Association and Institutional Perspectives on the NSPM-33 Draft Research Security Program Standard Requirements

May 25, 2023
Co-chairs

Doug Backman, University of Central Florida
Lisa Nichols, University of Michigan
Sarah Stalker-Lehoux, National Science Foundation
Mark Sweet, University of Wisconsin-Madison
Panelists

Kris West, Director Research Ethics and Compliance Committee, Council on Governmental Relations

Laura Raderman, Policy and Compliance Coordinator for Information Security at Carnegie Mellon University representing the Educause NSPM-33 Working Group

Lindsey Spangler, Associate Dean, Research Integrity, Duke University;

Amanda Humphrey, Chief Research Operations Officer, Northeastern University
OSTP Proposed Research Security Program Standards

Kris West
Director, Research Ethics & Compliance, COGR
kwest@cogr.edu
OSTP Proposed Research Security Program Standards

• Draft standards
• 88 Fed. Reg. 14187

Comments due June 5, 2023.
The Path to the Standards

Jan. 2021
- NSPM-33
- Requires research security programs for institution with >$50M annual science & engineering

Jan. 2022
- NSPM-33 Implementation Guidance
- Identifies program elements: cybersecurity, foreign travel security, research security training, export control training
  - Identifies cybersecurity elements

Aug. 2022
- CHIPS & Science Act of 2022
- Research security training requirements and certification
  - Training guidelines and training modules
How are COGR & Other Associations Responding?

- Optimizing 5-page limit on comments
  - Cross-reliance on fellow associations’ comments
  - Reliance on associations with particular subject matter expertise
- Gathering input from members
- **Joint association request to OSTP to hold listening sessions** for stakeholders on the proposed standards
- **Draft talking points** that institutions may use in their own responses
Institutional Concerns
Topics for Framing Responses

- Equity
- Clarity
- Feasibility
- Burden
- Compliance
Standards should be Risk-Based

• NSPM-33 Implementation Guidance – “Tangible benefit should result from and justify any accompanying cost/burden”
  HOWEVER, draft standards are not risked based
• One size does not fit all
• Examples
  Foreign travel standards
  Cybersecurity
Standards Should be Consistent Across Agencies

• Ensure that there is one set of standards to which institutions must certify.
• Multiple, different agency standards will complicate and confound processes, training, and compliance.
• OSTP should identify specific circumstances in which agencies may include additional, more rigorous requirements in solicitations.
Standards Should be Clear

- Definitions – Define terms in appendix and use those defined terms consistently in Standards.
  
  Example: Multiple terms for reportable events.

- Financial Trigger for Applicability – Use one source (USAspending.gov) as authority for determining what institutions are required to establish a research security program.
  
  OSTP should provide notice to institutions who they determine meet financial trigger.

- Effective Date – Clarify whether one year compliance period runs from date OSTP publishes standards, or each agency publishes its standards.
Standards Should Afford Flexibility to Institutions

• NSPM-33 Implementation Guidance states “Research organizations should be provided flexibility to structure the organization’s research security program to best serve its particular needs, and to leverage existing programs and activities where relevant.”

• Risk-Based: Institutions should have flexibility to consider context in which standards will be implemented. Examples: Cybersecurity standards, foreign travel standards
Specific Provisions of Concern

- **Travel**
  NSPM-33 Implementation Requirements – travel requirements “as appropriate” but proposed standard is MUCH broader.
  Institutional flexibility to determine disclosure and authorization necessity and criteria
  Clarify who and what is covered

- **Cybersecurity**
  Standards need risk-based context!

- **Export Controls**
  Edit the example

- **Training**
  Clarity is needed regarding nexus with RECR training, training schedule
  How will the upcoming training modules fit in?
  Alignment with Chips & Science Act
Big Picture Concerns

• Equal standards isn’t the same as equitable standards
  Emerging research institutions
  “Low” risk and fully transparent research

• When is international collaboration OK?
  Lack of positive models
  Is collaboration with China OK?

• And then there’s the cost! Are we splitting the tab equally?
NSPM-33 Cybersecurity Protocols
• **Stated focus is preventing ransomware and other data integrity attacks**
  The proposed protocols are specific to confidentiality, while some can also protect integrity, there are additional protocols that cybersecurity experts would recommend for integrity.

• **No background information on how to assess whether an organization meets these requirements**
  Based on FARS Basic Safeguarding Clause (54.204-21) for Federal Contract Information

• **Out of date, technology specific requirements**
  Periodic scans

• **Risk-based approaches are not considered**
Challenges

• **Interpretation**
  Someone who is not familiar with CMMC level 1, NIST SP 800-171A will interpret the requirements differently than someone who is.
  - One link to the general NIST cybersecurity page is included

• **Costs to implement unrelated OMB M-21-31**
  Audit logs are only tangentially related to limiting system access. Audit log management (retention, review, etc) are resource intensive

• **Personally owned devices**
  Very common for students to use personally owned (and managed) devices for research

• **Scope of “publicly accessible”**
  Research project home pages? Entire set of University web pages? Faculty web pages?
Recommendations

• OSTP should replace the specific protocols with a directive for a risk assessment/risk management approach focusing on identifying objectives rather than specific measures

• If the protocols remain, they need to be updated to explicitly state:
  Institutions will have to flesh out implementation details and metrics
  Institutions will have the discretion to adopt alternative measures where appropriate and with documentation and justification
Limit information system access to authorized users and processes acting on behalf of authorized users, or devices.

Interpretation 1: Everyone must log on to the system

Interpretation 2 (from 800-171A 3.1.1):

<table>
<thead>
<tr>
<th>3.1.1</th>
<th>SECURITY REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.1.1</th>
<th>ASSESSMENT OBJECTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1[a]</td>
<td>authorized users are identified.</td>
</tr>
<tr>
<td>3.1.1[b]</td>
<td>processes acting on behalf of authorized users are identified.</td>
</tr>
<tr>
<td>3.1.1[c]</td>
<td>devices (and other systems) authorized to connect to the system are identified.</td>
</tr>
<tr>
<td>3.1.1[d]</td>
<td>system access is limited to authorized users.</td>
</tr>
<tr>
<td>3.1.1[e]</td>
<td>system access is limited to processes acting on behalf of authorized users.</td>
</tr>
<tr>
<td>3.1.1[f]</td>
<td>system access is limited to authorized devices (including other systems).</td>
</tr>
</tbody>
</table>
Northeastern University Overview
Institutional Profile

- **Established**: 1898
- **Type**: Private Graduate & Undergraduate
- **Location**: Boston, MA and 12 regional/global campuses
- **Of note**: cleared facility
NSPM-33: NU Current State

- Export control training: 100% completed
- Research security training: 60% completed, 40% in progress
- Cybersecurity: 80% completed, 20% in progress
- Foreign travel security: 90% completed, 10% in progress
In rolling out NSPM-33 timing is also a challenge:

- **Clarity/urgency**: rules are not finalized yet but to get it done in time, we have to start to plan for implementation
  - Ex. difficult to gauge what we will need to supplement from the NSF modules
- **Community engagement**: since the requirements are not finalized, challenge of how much to communicate to each audience & to convey guidance that will be durable (don’t want to have to re-train)
- **Resources**: staffing to meet demands of global campus network, as well as costs of software, etc.
Duke University Overview
Institutional Profile

- **Established**: 1924
- **Type**: Private Graduate & Undergraduate
- **Location**: Durham, NC
- **Research Portfolio Size**: FY’22: $902M (fed), $1.39B (total)
- **University/Health System**: Multiple stakeholder groups exist in two places—Health System (SOM/SON) and the University (all other schools)
Future Potential Challenges

- **Clarity:** The lack of clarity/consistency in some of the definitions, especially with who is required to complete an activity, makes it difficult to fully scope and plan.

- **Maintaining engagement:** making sure relevant stakeholders in central offices are engaged and willing/able to change existing processes to meet requirements.

- **Minimizing burden:** with newer disclosure requirements, data management and sharing policy, RCR/RECR-- introducing new initiatives to both faculty and administrators can be difficult and overwhelming.

- **Resourcing:** there’s never enough time, money, or people.
Quick Pulse Survey: Current State
Survey sent last week

- Anonymous
- 8 questions
- 24 respondents
- Average of 21 respondents per question – small sample

**Goal:** gauge readiness across the membership
2: Is your institution struggling with any of the cybersecurity requirements? (4 responses)

- Audit
- Training
- Understanding the requirements
- Confirming the standards mean what the institution thinks they mean
Current Institutional Practices: International Travel & Laptops

Does your institution provide loaner laptops for international travel?

- Yes – we have a robust central program for loaner laptops specifically for international travel.
- Yes – we have a central program for loaner laptops but it is not specific to or used extensively for international travel. We wouldn’t have the capacity for extensive use.
- Somewhat – some colleges and schools within the institution provide loaner laptops for international travel.
- No – we do not have a central program for loaner laptops specifically for international travel and few if any programs at colleges and schools.
- I’m not sure
- Other

We have a program, but faculty are not aware
Current Institutional Practices: Travel Registration

Other:
- Only for students
- Only if institutional funds
- Process in place, but it is not regularly followed
Current Institutional Practices: Travel Authorization

Other:
- Authorization only to high-risk destinations or individuals holding security clearances
- Travel is supposed to be approved but the policy is not well known/enforced
- Question about what is meant by authorization, passive or active sign-off
Current Institutional Practices: Scope of Authorization

What travel (not involving students/a student trip) does your institution require faculty disclosure and/or authorization for (SELECT ALL THAT APPLY): 20

- Any travel paid for by the institution
- Travel to high-risk locations
- Any international travel associated with university business regardless of sponsor/reimbursement
- I'm not sure
- Other
Current International Practices: Security Briefings

Does your institution currently provide security briefings and advice regarding electronic device security prior to international travel?

- Yes – we provide security briefings and advice for all international travel [20]
- Somewhat - if requested or if to a comprehensively sanctioned country or an individual with security clearance
- No – personal briefings are not generally provided, however, we have many resources available on our website and sometimes provide workshops or webinars
- No – personal briefings are not generally provided and we currently have few resources available
- I’m not sure
- Other
Current Institutional Practices: Training Modules

Is your institution waiting for the federally funded research security training modules before implementing any form of new research security training? (21)

- Yes – grateful that this is being taken care of
- No – we want to incorporate this into other existing training or develop our own modules
- No – we want to use training currently available by other providers
- No – we are concerned that we will be out of compliance if we wait
- I’m not sure
- Other
Quick Pulse Survey

Key Takeaways

- A lot of variability across the participating institutions
- Most institutions that responded do not currently fully meet the cybersecurity requirements – the decentralized nature of universities and use of personal laptops are considerations
- Many institutions had some form of loaner laptop program but most do not have a robust central program targeted to international travel
- Institutions were more apt to require travel registration/disclosure, but not authorization
- Institutions responding generally don’t provide travel briefings or only for high-risk travel
- Most are waiting for the federal training modules, but a few are forging ahead
Questions?