

Security Panel

October 31, 2018

Bill Schuster and Beth Reed, NRC/NRR

Janine Mason, DHS/OIP

Lance English, NRC/NSIR

Agenda

- Bill Schuster - Part 37 Implementation
- Beth Reed - NPR Security Related Topics
 - Mailing Sensitive Documents
 - Reporting Events to the NRC
 - Cyber Security
- Janine Mason - Critical Infrastructure and NPR Subcouncil
- Lance English - Foreign National Program

Physical Protection of Cat I and II Quantities of Materials

William Schuster, Reactor Engineer
Research and Test Reactors Oversight Branch

2018 TRTR Conference
October 31, 2018

Part 37 - Background

- Preceded by Orders (RAMQC)
- Final Rule: 78 FR 17007
 - Pub. Mar 19, 2013; Eff. May 20, 2013
 - Compliance by Mar 14, 2014

Table 1 – Category 1 and Category 2 Threshold

(From Appendix A to Part 37 – Category 1
and Category 2 Radioactive Materials)

Radioactive Material	Category 1 (TBq)	Category 1 (Ci)	Category 2 (TBq)	Category 2 (Ci)
Americium-241	60	1,620	0.6	16.2
Americium-241/Be	60	1,620	0.6	16.2
Californium-252	20	540	0.2	5.40
Cobalt-60	30	810	0.3	8.10
Curium-244	50	1,350	0.5	13.5
Cesium-137	100	2,700	1	27.0
Gadolinium-153	1,000	27,000	10	270
Iridium-192	80	2,160	0.8	21.6
Plutonium-238	60	1,620	0.6	16.2
Plutonium-239/Be	60	1,620	0.6	16.2
Promethium-147	40,000	1,080,000	400	10,800
Radium-226	40	1,080	0.4	10.8
Selenium-75	200	5,400	2	54.0
Strontium-90	1,000	27,000	10	270
Thulium-170	20,000	540,000	200	5,400
Ytterbium-169	300	8,100	3	81.0

Part 37 - Inspection Implementation

- Oversight responsibility
 - NRC
 - Not located in an Agreement State
 - Part 37 material is under the Part 50 license
 - Agreement States

Part 37 - Inspection Timeframe

- Conducted with next security inspection
- Frequency
 - Typically 3 or more years
 - Based on material quantity and form

Part 37 - Inspection Items

- Access Authorization
 - Investigations
 - Access Authorization Program Review
- Security Program
 - LLEA Coordination
 - Security Zones
 - Monitoring and Detection
 - Maintenance and Testing
 - Mobile Devices
 - Security Program Review
- Transportation

Part 37 - Summary

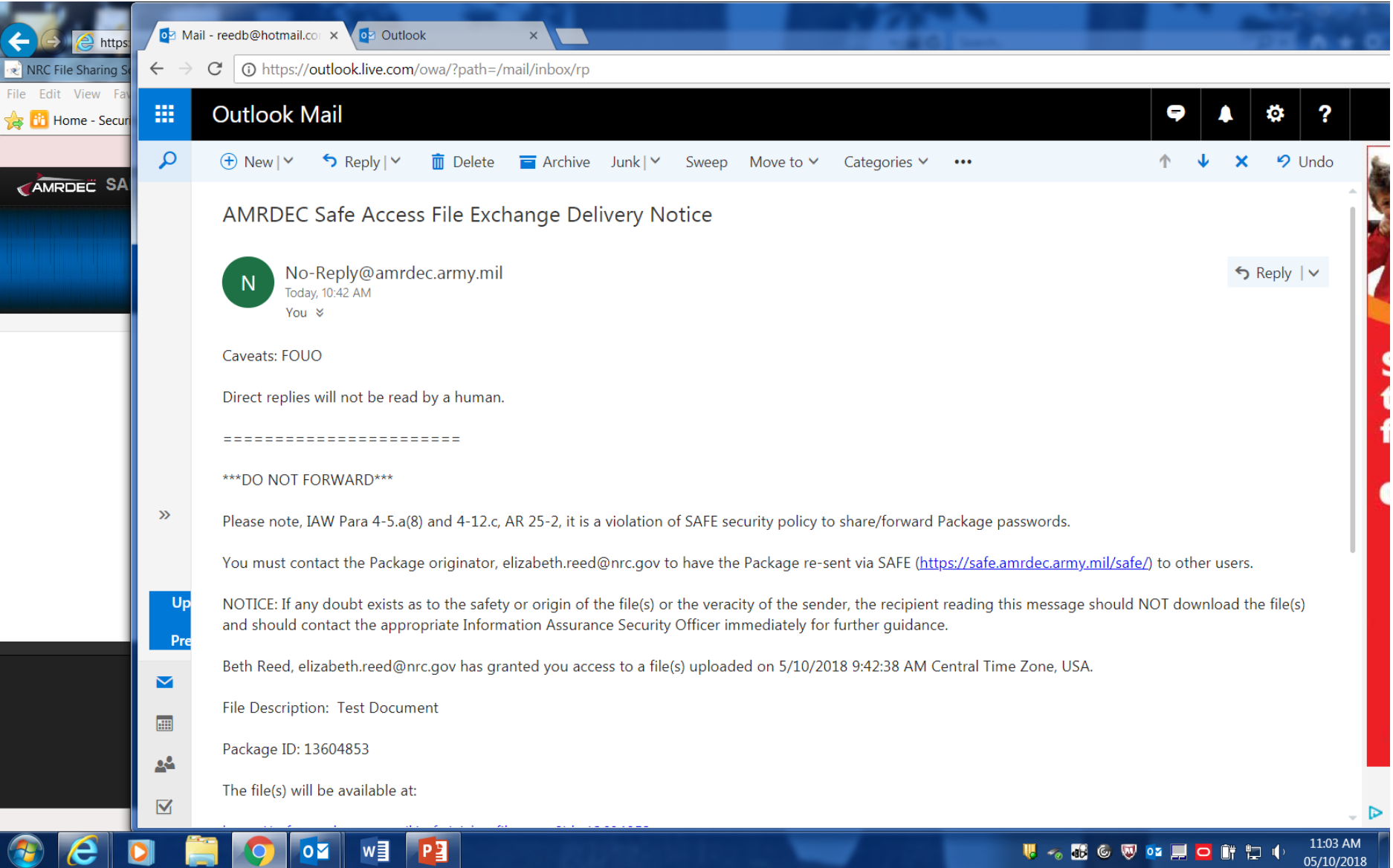
- Taking possession of sources or protecting under Part 73 PSP can present challenges
- Key to compliance is documentation

Regulatory Discussion


Beth Reed, Security Specialist
Research and Test Reactors Oversight Branch
2018 TRTR Conference
October 31, 2018

New NRC Process for E-Mailing Official Use Only Documents

- NRC is no longer allowed to e-mail OOU or PII documents to anyone external to the NRC
 - Yellow Announcement: YA-17-0068 (ML#17200D030)
 - Management Directive 12.5
- Types of documents
 - Security Plan RAI's
 - Security Inspection Report
 - License Operator Medical Information
- Temporary fix is to use a third party site (Army)
 - [AMRDECT SAFE at https://safe.amrdec.army.mil/safe/](https://safe.amrdec.army.mil/safe/)



AMRDEC Safe Access File Exchange Delivery Notice

 No-Reply@amrdec.army.mil
Today, 10:42 AM
You

Reply

Caveats: FOUO

Direct replies will not be read by a human.

=====

DO NOT FORWARD

>>

Please note, IAW Para 4-5.a(8) and 4-12.c, AR 25-2, it is a violation of SAFE security policy to share/forward Package passwords.

You must contact the Package originator, elizabeth.reed@nrc.gov to have the Package re-sent via SAFE (<https://safe.amrdec.army.mil/safe/>) to other users.

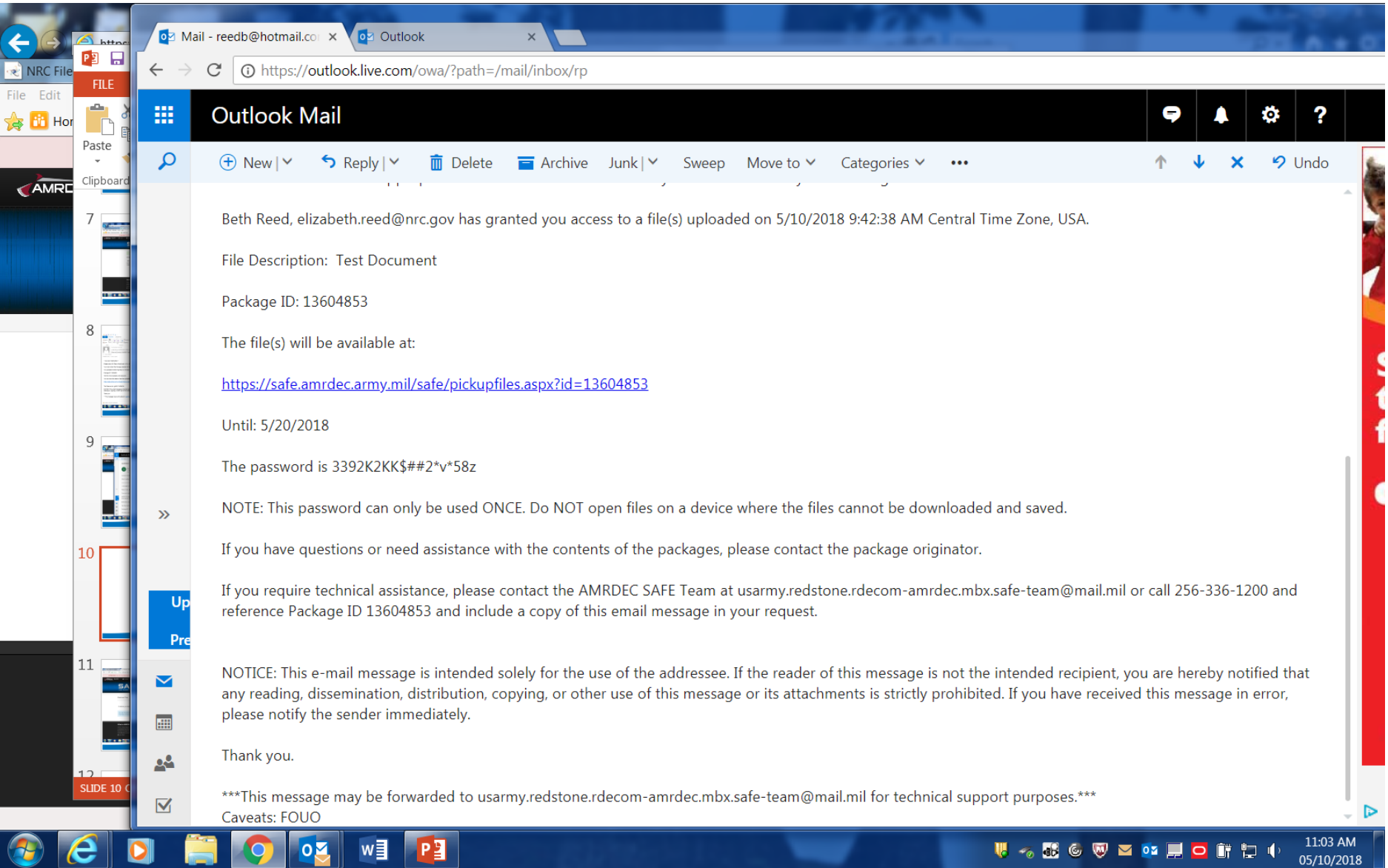
NOTICE: If any doubt exists as to the safety or origin of the file(s) or the veracity of the sender, the recipient reading this message should NOT download the file(s) and should contact the appropriate Information Assurance Security Officer immediately for further guidance.

Beth Reed, elizabeth.reed@nrc.gov has granted you access to a file(s) uploaded on 5/10/2018 9:42:38 AM Central Time Zone, USA.

File Description: Test Document

Package ID: 13604853

The file(s) will be available at:



Mail - reedb@hotmail.com x Outlook x
https://outlook.live.com/owa/?path=/mail/inbox/rp

Outlook Mail

New | Reply | Delete | Archive | Junk | Sweep | Move to | Categories | Undo

Beth Reed, elizabeth.reed@nrc.gov has granted you access to a file(s) uploaded on 5/10/2018 9:42:38 AM Central Time Zone, USA.

File Description: Test Document

Package ID: 13604853

The file(s) will be available at:

<https://safe.amrdec.army.mil/safe/pickupfiles.aspx?id=13604853>

Until: 5/20/2018

The password is 3392K2KK\$##2*v*58z

NOTE: This password can only be used ONCE. Do NOT open files on a device where the files cannot be downloaded and saved.

If you have questions or need assistance with the contents of the packages, please contact the package originator.

If you require technical assistance, please contact the AMRDEC SAFE Team at usarmy.redstone.rdecom-amrdec.mbx.safe-team@mail.mil or call 256-336-1200 and reference Package ID 13604853 and include a copy of this email message in your request.

NOTICE: This e-mail message is intended solely for the use of the addressee. If the reader of this message is not the intended recipient, you are hereby notified that any reading, dissemination, distribution, copying, or other use of this message or its attachments is strictly prohibited. If you have received this message in error, please notify the sender immediately.

Thank you.

This message may be forwarded to usarmy.redstone.rdecom-amrdec.mbx.safe-team@mail.mil for technical support purposes.
Caveats: FOUO

ATTENTION: Due to circumstances beyond our control, all packages uploaded before Friday, 13 April 2018 will have to be uploaded again. We are sorry for any inconvenience this may cause.

SAFE

Safe Access File Exchange

SAFE is designed to provide AMRDEC and its customers an alternative way to send files other than email. SAFE supports file sizes up to 2GB.

[Click here for Getting Started Guide](#)

Retrieve Files

To retrieve your file(s), please enter your password:

Submit

[Where is my Password?](#)

You may only download a file **ONE TIME**.

The file(s) will be locked from further downloads after you finish downloading all files in the package.

What is AMRDEC

The U. S. Army Aviation and Missile Research Development and Engineering Center, a subordinate laboratory to the Research, Development and Engineering Command, is the Army's focal point for providing research, development, and engineering technology and services for aviation and missile platforms across the lifecycle.

[Learn More](#)

Quick Links

[Home](#)

[About](#)

[Getting Started Guide](#)

Resources

[Security Notice](#)

[Accessibility Notice](#)

[ISalute](#)

Support

[Knowledge Base](#)

[Version History](#)

Sending Non-Public Documents to the NRC

- Sensitive Information
 - Security-Related Information
 - Request for NRC Approved Reviewing Official
 - Responses to Security Plan RAI's
 - Medical Information
 - License Operator Request
- Safeguards Information
 - Physical Security Plan
 - Responses to Security Plan RAI's



Marking Documents under 10 CFR 2.390

- 10 CFR 2.390(b)(1)(i)(A), Mark at the top and bottom of each page with language similar to: “**confidential information submitted under 10 CFR 2.390,**” “**withhold from public disclosure under 10 CFR 2.390,**” or “**proprietary,**” to indicate that it contains information the submitter seeks to have withheld.
- For withholding SRI, use: “Security-Related Information – Withhold Under 10 CFR 2.390.”
- Update: Mark the header and footer of the transmittal letter with “Security-Related Information – Withhold Under 10 CFR 2.390.”
- Include separation statement

Mailing Documents under 10 CFR 2.390

- Single Envelope
- Address: U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001 **ATTN: Document Control Desk**
- Do not address directly to the PM or Security Specialist

Marking Documents SGI or SGI-M

- The **transmittal letter** forwarding the **physical security plan (PSP)** to the U.S. NRC, and each page of the PSP, must be marked “Safeguards Information – Modified Handling” (or “Safeguards Information” if applicable) on the header and footer.
- The **transmittal letter** should also include a “separation from enclosure” statement if the letter itself does not contain SGI or SGI-M.
- The first page of the **PSP** needs to include:
 - A statement warning of unauthorized disclosure subject to civil and criminal penalties.
 - The name, title, and organization of the individual who made the SGI or SGI-M designation, and the date it was made.

Transmittal Letter and First Page of the PSP

SAFEGUARDS INFORMATION – MODIFIED HANDLING

[Facility name & address]

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
ATTN: (Project Manager)

[DATE]

SUBJECT:

[INSERT TEXT]

[SIGNATURE]

When separated from Safeguards Information designated as Safeguards Information – Modified Handling enclosure(s), this document is decontrolled provided the transmittal document does not otherwise warrant protection from unauthorized disclosure

Warning: Violation of Section 147 of the Atomic Energy Act, "Safeguards Information," is subject to Civil and Criminal Penalties

Safeguards Information Determination made by:
Organization _____
Name/Title _____
Date _____

SAFEGUARDS INFORMATION – MODIFIED HANDLING

SAFEGUARDS INFORMATION – MODIFIED HANDLING

Mailing SGI Documents

- Must be packaged in two sealed envelopes
 - Outer envelope: U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001 ATTN: Document Control Desk
 - Inner envelope: Name and address of the intended recipient and marked on both sides, top and bottom, with the words "Safeguards Information-Modified Handling"
- Good idea to use a mail service that will track the package

Who to call and How

- Call the Headquarters Operation Officer (HOO) at 301-816-5100
 - The HOO will notify the appropriate RTR staff (PM, security specialist)
- Be prepared to answer specific questions about event, the facility and the reactor status



Information for the HOO

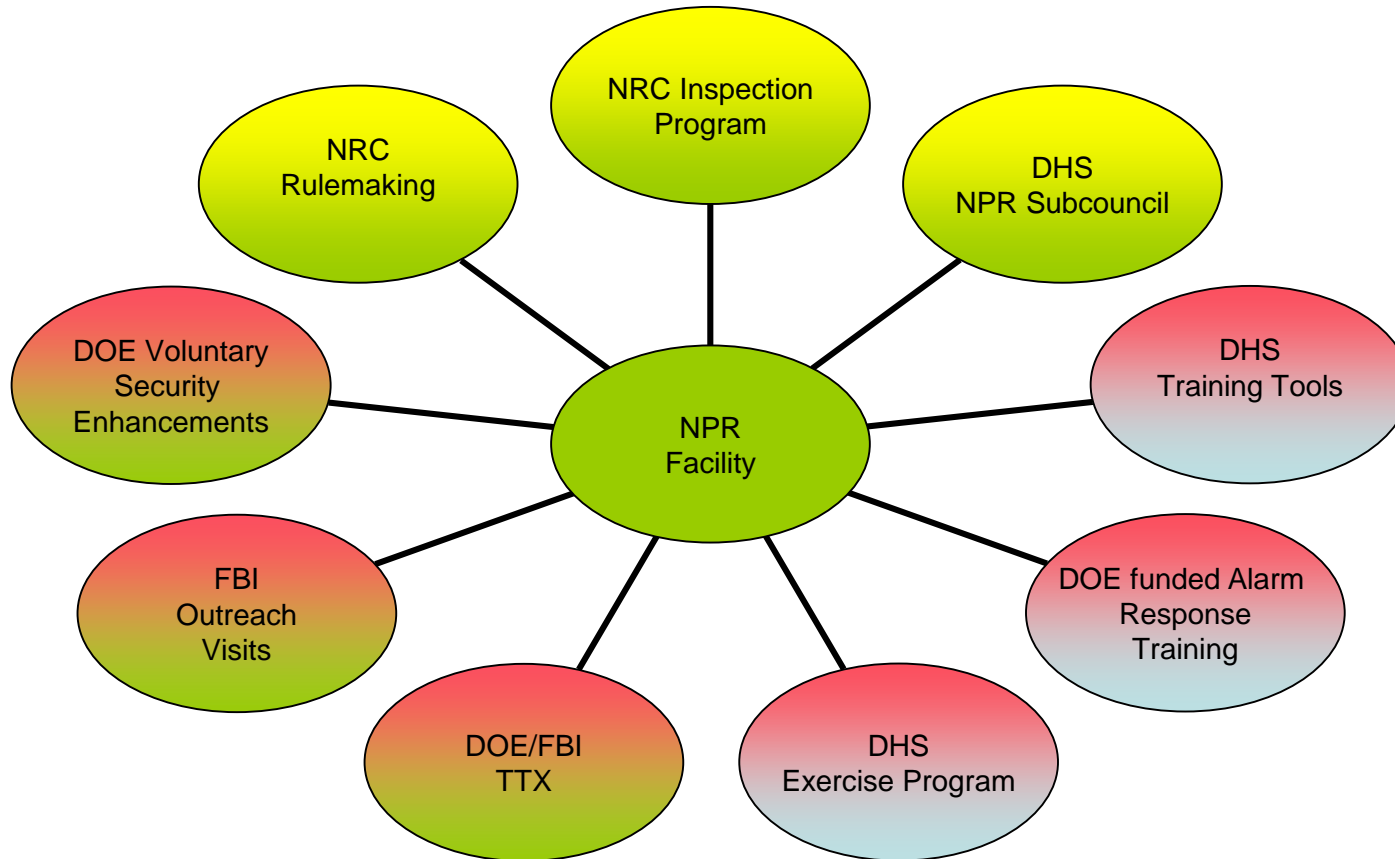
- Name of facility and caller, and call back number
- Time and date of event
- Reactor Information
 - Type
 - Power level and max pulse (if applicable)
 - Status
- Event Classification
 - EAL
 - Safeguards events/Security plan requirements
 - Information purposes - voluntary
- Technical Specification requirements

Cyber Security

- Finalizing the hypothetical all digital NPR Report
 - To determine if a cyberattack presents a mechanism of release of radioactive material that has not already been evaluated by the NRC
 - Compare consequences of a cyberattack to that of the previously assessed physical security consequences (2006)
- Document is under management review
- Conclusion of report will be used to justify decision for rulemaking



Interagency Resources



The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

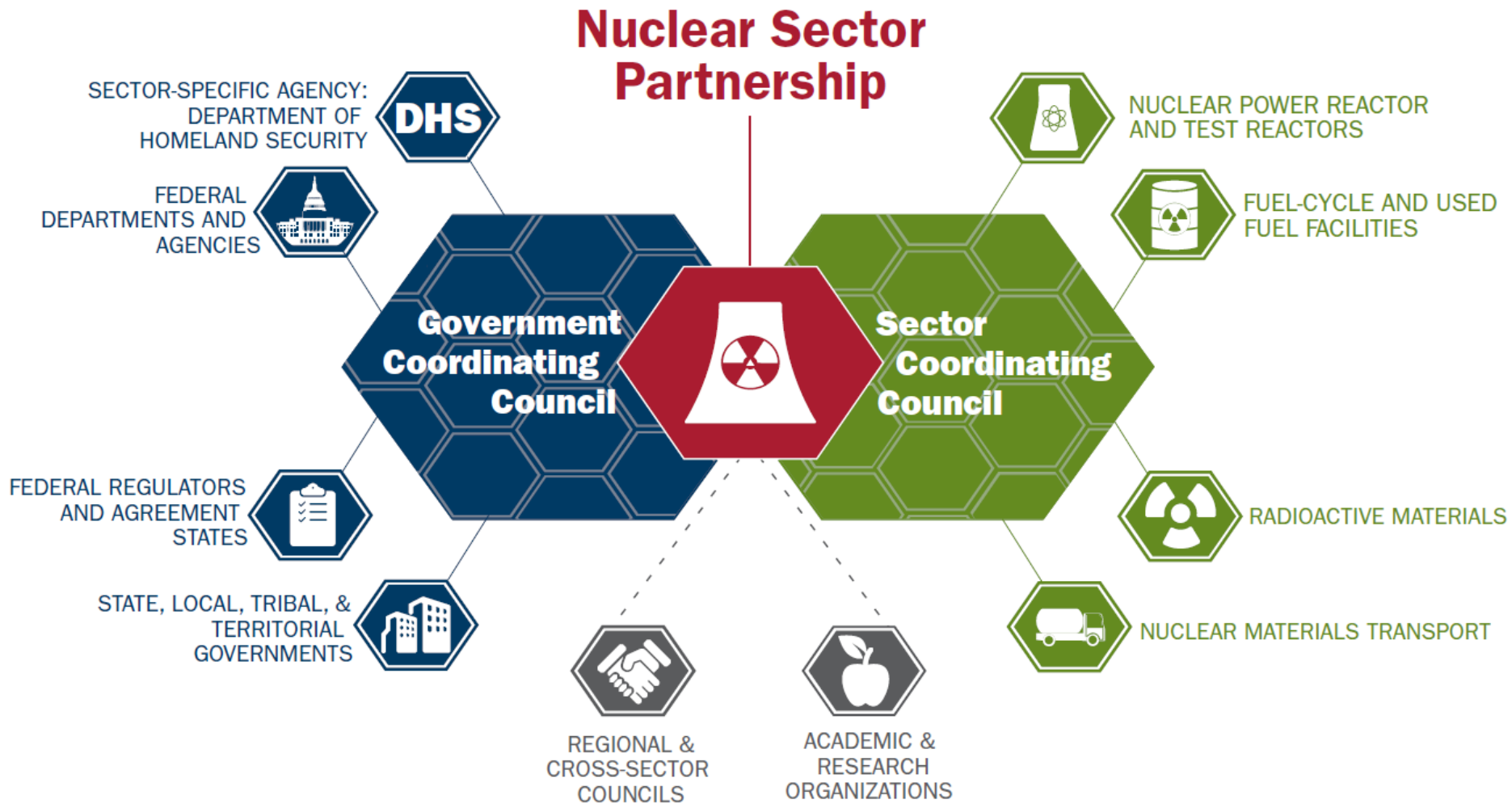
Nuclear Sector-Specific Agency

Non-Power Reactor Subcouncil Overview



Homeland
Security

Sector Partnership Environment



Non-Power Reactor Subcouncil

Mission: To provide effective coordination of security strategies and activities, policies and communications across Government and between the Government and NPR community.

- To coordinate with emergency management and public health and safety communities regarding consequence-management issues associated with any malevolent act involving the NPR subsector.

Goals: To coordinate efforts to sustain or enhance the necessary protection of the subsector assets through the following activities:

- Identify NPR security and preparedness issues that would benefit public-private coordination, and the communication and coordination of those issues.
- Identify potential enhancements to NPR security and preparedness plans, programs, policies, procedures and strategies.
- Recognize successful programs and practices through the sharing of experiences, ideas, effective practices and innovative approaches related to NPR protection.
- Leverage complementary resources within government and between government and industry.



Non-Power Reactor Subcouncil

NPR Subcouncil (NGCC/NSCC) Leadership

- Oregon State University (NSCC-NPR Co-Chair)
- Rhode Island Nuclear Science Center (NSCC-NPR Co-Chair)
- Nuclear SSA (NGCC-NPR Co-Chair)

Interagency Partners and Roles:

- Department of Homeland Security (DHS)
 - Partnership
 - Infrastructure Protection
- Nuclear Regulatory Commission (NRC)
 - Regulation
 - Cyber
- Department of Energy/National Nuclear Security Administration (DOE/NNSA)
 - Voluntary Security Enhancement Program
 - Alarm Response Force Training/Table Top Exercises
- Federal Bureau of Investigation (FBI)
 - Outreach Visits



**Homeland
Security**

Partnership Mechanisms

HSIN-CI

- The Homeland Security Information Network – Critical Infrastructure (HSIN-CI) is a secure portal that provides a “peer to peer” collaboration space for members to engage in real-time.
- Each subsector has its own subportal within the Commercial Facilities portal.
- Resources available on HSIN-CI include analysis, alerts, bulletins, training, and Suspicious Activity Reporting.
- To register, email: hsinci@hq.dhs.gov

The screenshot displays the HSIN-CI website interface. At the top, the header includes 'HSIN Homeland Security Information Network' and 'Community Directory'. Below the header is the 'Critical Infrastructure (CI) Home' section, which features a navigation menu with 'Sector Overviews', 'Content Providers', 'Resources', 'About CI', and 'CI Home'. The main content area is titled 'Protective Measures' and includes a 'View topic content' link. A large image of a construction worker is featured with the text 'Protective Measures'. To the right, there is a 'Search By Topic' section with a list of categories: Active Shooter, BlackEnergy, Continuity of Operations, Cybersecurity, Domestic Extremism, GPS Activities, Improvised Explosive Device, Insider Threat, Natural Disaster, Power Grid Attacks, Protective Measures, Terrorism TTPs, Travel Warnings, and Unmanned Aircraft Systems. Below the main content, there are four sections: 'Terrorism Alerts' featuring the NTAS logo and an 'ACTIVE BULLETIN' link; 'Recent CI Documents (30 Days)' listing 'CI Home (98)' and 'TSA Intel on HSIN CI (105)'; 'Latest Documents' listing various reports and documents with dates; and 'My CI Communities' featuring a row of community logos and a list of community names including 'CI Cyber Information', 'CI Security and Resilience Training', 'EXERCISE Cascadia Rising', 'NCCIC Knowledge Operations Management', 'Office of Cyber & Infrastructure Analysis (OCA)', and 'FCII Program'.



Homeland
Security



Homeland Security

For more information visit:

<https://www.dhs.gov/nuclear-reactors-materials-and-waste-sector>

Email: NuclearSSA@hq.dhs.gov



NRC'S Counterintelligence Briefing

**TRTR Conference – Newport, Rhode Island
October 31, 2018**

**Lance English, Counterintelligence Program Manager - NRC
Desiree Davis, Intelligence Analyst - NRC
Joseph H. Altman, Special Agent - FBI**





Introduction

Counterintelligence programs aim to identify intelligence threats from state and non-state actors.

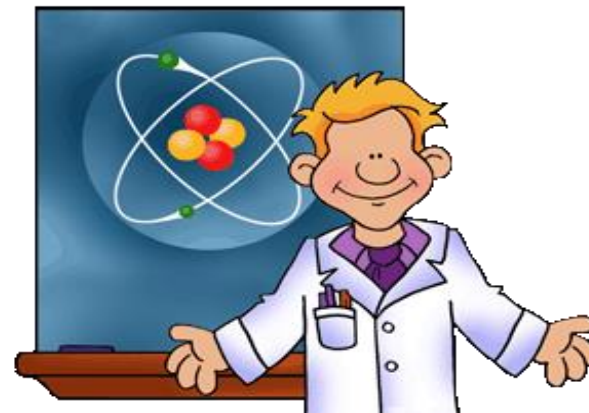
As a defensive counterintelligence program participant, you can help the NRC focus efforts on preventing foreign actors from penetrating your institution and protect your research from foreign actors.





Agenda

- ▶ Definition of Counterintelligence (CI)
- ▶ Education or Espionage (video clip)
- ▶ FBI Presentation CI Awareness
- ▶ Importance of Foreign Visitor Screening
- ▶ Federal Government Response
- ▶ What You Can Do to Help
- ▶ Reporting



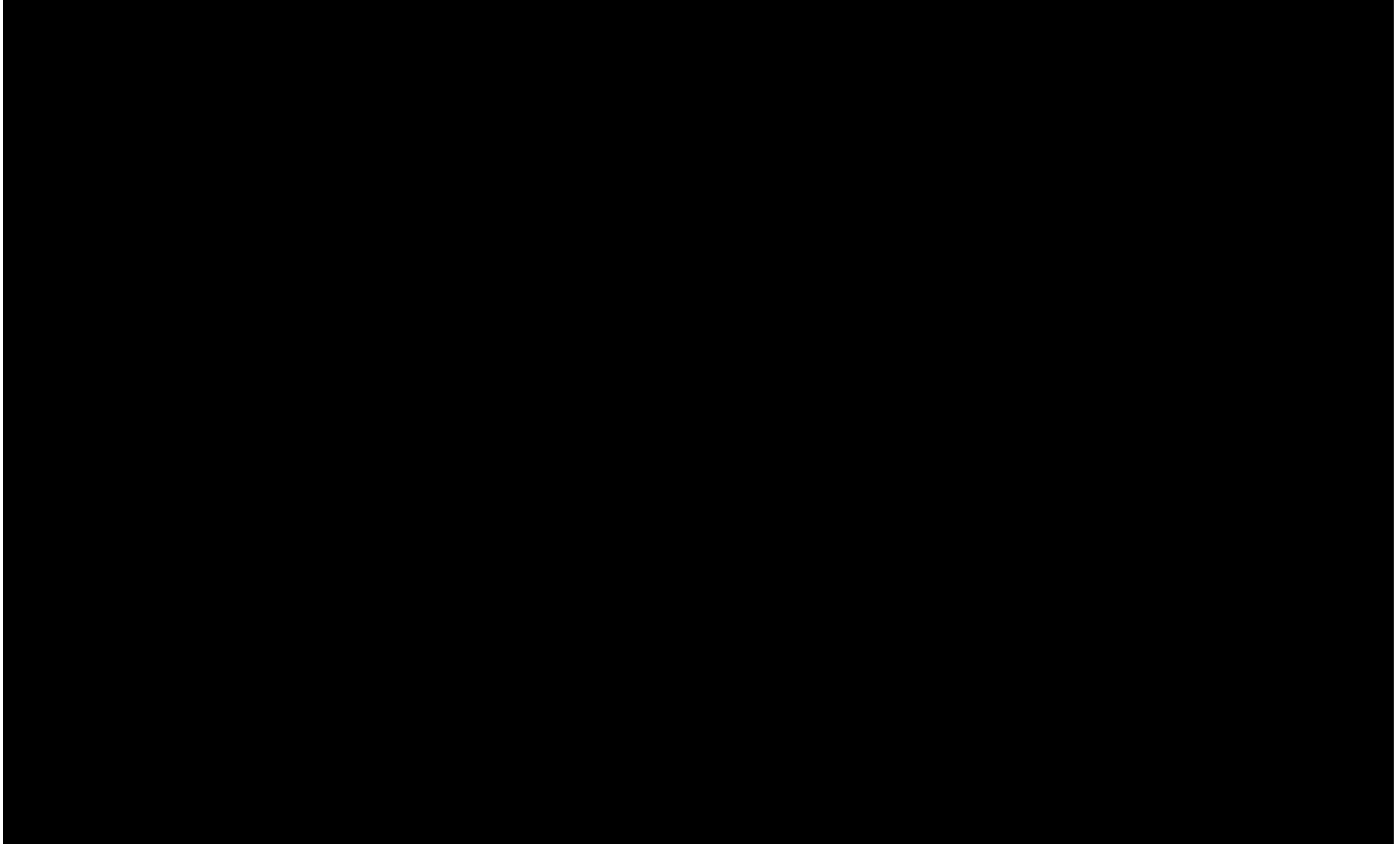
Spies look like this...



...not this



Education Or Espionage?





FBI Boston Division: Counterintelligence Awareness Briefing

Visitors: Risks & Mitigations October 2018

Briefing Conducted by:
FBI Boston Division
SA Joseph H. Altman



FBI Counterintelligence Strategy

OUR MISSION

To protect the United States by identifying, understanding, and combating foreign government activities that pose a threat to national security

↳ **Not Just Hostile Intelligence Services**

OUR STRATEGY

1. Determine what information, technology, or other assets our adversaries want to obtain
2. Prioritize which of those are most important to protect
3. Determine who has those priority items
4. Leverage the broadest set of tools and allies to protect those priority items

↳ **Emphasis On Preventing Harm**





Trends in Espionage

- ▶ Collection against the U.S. has roughly doubled since the end of the Cold War.
- ▶ **Focus of Foreign Intelligence has shifted from military secrets to critical technology and U.S. proprietary economic information.**
- ▶ Political and military allies are just as active in technology/economic collection as our traditional adversaries.



Foreign Threat

100+ Countries Targeted U.S.
Technologies



▶ **Friend and Foe**

▶ Rich and Poor

▶ Low and High Technologies

▶ Government and Private



What Do They Want?

- ▶ Proprietary formulas and processes
- ▶ Research and Development Information
- ▶ Prototypes or blueprints
- ▶ Security and Physical Plant Information
- ▶ Employee Lists/Phone Directories
- ▶ Access control information
- ▶ Software (including source codes)
- ▶ Corporate / Marketing strategies
- ▶ Customer Data
- ▶ Negotiation strategies



Common Tactics / Techniques

- ▶ Corporate Insider (access/knowledge)
- ▶ Unsolicited Correspondences & Request for Information
- ▶ Cyber
- ▶ Elicitation
- ▶ Exploitation of Joint Venture/Research Relationships
- ▶ Acquisition of Technology
- ▶ Trade Shows, Exhibits, Symposia, Conventions and Seminars
- ▶ Internet Social Networking Risks
- ▶ **Foreign Visits /Foreign Delegations**
- ▶ Foreign Acquisition of Technology and Companies
- ▶ Exploiting Overseas Travel



Exploitation of Foreign Visit

Techniques:

- **Peppering:** Visitors asking the same question in different styles or one visitor asking the same question to multiple U.S. contractor employees
- **(Primary Goal:** These techniques are specifically designed to produce potentially embarrassing incidents and appeal to your good side)
- **Wandering Visitor:** The visitor uses the distraction provided by a large delegation to slip away, out of the control of the escort
- **Divide and Conquer:** Visitors take the U.S. team members into different areas to discuss issues in order to deprive the U.S. person of his safety net of assistance in answering questions
- **Switch Visitors:** A collector added to the group without leaving enough time for a background check on the new visitor
- **Bait and Switch:** The visitors say they are coming to discuss business that is acceptable for discussion, but after they arrive their agenda switches to different questions and discussion topics
- **Distraught Visitor:** When the visitor's questions are not answered he/she acts insulted or creates an uncomfortable scene in an attempt to psychologically coerce information from the target



Exploitation of Foreign Visit

Techniques:

- Arriving at a facility unannounced
- Taking notes and photographs
- Last minute or unannounced additions to a visiting delegation
- Foreign Liaison Officer (FLO) or embassy official attempts to conceal official identity during commercial visits.
- Visitors claim business-related interest but lack experience researching and developing technology
- Visitors ask to meet personnel from their own countries and attempt to establish continuing contact with them.



Exploitation of Foreign Visit

Security Countermeasures

- Do not allow suspicious unannounced foreign visitors access to the facility. Simply tell them no one is available, and that they should schedule an appointment for another date.
- Do not allow last minute additions or substitutions to a foreign delegation to have access to the facility. Ask them to remain in the lobby while the others are permitted access. This could potentially keep an intelligence officer out of the facility and encourage proper visitation procedures.
- Verify personal identification against the original visit request when foreign visitors arrive to ensure they are who they say they are.
- Ensure there is a sufficient number of escorts to control a visiting delegation if it should be split into multiple groups.



Exploitation of Foreign Visit

Security Countermeasures

- Ensure escorts are briefed as to what is critical within the facility and that they know what requires protection from the foreign visitors
- Ensure facility employees are briefed as to the scope of the foreign visit and to not discuss anything beyond what is approved
- If a visitor becomes offended when confronted during a security incident, recognize the confrontation as a collection technique and ask the visitor to leave the facility if he or she cannot abide by the rules
- Do not permit any cameras or note taking if something in the facility is "sight sensitive"



Exploitation of Foreign Visit

Security Countermeasures

- If the delegation attempts to make additional contacts with escorts and speakers, make sure they keep discussions to the agreed-upon topics and information
- Conduct a walkthrough of the facility to ensure the visitors will not have audible or visible unauthorized access. Escorts should maintain visual contact with all visitors at all times
- If these or any other suspicious incidents occur, please ensure that they are reported immediately to your security office



Exploitation of Foreign Visit

Security Countermeasures

- Brief visitors on their obligations and responsibilities including limitations on access or use of computers, copiers, or fax machines, and access limitations to buildings or rooms
- Do not allow visitors to use networked computers; provide stand-alone computers if needed
- Conduct regular computer audits to detect any efforts by visitors or employees to exceed their approved computer access



Not Just “Spy vs. Spy” Anymore

THEN

- Intelligence officers
- People recruited by intelligence officers

NOW

- Intelligence officers
- People recruited by intelligence officers
- Hackers
- Businesspeople
- Academics
- Researchers
- Diplomats
- **Anyone else who can get their hands on something of value**



Importance of Foreign Visitor Screening

The best first step for a FIS or terrorist is physical access to you and your facility.

- Inserting a thumb drive into a computer replacing a computer cable
- Using the visit to arrange a social off-site



Your best defense is to know with whom you are dealing and whether the US Government can inform you about potential risks.



Federal Government Response

Two White House initiatives will organize U.S. government resources for better vetting of those entering the U.S. It will also put resources at your disposal to understand the identity of individuals seeking access to you and your facility:

- National Security Policy Memorandum 7
 - Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans; establishes support for the national vetting enterprise
- National Security Policy Memorandum 9
 - Establishes the National Vetting Center under DHS to coordinate the management and governance of the national vetting enterprise.



The Foreign Access Management Enterprise (FAME) is run by the DHS Chief Security Officer to help DHS and USG agencies better understand the threat posed by foreign visitors.

- FAME is a short-term resource as the larger robust capability is built



What You Can Do to Help

- **Implement comprehensive foreign visitor screening.**
 - Knowing about potential risks will help safeguard you, your personnel and your facility.
- **Contact the NRC Counterintelligence Program Manager regarding requests for access by foreign visitors.**
 - In return, you will receive notification if derogatory information was found.
 - Consider the results conjunction with other applicable requirements to determine whether an individual may be granted unescorted access
- ❖ Inform your local FBI contact regarding foreign visitor access requests.





Reporting

Remember, **YOU are the first line of defense against espionage!**

If you feel you are being solicited for information:

- Never feel obligated to answer questions that make you feel uncomfortable
- Be observant and take note of the person questioning you
- Maintain professional composure
- **REPORT, REPORT, REPORT** (ReportIt@nrc.gov)

REPORT It!

Points of Contact:

Lance English
NSIR/DSO/ILTAB
301-492-3006

Lance.English@nrc.gov

Desiree Davis
NSIR/DSO/ILTAB
301-492-3979

Desiree.Davis@nrc.gov



FBI Boston - WMD Program

Special Agent Joseph H. Altman

Weapons of Mass Destruction

FBI Boston

978-994-6047

jhaltman@fbi.gov

