.

- SEAD 3 defines covered individuals as:
  - certain persons who perform work on behalf of the executive branch and have been granted access to classified information or hold sensitive positions;
  - certain persons who perform work on behalf of a State, local, Tribe, or private sector entity and have been granted access to classified information or hold sensitive positions; and
  - certain persons working in or for the legislative or judicial branches and have been granted access to classified information and the investigation or determination has been conducted by the executive branch.

SEAD 3

- SEAD 3 was to be effective on June 12, 2017. The NRC requested an extension to the requirements until June 12, 2018.

- SEAD 3 requires reporting of 19 new data elements consistent with the Standard Form-86, "Questionnaire for National Security Positions," which applicants and clearance holders complete during the initial and periodic reinvestigation processes, respectively. However, SEAD 3 now requires these elements to be reported prior to participation in such activities or otherwise as soon as possible following the start of their involvement.

SEAD 3

- Most notably, SEAD 3 requires covered individuals to obtain prior agency approval before conducting unofficial foreign travel.

- The staff benchmarked 10 other Federal agencies to understand the different implementation approaches across the Government.
  - The staff's benchmarking efforts concluded that other Federal agencies apply SEAD 3 to all cleared staff and contractors, and in some cases to others deemed to be in sensitive positions.
  - Generally, other Federal agencies require pre-travel approval for travel to countries that do not reside on an agency-developed approved destination country list.
  - Additionally, some other Federal agencies disapprove travel to destination countries on an agency-developed threat country list.
  - No agencies are allowing covered individuals to travel without pre-travel approval except as noted in SEAD 3, such as travel to U.S. territories or short notice emergent travel.

SEAD 3, Element 1 – Unofficial Foreign Travel Reporting

- Complete itinerary
- Dates of travel
- Mode of transportation and identification of carriers
- Passport data
- Names and association (business, friend, relative, etc.) of foreign national traveling companions
- Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.)
- Unplanned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (post-travel reporting)
- Name, address, telephone number, and relationship of emergency point of contact
- Unusual or suspicious occurrences during travel, including those of possible security or counterintelligence significance (post-travel reporting)
- Any foreign legal or customs incidents encountered (post-travel reporting)

SEAD 3, Other 18 Reporting Elements

- Unofficial contact with a known or suspected foreign intelligence entity
- Continuing association with a known foreign national(s) or foreign national roommate(s)
- Involvement in Foreign Business
- Foreign bank accounts (new)
- Ownership of Foreign Property (new)
- Foreign Citizenship (new)
- Application for a foreign passport or identity card for travel (new)
- Possession of a foreign passport or identity card for travel (new)
- Use of a foreign passport or identity card for travel
- Voting in a foreign election (new)
- Adoption of non-U.S. citizen children (new)
- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure (new)
- Media Contacts
- Arrests
- Financial issues and anomalies
- Cohabitant(s)
- Marriage
- Alcohol- and drug-related treatment

**New to Part 25 requirements but similar to requirements already in Standard Form 86—timeframe for reporting has changed*

Current Reporting Requirements under 10 CFR Part 25

- Arrests/charges/detentions
- Involvement in civil court actions
- Change in marital status (including legal separation)
- Change of name
- Change in cohabitation
- Outside employment that creates a conflict of interest
- Foreign national contacts including business or personal contacts
- Any travel to foreign countries for which the U.S. Department of State has issued a travel warning
- Enrollment in a drug or alcohol treatment program
- Changes in financial status (debt collection, bankruptcy, foreclosure, federally- guaranteed loans, tax liens, or failure to file or pay Federal or State taxes)
- Treatment for emotional, mental, or personality disorders (except marriage, grief, or family counseling not related to violence by you or strictly related to adjustments from service in a military combat environment)
- Travel to a foreign country where a passport other than a U.S. passport is used to enter or leave the country
- While on travel, any arrests, and detentions, issues with customs or law enforcement, or concerns that you were being followed or monitored while on official or unofficial foreign travel

Implementation of SEAD 3

Staff proposed implementation of SEAD 3 is consistent with the staff's proposed implementation of the NISPOM ITP as previously discussed:

- The NRC staff are recommending to the Commission that we pursue a license commitment by incorporating the requirements into the Standard Practice Procedures Plan in accordance with 10 CFR Part 95.

- SEAD 3 requirements planned implementation by **June 2018**. The staff are seeking input from licensees throughout this process.

- By modifying the SPPP, which is already committed to in each license, the licensee makes the requirements a license commitment without having to do an amendment to the license itself.

FOCI Questions

- Comment from Industry:
  - FOCI process is too burdensome.

- NRC's Comment:
  - We agree, please send an email to me and let me research each particular case. We may have some methods to now address the issue.
  - Darryl.Parsons@nrc.gov

10:00 am – 10:30 am

Questions and Answers

10:30 am – 11:00 am

Proposed SPPP Language and Discussion

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

NISPOM ITP suggested language for SPPP for possessing facilities

Procedures have been developed which establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat in accordance with Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) insider threat program requirements.

These procedures include at a minimum: (1) appointment of an insider threat program senior official (ITPSO); (2) training for employees covered under the program; (3) annual self-inspections of the insider threat program; (4) timely reporting for any potential or actual insider threat; and (5) user activity monitoring on any classified information system.

NISPOM ITP suggested language for SPPP for non-possessing facilities

Procedures have been developed which establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat in accordance with Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) insider threat program requirements.

These procedures include at a minimum: (1) appointment of an insider threat program senior official (ITPSO); (2) training for employees covered under the program; (3) annual self-inspections of the insider threat program; and (4) timely reporting for any potential or actual insider threat.

SEAD 3 suggested language for SPPP for both possessing and non-possessing facilities

Procedures have been developed for individuals who have access to classified information or hold a sensitive position which establish and maintain standardized reporting requirements in accordance with the 19 elements as required by the Office of the Director of National Intelligence (ODNI) Security Executive Agent Directive 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position," dated December 14, 2016.

Example of what the Staff will be looking for during SPPP Reviews

Reviewer's Checklist for Non-Possessors SPPP

☐ Does the licensee commit to having procedures that establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat in accordance with Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) insider threat program requirements?

☐ Do the licensee's insider threat program procedures commit to addressing the appointment of an insider threat program senior official (ITPSO)?

☐ Do the licensee's insider threat program procedures commit to training for employees covered under the program?

☐ Do the licensee's insider threat program procedures commit to annual self-inspections of the insider threat program?

☐ Do the licensee's insider threat program procedures commit to timely reporting for any potential or actual insider threat?

☐ Does the licensee commit to having procedures for individuals who have access to classified information or hold a sensitive position which establish and maintain standardized reporting requirements in accordance with the Office of the Director of National Intelligence (ODNI) Security Executive Agent Directive 3 (SEAD 3)*, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position,"* dated December 14, 2016?

☐ Does the licensee address the fact that there are 19 required data elements for reporting under SEAD 3 and that the information under each element must either be self-reported or reported for others? See the table below to ensure the 19 data elements are acknowledged and addressed in licensee procedures.

Meeting Adjourned

There will be a second public meeting on

March 12th

with a focus on answering questions that have been identified today.

Thank you for your participation!

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