**Research and Development National Security Policy (NSPM-33) Guidance**

**For URI Principal Investigators, other Faculty and Staff involved with Sponsored Projects**

On January 14, 2021, the White House issued the “[Presidential Memorandum on United States Government – Research and Development National Security Policy](https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/),” known as [NSPM-33](https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/). NSPM-33 directs a national response intended to safeguard the security and integrity of federally funded R&D in the United States.

On January 4, 2022, the White House Office of Science and Technology Policy (OSTP) and the National Science and Technology Council issued [guidance](https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf) to federal research agencies and released an [implementation guide for the NSPM-33](https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf). The guidance directs agencies, including but not limited to NIH and NSF to work together to develop model forms and instructions that clarify what information must be disclosed in federal grant applications, standardized across agencies to the greatest extent possible. Please visit URI’s PreAward website for the most up-to-date NIH and NSF agency disclosure guidance [Federal Agency Information – Division of Research and Economic Development (uri.edu)](https://web.uri.edu/research-admin/central-pre-award/federal-agency-information/).

In February of 2023, OSTP in partnership with Federal agencies and external research communities, released draft guidance for public comment (due by June 5, 2023) regarding the implementation of NSPM-33.

**What are the priorities of NSPM-33?** The priorities of NSPM-33 are (1) protecting America’s security and openness; (2) making disclosures and research security policies clear so that researchers can comply; and (3) ensuring that the policies do not fuel xenophobia or prejudice.

**What are the five key NSPM-33 provisions**?The draft guidance details the implementation of five key NSPM-33 provisions:

1. Disclosure Requirements and Standardization
2. Digital Persistent Identifiers
3. **Consequences For Violating Disclosure Requirements**
4. Agency Information Sharing
5. Research Security Programs

**What is the significance of the NSPM-33 Research Security Program Requirement?** NSPM-33 requires research institutions that receive in excess of $50 million per year to certify that they have implemented a research security program that includes increased **cybersecurity, foreign travel security, research security training, and export control training.** Because URI receives more than $50 million in annual federal research funding, a Research Security Program is required. URI is committed to strengthening its research enterprise within these major areas outlined by NSPM-33.

**What is URI doing to comply with NSPM-33 Requirements?** URI is reviewing its applicable procedures against what we currently know about the NSPM-33 requirements. As we learn more from Federal agencies about their updated requirements, we will update the Research Community about the changes we will need to implement to comply with NSPM-33. In the meantime, we encourage our Researcher Community to continue to:

1. Be transparent regarding other research support, other research activities, and research collaborations when submitting proposals.
2. Take extra precautions for foreign travel to high risk areas by taking a URI loaner laptop [International Traveler Laptop Loaner Program – Reserving Equipment – Division of Research and Economic Development (uri.edu)](https://web.uri.edu/research-admin/office-of-research-integrity/export-controls/laptop-loaner-program/reserving-equipment/).
3. Engage in continuous education and complete URI’s Export Control Training (Module16800)

<https://www.citiprogram.org/default.asp> and DoD’s CUI Training [https://securityhub.usalearning.gov](https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsecurityhub.usalearning.gov%2F&data=04%7C01%7C%7Cdb06d261de36436f2ffc08d9f883785e%7C17f1a87e2a254eaab9df9d439034b080%7C0%7C0%7C637814065817366418%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=8OPal9wk1plhzC3cdlDEKiGEHz43zXZbH%2F1Ff9LDKzI%3D&reserved=0) even if your research is not controlled.

1. Review URI [Policy # 07.102.2 on IT Endpoint Projection](https://web.uri.edu/policies/wp-content/uploads/sites/928/IT-Endpoint-Protection-20220607-07.102.2.pdf) being implemented by IT Security that requires all university electronic devices use appropriate security measures and have appropriate security software installed.
2. Become familiar with URI’s [separate research network](https://its.uri.edu/research-zone/).

To report changes to disclosure documents related to existing awards, please contact franca@uri.edu. For cybersecurity questions, please contact mkhalfayan@uri.edu and for Export Control questions, please contact carolconnolly@uri.edu.