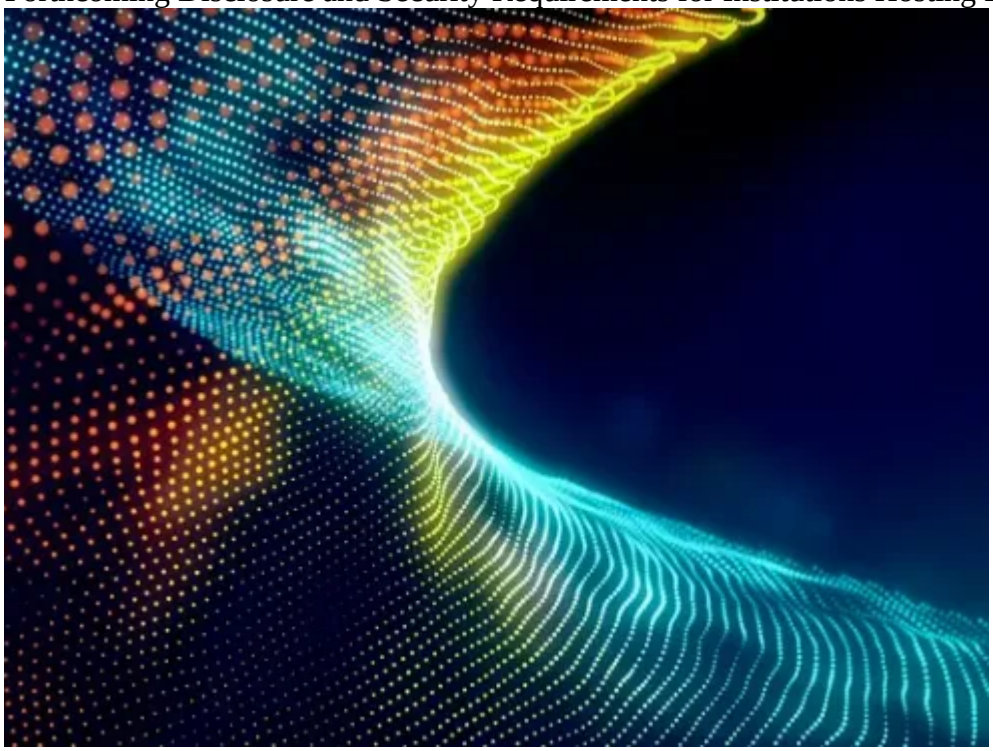
Updates
June 07, 2022
Forthcoming Disclosure and Security Requirements for Institutions Hosting Federally Funded Research



NSPM-33

National Security Presidential Memorandum-33 (NSPM-33) and implementation guidance from the National Science and Technology Council (NSTC) direct federal agencies to standardize and enhance disclosure and security requirements that apply to federally funded research and development (R&D). These new requirements will have direct effects on academic and research institutions that receive federal funding.

All federal research funding agencies will be required to bolster and standardize reporting and disclosure requirements. Academic and research institutions that receive federal funding for research will be subject to disclosure requirements as a condition of eligibility for federal R&D awards.

Moreover, institutions that receive significant federal funding will incur additional requirements related to research security and integrity. In particular, research security programs that include cybersecurity, insider threat, and export control components must meet certification requirements.

Background

NSPM-33 was issued in the final days of the Trump administration and endorsed by the Biden administration in August 2021. The NSTC released its implementation guidance in January 2022. The guidance focuses on standardized disclosure requirements, tracking disclosures through digital persistent identifiers (DPIs), consequences for noncompliance, information sharing between research agencies, and research security program measures. Although NSPM-33 is directed at federal agencies, it requires those agencies to mandate enhanced disclosure and security programs at academic and research institutions that receive federal funding.

Timeline

Though we are waiting on additional guidance, such as how the government will use the disclosed information to determine the allocation of funding and the certification standard for national research security program compliance, *some efforts are required "as quickly as is feasible,"* such as the implementation of DPIs. Furthermore, "[q]ualifying research organizations should establish a research security program as soon as possible," though the formal requirement to comply for eligible institutions is January 2023. The research security program certification requirements are significant. Eligible institutions may need significant lead time to meet the January 2023 compliance date.

Significantly, NSPM-33 and its implementation should be viewed in the context of sustained U.S. government efforts to secure the federal R&D enterprise and enforce disclosure requirements. The government has adopted a "whole-of-government" approach that includes, among other tools, criminal prosecution, civil enforcement, and suspension and debarment. In that regard, NSPM-33 should be seen, in part, as a refinement of government efforts to enhance disclosure and transparency, and to streamline enforcement for noncompliance.

Enforcement

Over the last four years, the federal government has scrutinized the misappropriation of U.S. intellectual property, technology, and research efforts by foreign governments. That effort also targeted federally funded researchers' alleged nondisclosures of foreign positions and funding. In 2018, the U.S. Department of Justice (DOJ) announced the controversial China Initiative, an enforcement push designed to protect U.S. R&D from alleged widespread intellectual property theft by Chinese entities and nationals. Under the China Initiative, the DOJ charged more than 61 cases. More recently, federal funding agencies such as the National Institutes of Health (NIH) clarified and/or enhanced disclosure requirements for federally funded research grants. Although the DOJ formally terminated the China Initiative in February 2022, Assistant Attorney General Matt Olsen made clear that criminal enforcement of disclosure requirements remains an option in appropriate cases.

Criminal prosecution, of course, is not the only remedy available to the government. Civil enforcement under the False Claims Act (FCA) or other authorities, as well as suspension and debarment, are other options for the government to proceed against individuals and institutions for noncompliance.

In that regard, NSPM-33's new reporting requirements for individual researchers and institutions expand existing disclosure obligations. As a practical matter, every research institution that applies for federal funding will be

subject to the expanded reporting requirements imposed by the NSPM. The ongoing enforcement activity has increased the stakes of failure to comply.

NSPM-33 specifically highlights that failure to adhere to the disclosure requirements may lead to criminal, civil, or administrative consequences. Extreme cases could jeopardize the Higher Education Act (HEA) Title IV funds, which would result in the denial of federal student financial aid to students. Research institutions are encouraged to come forward and self-disclose omissions or inaccuracies. Self-reporting will be favorably considered during the process of resolving noncompliance.

Requirements to Comply

Disclosure Requirements

The new requirements will likely clarify what information must be disclosed and who is responsible for confirming that the disclosures are complete and accurate—both of which have been contentious issues during government enforcement actions. Federal funding agencies will require disclosures in four general areas: (1) organizational affiliations and employment, (2) positions and appointments, (3) foreign government-sponsored talent recruitment programs, and (4) current and pending support and other support. All four categories will apply to Tier I individuals, such as principal investigators, program officers, and intramural researchers. Tier II individuals, such as peer reviewers and advisory committee/panel members, will only be required to make disclosures in the first three areas.

Although NSPM-33 requires funding agencies to harmonize disclosure requirements to the extent possible, some variation in these general requirements is permissible as required by statute or regulation, where more stringent protections are necessary. For example, particularly sensitive R&D projects could require disclosures from broader classes of individuals, such as students.

With regard to Tier I individuals, NSTC-directed funding agencies are directed to require disclosures of enumerated categories of information within three main areas and specified where those disclosures should be made. Taken together, the requirements not only harmonize and update disclosure requirements, but also appear intended to fill substantive gaps and clarify the responsibility of individuals and organizations to ensure that disclosures are complete, up-to-date, and accurate. Stating the requirements more clearly, comprehensively, and consistently will make participants aware of their specific obligations, but may also provide a more solid base for enforcement in the event of noncompliance.

First, the "Personal Information" disclosures include (1) professional background and qualifications; (2) organizational affiliations; (3) appointments, *regardless of remuneration or time commitment*; and (4) paid consulting.

Second, the "Research Funding Information" disclosures consist of (1) current and pending support, *defined broadly*; (2) current and pending participation in, or applications to foreign government programs, including *talent recruitment programs*; (3) in-kind contributions not intended for use on the proposed project; (4) visiting scholars funded by another institution; (5) students and postdoctoral researchers funded by another institution; (6) travel supported or paid for by another institution in connection with research activities with an associated time commitment; and (7) a certification *by the Tier I individual* that the disclosure is accurate, current, and complete.

Third, the "Project Information" disclosures include (1) in-kind contributions that support the proposed project; (2) capital funding such as private equity or venture capital; and (3) *supporting documentation* such as contracts, grants, and agreements between Tier I individuals and foreign governments, instrumentalities, or entities, including talent recruitment programs.

Agencies will also provide for updates to and corrections of disclosures after submission. Moreover, they will require research organizations to certify that every covered individual listed in an application has been made aware of their disclosure requirements and the potential criminal penalties for knowingly making false representations.

To ease the administrative burden and streamline compliance, NSTC required federal agencies to work together to develop model forms for use and modification by research institutions. NSTC directed agencies to publish model forms in May 2022, so those may be released soon.

Implementation of Digital Persistent Identifiers

To better track disclosures in an effort to both increase security and reduce administrative burden, agencies will require the use of DPIs that integrate into the grant application process. Agencies and institutions alike will need to be mindful of compliance with data privacy laws.

Information Sharing

Research institutions should be aware that agencies have an obligation to share violations of disclosure requirements. As such, disclosures need to be complete, accurate, and uniform to all agencies.

Research Security Certification

Research organizations that received at least $50 million or more in total federal science and engineering support for the previous two fiscal years as recorded on USASpending.gov will be required to certify compliance with the research security program requirement to remain eligible for federal funding. Certification entails satisfying four substantial requirements:

- **Cybersecurity.** NSTC has identified 14 protocols and procedures to satisfy the cybersecurity element of certification.
- **Foreign travel security.** Research institutions will be responsible for maintaining an international travel policy 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." Research institutions should maintain records of international travel by faculty and staff covered in the policy and provide security briefing and assistance with electronic device security as appropriate.
- **Research security training.** This will include both periodic training and tailored training in the event of a research security incident.
- **Export control training as appropriate.**

Research organizations will also be required to designate a research security point of contact with a publicly accessible means to contact that individual.

Conclusion

The federal government is heavily enforcing threats to the independence of federally funded research. As such, they have imposed new disclosure requirements that affect every institution that receives federal funding. There are serious consequences for noncompliance, though good faith efforts and self-reported mistakes may mitigate penalties. Institutions that receive over $50 million in federal research funding are subject to additional requirements, most notably the certification of a robust security program. Although not all the expectations or certifications have been ironed out, institutions are expected to begin making a good faith effort to comply as soon as feasible.

Research institutions that receive federal R&D support should consult counsel to ensure that their disclosure and security programs comply with new requirements. Counsel can help design and implement compliance programs and keep them up to date.

Authors

Explore more in

Business Litigation | National Security | White Collar & Investigations | Privacy & Security | Government Contracts | Data Security Counseling and Breach Response | Healthcare

Related insights

Update

Privacy Law Recap 2024: Class Actions and Mass Arbitrations

Update

DOJ's Final Rule on Data Transfers: Impacts Across Industries