RED
Research Education Development

Symposium for Research Administrators

University of Wisconsin-Madison
October 25th, 2022

Research Security

Mark Sweet, RSP
Patti Havlicek, DoIT Cybersecurity
Tom Demke, Export Controls
Jennifer Rodis, RSP

Overview

- Introductions
- “Research Security” - what is it?
- NSPM-33
- UW – Madison current state
- Important points for research administrators
- Panel discussion and Q&A

Research Security: What is it?

Research Security

Ensuring the openness, transparency, and integrity of the U.S. research enterprise and protecting innovations and intellectual property funded by the U.S. federal government.

Research Security

- Shift in language and scope from “Foreign Influence”
- Focus of the federal government
- Encompasses many facets from awareness to disclosure
- Important federal legislation/regulations:
  - National Defense Authorization Act (NDAA)
  - National Security Presidential Memorandum 33 (NSPM-33)
  - Higher Education Action – Section 117
  - CHIPS and Science Act

NSPM – 33

National Security Presidential Memorandum -33

- NSPM – 33
- Issued January 14, 2021
- Result of work over several years by the Office of Science & Technology Policy (OSTP) and the National Science and Technology Council (NSTC)
- Directs federal agencies to develop plans to strengthen the protections of federally sponsored research and development

NSPM-33 Implementation Guidance

- Issued January 2022
- Most of the Guidance are directives to the federal agencies
- Includes some very specific directives

NSPM – 33 Components

- Acknowledgment that U.S. science and engineering attracts the best talent from around the world
- Recognition that some foreign governments seek to exploit the openness of the U.S. research enterprise
- Some federal policies have contributed to a diminution of the ability to attract global talent and specifically fuel xenophobia, especially towards Asian Americans
- Clear statements that research security policies and practice must not fuel xenophobia or prejudice
- Acknowledgement that federal polices have not been clear enough to protect research security while maintaining our core ideals

NSPM-33 General Guidance

- Agencies continue to support openness and transparency
- Agencies should coordinate and work with the National Science and Technology Council and in line with existing laws and regulations
- Standardize to reduce administrative burden and engage with research community
- Agencies should utilize a risk-based approach
- Avoid retroactive application of policies which may unnecessarily harm researchers

NSPM-33 General Guidance

- Requirement of NSPM-33:

Agencies must implement NSPM-33 provisions and related requirements in a nondiscriminatory manner that does not stigmatize or treat unfairly members of the research community, including members of ethnic or racial minority groups.

NSPM-33 Guidance Components

- Disclosure Requirements and Standardization
- Digital Persistent Identifiers
- Consequences for Violation of Disclosure Requirements
- Information Sharing
- Research Security Programs

Disclosure Requirements and Standardization

- Provide clarity and standardization across agencies to achieve uniformity
- Standardization of disclosure forms and formats: Federal Register Notice – UW-Madison will be commenting
- Limiting to covered individuals as defined in Section 223 of 2021 NDAA
- Clarification of what must be disclosed
- Requirements for disclosing participation in foreign programs and foreign contracts to research agencies
- Process(es) for individuals to correct inaccurate or incomplete submissions

Digital Persistent Identifiers (DPIs)

- A way to unambiguously identify a person or digital object
- ORCiD is the main DPI
- Federal agencies are beginning to ask for ORCiD
- Publishers are often requiring it

Digital Persistent Identifiers (DPIs)

- Incorporation of DPIs into grant disclosure processes:
  - Agencies should allow submission of required disclosure information via a DPI service
- NIH and NSF are recommending use of ORCiD
- Work with investigators to obtain an ORCiD

Consequences for Violations of Disclosure Requirements

- Points out a number of existing regulations which can be utilized for violations
- Consideration when determining the appropriate action/consequences:
  - Harm to agency, federal government, taxpayers, national security
  - Intent, pattern of violation vs. isolated incident
  - Knowledge of requirements, policies, procedures, training available to offender
- Encouragement to correct past omissions

Information Sharing

- Provide clarity regarding circumstances for agencies to share information about disclosure violations
- Violations may be shared with law enforcement agencies or SAM.gov

Research Security Program

- Requirement of entities receiving $50M+ in federal R&D funds the previous two years (UW – Madison is in this group ☺)
- Describes the elements of the Research Security Program:
  - Point of Contact (similar to Responsible Official)
  - Cybersecurity protocols and awareness training
  - Foreign Travel Security
  - Research Security Training program
  - Export Control Training
  - Certification

UW – Madison Current State

UW – Madison Current State

- White paper presented to the OVCRGE in June
- RSP, OLA, Export Controls, Cybersecurity, Risk Management, RCR, International Division contributed
- Assessment of current state and recommendations for meeting Research Security Program
- Waiting for additional clarification from federal government in many areas

UW – Madison Current State

- **Point of Contact**: need to take action; awaiting clarification from feds on type of position
- **Cybersecurity**: good place with policies; distributed IT is a challenge
- **Foreign Travel Security**: may need some policy changes
- **Research Security Training Program**: waiting additional clarification from feds on what requirements are
- **Export Controls Training**: a program is in place; some enhancements likely
- **Certification**: need clarity from feds how and who certifies

Disclosures

- Major component of research security
- Current agencies are closely scrutinizing information in Biosketches and Other/Current & Pending Support
- Agencies are questioning discrepancies between these documents and information in other sources (i.e., publication data)

Cybersecurity

Common DFARS Clauses

As contracts received from the Department of Defense, it is common to see several specific Security DFARS Clauses.

Our goal today is to make you aware of these clauses, clarify their requirements and review if UW-Madison can be compliant.

252.204-7008
Compliance with Safeguarding Covered Defense Information Controls

What is required?

The research project will implement security requirements as outlined by NIST (National Institute of Standards and Technology) – specifically the 800-171 control set.

Are we compliant?

YES! UW-Madison has had a risk management program since 2015 which is based on this control set.

252.204-7012
Safeguarding Covered Defense Information and Cyber Incident Reporting

What is required?

1) UW-Madison will provide adequate security on all systems being utilized to review, process, store or transmit DoD data based on NIST 800-171 standards
2) If an incident with a UW-Madison system is discovered, UW-Madison must conduct a review for evidence of the compromise and report the incident to the DoD at https://dibnet.dod.mil.
3) UW-Madison will have a medium assurance certificate to allow reporting to the DOD.

Are we compliant?

YES, YES and YES! Our Incident Response program summary: https://it.wisc.edu/about/division-of-information-technology/enterprise-information-security-services/office-of-cybersecurity/reporting-an-incident-to-it-security/.

252.204-7019
Notice of NISTSP 800-171 DoD Assessment Requirements
(NEW CMMC REQUIREMENT)

What is required?

Everything listed in DFARS Clause 252.204-7008 PLUS a current network assessment for the specific network that will be used to hold, manipulate or share DOD data.

Are we compliant?

We can be if the IT support team, researcher and Cybersecurity respond to a 110 question assessment control set and report the self assessment score and a plan for eliminating vulnerabilities to the DoD via their system SPRS (Supplier Performance Risk System).

252.204-7020
NIST SP 800-171 DoD Assessment Requirements
(NEW CMMC REQUIREMENT)

What is required?

The DoD will require the completion of a paid, third-party risk review of the systems utilized by UW-Madison to support the use of the DoD data. This clause makes the personnel, funding, and time available for this activity.

Are we compliant?

At this time, UW-Madison has been completing Basic Self-Assessments on an as needed basis for DoD contracts with these clauses. There has not been a mandate for a paid third-party assessor to be used for validation of CMMC participation. It needs to be determined by the unit receiving the data and the supporting staff if this is an activity that would be funded for the purposes of utilization of the data.

Export Control Updates

Export Control Updates

- UW-4020, Policy on Interactions with Restricted Parties
  - Because of security and economic concerns, persons and organizations are being added to the federal gov't's restricted party lists on a frequent basis
  - UW-4020
    - Describes what interactions are allowable
    - How we address such interactions if pursued by faculty, staff or students
  - Some situations may not be allowable, others may require a license, end use statement, TCP or completion of an internal attestation form

Export Control Updates

- International Shipping and Travel Reminder
  - Contact the ExCO prior to shipping or traveling internationally
    - To determine if there are any export control concerns
  - Hand-carrying internationally = export
    - Applies to equipment, materials, technology, data or software
  - International travel included as part of the Foreign Travel Security portion of the Research Security Program

Export Control Updates

- RAMP Update
  - Started the requirements setting process Oct 3
  - Main goal is to replace/update the current ExC functionality in WISPER into Huron
    - Secondarily add common ExC forms to Huron, such as MTA and full project assessment forms
  - The two ExC questions (in project tab) have been moved to the compliance questions
    - So they will answered for all proposals and reviewed if the proposal is awarded
    - Removed old compliance question 8 regarding projects in science, engineering and tech
  - Plan to include some RAs around campus to help in the testing

Important Points for Research Administrators

Important Points for Research Administrators

- Concerns about foreign interference and research security are not tied to a specific administration and are not going away
- Have an awareness of cases, data, and potential consequences released by federal agencies. The problems that have been uncovered include:
  - Undisclosed sources of foreign research support
  - Undisclosed conflicts of interest
  - Conflicts of commitment
  - Violations of peer review integrity rules
- See Further Reading slides

Important Points for Research Administrators

- Be familiar with campus resources and guidance
- Remind faculty and academic staff to disclose activities and relationships, including those with foreign entities
  - Ask faculty and academic staff if they have reported **all** outside activities and relationships
  - What is reported in the OAR system is separate from Other/Current & Pending Support documents
  - Make use of the UW – Madison Disclosure Matrix

Important Points for Research Administrators

- Agencies are attempting to harmonize guidance and forms, but there is still room for individual agency requirements: pay close attention to agency instructions
- Many changes are coming. Federal laws, regulations, and policies will affect this:
  - CHIPS and Science Act will require, among other things, institutions and investigators to make certifications regarding foreign talent recruitment programs
  - CHIPS and Science Act and NSPM-33 require personnel to take research security training

Important Points for Research Administrators

- Federal focus on research security will result in regulation changes
- Pay attention to funding announcements and policy changes from feds
- Ensure consistency between biosketch, other/current & pending support, RPPRs – manual process

Campus Resources

- RSP
  - https://rsp.wisc.edu/internationalresearchcollaborations/
  - https://rsp.wisc.edu/other-support-information.cfm
- Outside Activities Reporting (COI/COC)
  - https://research.wisc.edu/compliance-policy/outside-activities-reporting/
- Export Controls
  - https://research.wisc.edu/integrity-and-other-requirements/export-control/
- Cybersecurity

Further Reading - NIH

- https://grants.nih.gov/policy/foreign-interference/about-foreign-interference
  - See sections on:
    - Types of Problems
    - Case Studies
- https://grants.nih.gov/policy/foreign-interference/data
  - See also: Brief Summary of NIH Foreign Interference Cases (August 8, 2022)

Further Reading - NSF

- https://beta.nsf.gov/research-security
- See sections on:
  - Foreign Interference and Risk Mitigation
  - Administrative Actions
  - Case Studies of Violations in Research Security

Other Resources

- NSPM-33 Implementation Guidance
- COGR's Matrix of Science & Security

Questions and Discussion