SmartSuite

Framework / Risk Management / Other

National Security Presidential Memorandum 33 (NSPM-33), United States Government-Supported Research and Development National Security Policy (January 14, 2021)

NSPM-33 (January 14, 2021) directs federal agencies to protect U.S. Government-supported R&D through standardized disclosure, vetting and research security programs above $50 million a year.



What it is

NSPM-33 is National Security Presidential Memorandum 33, the Presidential Memorandum on United States Government-Supported Research and Development National Security Policy of January 14, 2021, which directs federal agencies to strengthen protections of U.S. Government-supported research and development against foreign government interference and exploitation (Sec. 1). It is addressed to executive departments and agencies, and research institutions meet it through the disclosure, vetting and program requirements their funding agencies impose. Its best-known rule is Sec. 4(g): institutions receiving federal science and engineering support in excess of 50 million dollars per year must certify to the funding agency that they have established and operate a research security program.

At a glance

PUBLISHER
The White House (Office of Science and Technology Policy)

TYPE
Guidance

VERSION
NSPM-33 (January 14, 2021); OSTP research security program guidelines July 9, 2024

EFFECTIVE
January 14, 2021

DOMAIN
Risk Management

FAMILY
Other

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

Why it matters

- **A threshold institutions can test** Sec. 4(g) sets the line at more than 50 million dollars per year in federal science and engineering support; the 2024 guidelines define a covered institution as an institution of higher education, FFRDC or nonprofit research institution above that line in FY 2022 constant dollars on a three-year average of NCSES survey data.
- **Four named program elements** Cybersecurity, foreign travel security, research security training and export control training, each with a standardized way to certify it under Section II of the 2024 guidelines.
- **Disclosure that is standardized across agencies** Sec. 4(b) requires disclosure of affiliations and employment, other support, foreign talent recruitment programs and positions and appointments, in two tiers, with annual updates and standardized forms (Sec. 4(b)(ii) to (vi)).
- **Digital persistent identifiers** Sec. 4(b)(v) directs agencies to require researchers on federal grants to register with a service that provides a digital persistent identifier, so disclosures can be matched across agencies.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NSPM-33

Research Security Program Certification

Keep the written or electronic attestation to each federal research agency, the four-element evidence behind it and the program description that must be provided within 30 days of an agency request, in Compliance Management.

Disclosure and Conflict Register

Record each covered individual's affiliations, other support, talent recruitment program participation and positions under Sec. 4(b), with the Tier I or Tier II category, the digital persistent identifier and the annual update date, in Enterprise Risk Management.

International Travel Record

Maintain the organizational record of international travel for covered individuals that the foreign travel security element requires, with disclosure, authorization and device-security steps where the agency's award terms call for them.

Training Completion Evidence

Track research security training for all covered individuals, foreign travel security training at least once every six years, and export control training for those working with export-controlled technologies, with completion dates and the module or program used.

Cybersecurity Element Alignment

Map the institution's cybersecurity program to the NIST resource under CHIPS Section 10229 or, for the 2022 safeguards, to the fourteen basic protocols, with owners and evidence in Cyber & IT Risk.

Foreign Sponsor and Partner Review

Review foreign sponsors, collaborators and partnerships against export control and Entity List considerations in Third Party Risk Management, linking each review to the award and the researchers involved.

Common framework mappings

CIS Controls v8.1 | CMMC 2.0 | FERPA | FISMA | GDPR | HIPAA | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

NSTC NSPM-33 Implementation Guidance

Provides detailed guidance on implementing security measures under NSPM-33.

bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

NSTC Research Security Programs Overview

Outlines key elements of research security programs as per NSPM-33.

nsf.gov/research-security

NSPM-33 — Presidential Memorandum on United States Government-Supported Research and Development National Security Policy

The memorandum itself, issued January 14, 2021 (archived copy on the National Archives' Trump White House site).

trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy

Frequently asked questions

Which institutions must certify a research security program under NSPM-33?

Sec. 4(g) applies to research institutions receiving federal science and engineering support in excess of 50 million dollars per year. The 2024 OSTP guidelines define a covered institution as an institution of higher education, a federally funded research and development center or a nonprofit research institution that exceeds that amount in fiscal year 2022 constant dollars on the three-year average of federal R&D obligations in the NCSES Survey of Federal Science and Engineering Support (or the Survey of Federal Funds for R&D for FFRDCs).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What must a research security program include?

Under Section II of the 2024 guidelines, the institution certifies that its program includes cybersecurity, foreign travel security, research security training and export control training as appropriate. Sec. 4(g) of the memorandum listed cybersecurity, foreign travel security, insider threat awareness and identification and, as appropriate, export control training; the 2022 guidance added a research security point of contact and fourteen cybersecurity safeguarding protocols.

What do researchers have to disclose under NSPM-33?

Sec. 4(b)(ii) lists four categories: organizational affiliations and employment; other support, including in-kind resources provided directly to the individual; current or pending participation in programs sponsored by foreign governments, including talent recruitment programs; and positions and appointments, paid or unpaid. Tier I personnel (principal investigators and key personnel, program officers, intramural funding recipients) disclose all four; Tier II (peer reviewers, advisory committee and panel members) disclose all but other support. Updates are at least annual (Sec. 4(b)(iv)).

What is the timeline for the 2024 research security program guidelines?

Section IV gives relative deadlines rather than calendar dates: federal research agencies submit plans to OSTP and OMB within six months of the July 9, 2024 memorandum; updated agency policies take effect no later than six months after finalized plans are submitted; and agencies must give covered institutions adequate time, but not more than 18 months after the effective date of their plans, to implement the requirements. The 2022 guidance had allowed one year from issuance of the formal requirement.

Is NSPM-33 a law?

No. It is a presidential memorandum that directs executive agencies, and Sec. 6(c) says it creates no right or benefit enforceable against the United States. Institutions are bound through agency policies, award terms and conditions and the consequences in Sec. 4(b)(ix). The CHIPS and Science Act of 2022 later placed research security training and program requirements in statute (Section 10634, 42 U.S.C. 19234), which the 2024 guidelines implement together with NSPM-33.

License included / downloadable: Yes The memorandum and both guidance documents are U.S. Government publications available free of charge from the White House archives.

Full framework page and mappings: smartsuite.com/frameworks/nspm-33-research-security