Identifying Effective Practices for NSPM-33's Research Security Program Practices.

Moderator:
Kris West, Director Research Ethics & Compliance
COGR

Presenters (in order of presentation):

Clint Schmidt, Sr. Director, Research Security & Conflict of Interest,
Office for Research Protections
The Pennsylvania State University

Dan Norquist, Deputy Vice President for Research Operations, Office of Research Support and Operations
Washington State University

Elizabeth Peloso
Associate Vice Provost and Associate Vice President for Research Services
University of Pennsylvania

Allen DiPalma, Director,
Office of Trade Compliance
University of Pittsburgh

Identifying Effective Practices for NSPM-33's Research Security Program Practices.

AGENDA:

- **Foreign Travel Security**
- **Cybersecurity**
- **Research Security Training**
- **Export Controls**
- **Research Security Governance**

Foreign Travel Security

"Agencies should require that research organizations maintain international travel policies for faculty and staff traveling for organization business, teaching, conference attendance, research purposes, or any offers of sponsored travel that would put a person at risk. Such policies should include an organizational record of covered international travel by faculty and staff and, as appropriate, a disclosure and authorization requirement in advance of international travel, security briefings, assistance with electronic device security (smartphones, laptops, etc.), and preregistration requirements."

Source: NSPM-33 Implementation Guidance

Foreign Travel Security Poll #1

NPSM-33 Implementation Guidance states that agencies should require research organizations to maintain international travel policies that include, among other things, pre-registration requirements for covered international travel.

What best describes your institution's approach to this anticipated pre-registration requirement?:

A. We already require pre-registration for all international travel, so this should be easy.

B. We require pre-registration for international travel for some, but not all, international travel, and should be able to pivot to any new requirements with a few tweaks.

C. We have a pre-registration system for international travel but it is not required.

D. We don't currently require pre-registration for international travel but have started to have some conversations to prepare for this requirement.

E. We don't currently require pre-registration for international travel, and don't anticipate that we will take any action until we see the final Federal Register language.

Foreign Travel Security Poll #2

How will your institution determine where your traveler is when they're traveling internationally?

A. Tracked internally in electronic Human Resource System

B. Tracked in third-party Travel Registration System e.g., International SOS MyTrips, etc.

C. Paper based tracking

D. We don't have a plan for this yet.

E. Other (Please feel free to mention what your institution is doing in the Chat. Include the Poll # in your answer.)

Foreign Travel Security Poll #3

Is your institution using travel.state.gov as a resource for foreign travel security?

A. Yes

B. No

C. I don’t know

D. Other (Please feel free to mention what your institution is doing in the Chat. Include the Poll # in your answer.)

Foreign Travel Security Poll #4

Does your institution have a travel laptop loaner program?

A. Yes, a voluntary loaner program

B. Yes, a mandatory loaner program for some foreign travel

C. Some units/departments have loaner programs

D. None at this time

Foreign Travel Security Poll #5

How does your institution track electronic devices (smart phones, laptops) being used for research when traveling internationally?

A. Tracked internally in electronic HRS or other system

B. Paper based tracking

C. We don’t have a plan for this

D. Other (Please feel free to mention what your institution is doing in the Chat. Include the Poll # in your answer.)

Foreign Travel Security

Laptop loaner programs

- **Mandatory vs. optional for travel to certain countries?**
- **Cost associated with maintaining devices, management of program**

Travel registration systems and procedures

- **Third-party software available**
- **Enforcement/Compliance – reimbursement as the “carrot or stick”**
- **Opportunity to educate on risks**

Leverage or expand existing processes

Utilize federal resources in support of advisories and briefings

COGR

Cybersecurity Requirements

- The origin of the NSPM-33 Cybersecurity Requirements*
- Purpose
- We are NOT talking about…
- We ARE talking about…
- Caveats
- What did NSPM add that is not in FAR 52.204-21:
  - Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches.
  - Provide protection of scientific data from ransomware and other data integrity attack mechanisms.
- What did NSPM NOT include from FAR 52.204-21 (b)(1)(vii, viii, and xi)

Cybersecurity Poll #1

As part of future research security programs, agencies will require schools to satisfy cybersecurity requirements for their IT networks and research data. The NSPM-33 implementation guidance lists 14 basic safeguarding protocols and procedures.

Assuming your institution has generally reviewed this list, how do you assess your institution's readiness to address this requirement?

A. We primarily have a decentralized IT network, and we believe it will take substantial effort before we can comply with these requirements.
B. We primarily have a decentralized IT network, but we'll be able to comply with these requirements with minimal or moderate effort.
C. We primarily have a centralized IT network, and we believe it will take substantial effort before we can comply with these requirements.
D. We primarily have a centralized IT network, but we'll be able to comply with these requirements with minimal or moderate effort.

Cybersecurity Poll #2

Who at your institution is responsible to implement cyber security policies?

A. Unit

B. College

C. Central IT

D. Other (Please feel free to mention what your institution is doing in the Chat. Include the Poll # in your answer.)

Cybersecurity Poll #3

How will your institution manage insider threat awareness?

A. Developing a relationship with FBI

B. CITI or other trainings

C. Utilizing 3rd party software

D. Other (Please feel free to mention what your institution is doing in the Chat. Include the Poll # in your answer.)

Cybersecurity Poll #4

The NSPM-33 had many objectives around cybersecurity safeguarding protocols and procedures. How do you feel your institution is meeting these objectives?

A. We're ready.

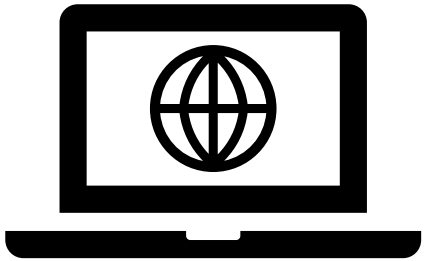
B. We have a plan, but it is not implemented.

C. We have just started implementing our plan.

D. We don't have a plan yet.

Cybersecurity Requirement Best Practices and Challenges

- Now what?
  - Don’t panic
  - Clear communication
  - Find an IT champion
  - Be perseverant
  - Analyze your risk
- Yes, there are worries
  - Highly decentralized
  - The asterisk*



Research Security Training

Agencies should require that, as part of their research security programs, research organizations provide training to relevant personnel on research security threat awareness and identification, including insider threat training where applicable. Research organizations should consider incorporating relevant elements of research security into existing training on responsible and ethical conduct of research for faculty and students. In addition to periodic training, research organizations should conduct tailored training in the event of a research security incident.

Source: NSTC/JCORE NSPM-33 Implementation Guidance

Research Security Training Poll #1

Research Security Training will be a required element of future research security programs.

What steps has your institution taken in anticipation of this pending requirement?

A. We currently require certain research staff to take research security training before they are permitted to participate in a sponsored research project.
B. We currently offer research security training for research staff but do not require them to take it before participating in a sponsored research project.
C. We don't offer specific research security training for research staff because we feel that other available training already covers this topic well.
D. We are waiting for the "Official" research security training to be released before we do implement training requirements.

Research Security Training Poll #2

Does your institution currently have any kind of research security training?

A. Yes, for a specific population of researchers, e.g., those who conduct classified or controlled unclassified information (CUI) research.

B. Yes, for all researchers on sponsored awards.

C. Yes, but it is not mandatory.

D. No, not currently.

Research Security Training Poll #3

If you are offering training, is the training:

A. Commercially developed

B. Developed internally by your institution

C. A combination of both commercially developed and institutionally developed training

Research Security Training Poll #4

If you are offering research security training, does it include insider risk training?

A. Yes

B. No

Research Security Training Poll #5

When new training requirements go into effect, will your institution apply them to only those individuals who work on sponsored awards, or to a broader audience?

A. We will apply them only to those individuals required to take training.

B. We will apply them to anyone involved in research.

C. We will apply them to a broad range of employees, beyond just the research community.

D. We have not yet decided.

Research Security Training Poll #6

How does your institution plan to provide research security training?

A. Face-to-face instruction

B. Online trainings e.g. CITI

C. Hybrid Offering

D. Other (Please feel free to mention what your institution is doing in the Chat. Include the Poll # in your answer.)

Research Security Training Poll #7

If Online training will be used, what training is your Institution considering?

A. Online trainings e.g. CITI

B. NSF Provided Training Modules

C. Institution Developed Training Modules

D. All of the above

E. Other (Please feel free to mention what your institution is doing in the Chat.)

Research Security Training

- CHIPS seems to indicate an annual training requirement, though NSF has not clarified

- 4 Training modules have been funded:
  - Importance of Research Security
  - Importance of Disclosures
  - Risk Management and Mitigation
  - International Collaborations

- Mandatory or optional use of the NSF funded modules?
- Integration into existing RCR training?
- Who are relevant personnel?

Export Controls Training, As Appropriate

"Agencies should require that research organizations conducting R&D that is subject to export control restrictions provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and for ensuring compliance with Federal export control requirements and restricted entities lists."

Source: NSTC/JCORE NSPM-33 Implementation Guidance

Export Controls Poll Question #1

Export Controls training is anticipated to be a requirement of any new research security program, but only as appropriate.

How does your institution primarily deliver export controls training?

A. We broadly offer in-person and/or online export controls training to all faculty and staff, but it is not mandatory.

B. We broadly offer in-person and/or online export controls training to all faculty and staff but only require it for those participating in restricted research or situations that require a technology control plan.

C. We require export controls training for all researchers regardless of their research type.

D. We don't have a good handle on export controls yet and don't know how we will satisfy this requirement.

Export Controls Poll #2

How does your institution deliver export control training?

A. Face-to-face instruction

B. Online trainings e.g. CITI Hybrid

C. Other (Please feel free to mention what your institution is doing in the Chat.)

Export Controls Poll #3

Is such export control training a change from current offerings?

A. No. We have already have export control training.

B. Yes. We are modifying our export control training.

C. Yes. We are adding export control training.

Export Controls Training, As Appropriate

What (Scope):	**R&D subject to export control restrictions: 1. Non-fundamental research; 2. Other export-controlled inputs.**
Who:	**Relevant personnel: 1. Direct participants in Non-fundamental research; 2. Individuals receiving/using export-controlled inputs.**
Processes/Offices:	**Sponsored Programs, Visas, Visitor Vetting, Purchasing, Shipping/Receiving, Tech Transfer, International (travel).**
How (Management):	**Targeted Training Through: 1. Technology Control Plans; 2. Restricted Party Screening Program.**
Compliance:	**Export Controls Office through a written export controls management plan.**

COGR

Research Security Governance

- "Qualifying research organizations should be those that met the $50 million threshold in total Federal science and engineering support for the previous two fiscal years, as recorded on USASpending.gov."
- "Agencies should require that, as part of their research security program, research organizations designate a research security point of contact (POC)…"
- "…and provide publicly accessible means to contact that individual (such as through a website or social media)."
- "Organizations conducting research involving classified or controlled unclassified information (CUI) may combine research security POCs…"
- "Some research organizations may choose to integrate research security requirements into existing programs—such as existing cybersecurity programs and responsible and ethical conduct in research training—to maximize efficiency."

Research Security Governance Poll #1

Will your institution created an advisory board, governance board, committee or other group to review research security matters, advise on regulatory interpretation, policies, and procedures and provide expertise to develop a Research Security Program?

A. Yes. We already have such a committee.

B. Yes. We plan to create a new committee after final guidance is released.

C. Maybe. We are still working on it.

D. No.

E. I don't know.

Research Security Governance Poll #2

Has your institution decided who should be your Research Security Point of Contact?

A. Yes, it is an existing team member

B. Yes, we have created a new position

C. No, we are still working on this

D. I don’t know

Research Security Governance Poll #3

At your institution, what offices/units are primarily involved in implementing the research security requirements? (Select all that are applicable.)

A. Office of Sponsored Programs
B. Compliance Offices (Export/COI)
C. Office of the General Counsel
D. Office of Research Administration
E. School Offices
F. Departmental Offices
G. Global Support Offices
H. IT Offices
I. Risk Management/Internal Audit
J. Technology Transfer

Research Security Governance Poll #4

How prepared are you to govern your Research Security Program (RSP)?

A. We're ready.

B. We have a plan and draft RSP, but it is not implemented.

C. We have just started implanting our RSP plan.

D. We don't have a plan.

Research Security Governance

How are our panelists' institutions handling governance of research security processes?