RED
Research Education Development

Symposium for Research Administrators

University of Wisconsin-Madison
November 8th, 2023

Research Security Program: NSPM-33

John Jay Miller

Interim Director Research Security Program, Research Policy and Integrity

Jennifer Rodis

Policy & Planning Analyst, Research and Sponsored Programs

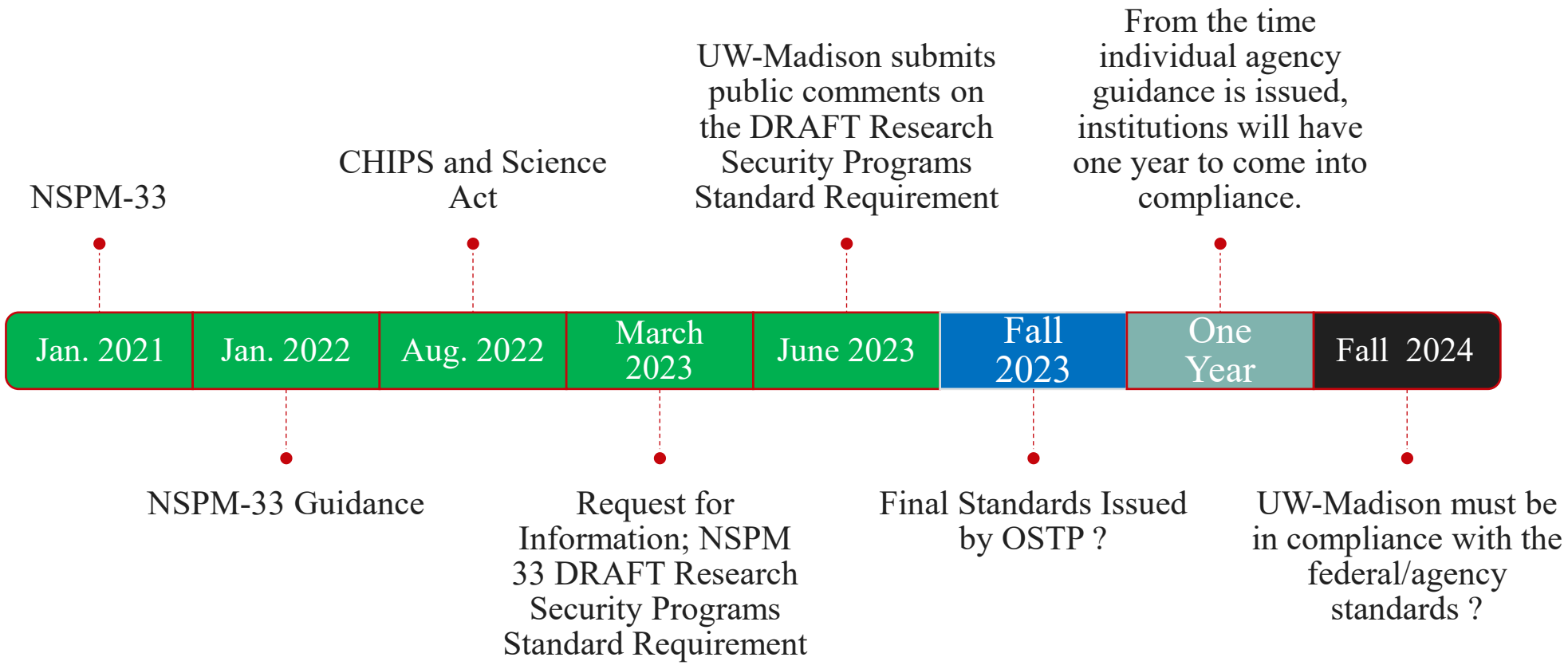
Overview of National Security Presidential Memorandum-33

The White House Office of Science and Technology Policy (OSTP) released guidance to federal agencies for implementing National Security Presidential Memorandum 33 (NSPM-33).

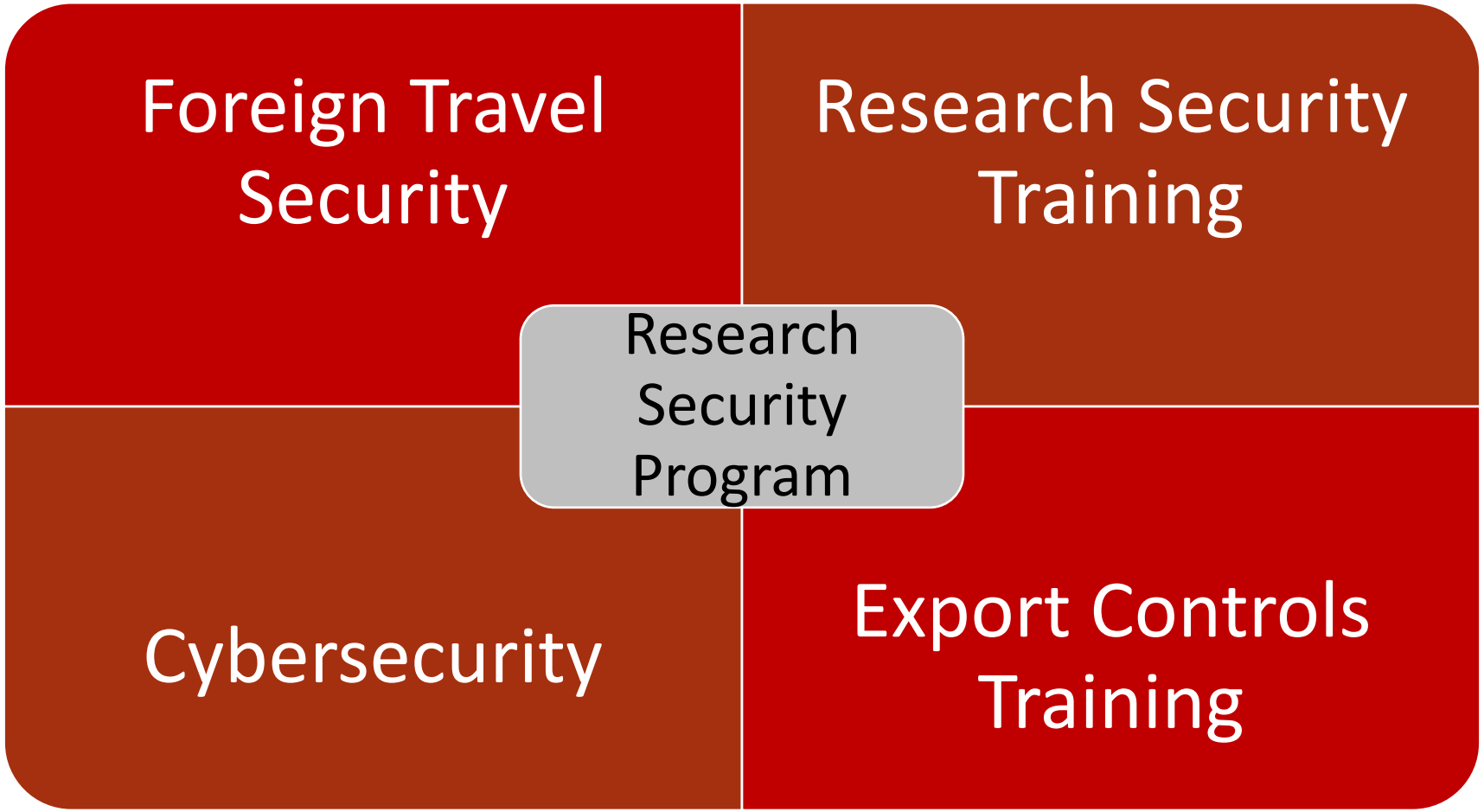
The guidance focuses on five key areas:

1. Disclosure requirements and standardization
2. Digital Persistent Identifiers
3. Consequences for violation of disclosure requirements
4. Information sharing
5. Research security programs

Research Security Program Timeline



Research Security Programs



Who Will It Impact

Directly:

- "Covered individuals"
  - An individual who contributes to the scientific development or execution of a federal research and development project; and
  - Is designated as a covered individual by the Federal research agency concerned (PIs and other senior/key personnel) seeking or receiving Federal research and development funding

Indirectly:

- Research Administrators
- IT staff (central/departmental)
- Supervisors
- Business Services (travel)
- International collaborations, etc.
- Human Resources

Research Security Program Implementation

1. Assessing where we are at and identifying areas that may need additional work.
2. Develop critical paths to implementation
3. Assign teams to complete (and allocate resources as needed)
4. Start to norm “future state”

Current Status of the DRAFT Research Security Programs Standard Requirement

1. Waiting for OSTP to release the final standards

2. Yet with so much to prepare for, we want to consider…

    - What should we act on now?

    - Where should we hold off on firm commitments?

3. The implementation review will help answer these questions

Overarching Program Standards

1. Institutional self-certification in Sam.gov on an annual basis
2. Must provide documentation of the maintained research security program within 30 days of a request from a research agency funding the award.
3. Should conduct regular self-assessments
4. Should manage the required elements as an integrated program
5. Must maintain clear response procedures to address reported allegations of research security non-compliance
6. Report incidents of research security violations to the federal awarding agency or agencies
7. The importance of non-discrimination as a guiding principle of U.S. research security policy

Foreign Travel Security

1. Must establish or maintain an international travel policy applicable to those on federal R&D projects & the policy must include:
    - Pre-authorized international travel for covered individuals
    - Mandatory security briefings, including information on device safety/security (including loaner devices)
    - Maintain an organizational record of travel
2. We have multiple travel policies that will need to be reviewed once the standards are finalized

Research Security Training

- Nine required elements of the training program
  - Must be kept up to date
- Training for all personnel
  - As appropriate for each faculty, staff, & students
  - Reference to responsible and ethical conduct of research (RECR)
  - Expectation the training is ongoing (no defined cadence)
- Maintenance of training records
- Specialized training following any research security breaches
  - Breach is not defined

Cybersecurity

1. 12 Protocols: we won't list them in detail because none of us are cybersecurity experts, but here are key issues

    1. No specific standards or reference to existing standards, such as NIST 800-53

    2. Ambiguity increases difficulty of consistent implementation & assessment of the program's adherence

    3. Could lead to gaps in practice across institutions

Export Control Training

1. Must provide training to relevant personnel on requirements and processes for:
   - Reviewing foreign sponsors, collaborators and partnerships
   - Ensuring compliance with Federal export control requirement, and
   - Restricted entities lists

2. The training must emphasize that the “fundamental research” exception has explicit limitations. For example, federally funded R&D of “applied” energy technologies (i.e., “applied research”), fall outside of any exception and are subject to export control laws.

Definitions: Examples That May Change Current Practice

1. New or changed definitions have the potential to change implementations further
2. **Conflict of Interest**: COI defined to include "funding" of research, which is a new facet of COI
3. **Covered International Travel**: this is a very broad scope with potential for large admin & financial burden
4. **Research Security Breach/Violation vs. Security Incident**: only incident is defined in the appendix but we must act on a Research Security Breach (and Violation) which is not defined

Practical: Training

1. Training is an emphasis
   - The National Science Foundation issued four grants to create training modules for the four areas
     - Modules are being developed
2. Integrating the training across the university is also an emphasis
3. We currently have training in all the necessary areas
4. Once modules are complete, we will review to determine how to implement

Practical: Policies

1. OSTP requires UW to have policies to direct our compliance
2. We currently have policies that address these federal requirements
3. And we will need to update, amend, and create new policies once the standards are finalized

Response to the Draft Research Security Standards

- Research Security Team established by OVCRGE to respond to draft standards. The Team is comprised of representees from the following areas: Office of Legal Affairs, Research and Sponsored Programs, International Division, Export Controls, Cybersecurity, Conflict of Interest, Research Compliance and Risk Management.
- Established a Research Security Program Website
- Established a Point of Contact
- UW has commented on the draft standards and other research security changes by federal agencies
- Coordinating implementation with the four identified areas and others
- Discussing ways to integrate training
- Following timeline of government's proposed implementation plan

Research Security Program Contact Information

Questions about the Research Security Program can be directed to:

John Jay Miller
Interim Director of the Research Security Program
john.miller@wisc.edu.
608-265-5122

Mark Rickenbach
Interim Associate Vice Chancellor for Research Policy and Integrity
mark.rickenbach@wisc.edu
608-890-0225