

NSPM-33 – Research Security

NSPM-33 sets federal requirements to protect U.S.-funded research from foreign influence, undisclosed collaborations, and security risks.



What it is

U.S. NSTC NSPM-33 — National Security Presidential Memorandum 33 is a U.S. federal policy directive that strengthens research security and integrity at institutions conducting federally funded research. The memorandum establishes comprehensive requirements intended to protect sensitive research from foreign interference and promote transparency, accountability, and responsible conduct within the research ecosystem.

Published by the White House and overseen by the National Science and Technology Council (NSTC), NSPM-33 applies to federal executive agencies, research institutions, and universities receiving federal research funding. It addresses key areas including cybersecurity controls, risk management procedures, disclosure requirements for conflicts of interest and foreign relationships, and oversight of research personnel and data.

At a glance

PUBLISHER The White House (Office of Science and Technology Policy)	TYPE Guidance	VERSION 2021
EFFECTIVE January 14, 2021	DOMAIN Risk Management	FAMILY Other
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>

Why it matters

- **Strengthen research security governance** Promote consistent oversight of research security processes and help organizations identify and mitigate emerging threats across research activities.
- **Enhance compliance with federal mandates** Enable organizations to meet federal research security requirements, reducing the risk of funding disruptions and reputational harm.
- **Improve protection of sensitive information** Support safeguards that reduce unauthorized access to confidential or proprietary research data and intellectual property.
- **Increase transparency and accountability** Establish reporting and disclosure standards that improve clarity regarding external collaborations, financial interests, and researcher affiliations.

How SmartSuite supports NSPM-33

Research Security Governance Library

Structure NSPM-33 requirements covering research security programs, disclosure obligations, and institutional oversight.

Federally Funded Research Project Tracking

Track federally funded research projects, participating institutions, and associated security obligations.

Researcher Disclosure and Reporting Obligations

Manage researcher disclosures, affiliations, and reporting obligations required for research security compliance.

Foreign Collaboration and Risk Monitoring

Track international partnerships, collaborations, and potential research security risks.

Training and Awareness Programs

Manage researcher security training programs and track completion for compliance verification.

Research Security Posture and Federal Oversight Reporting

Provide dashboards showing research security posture, disclosure status, and readiness for federal oversight reviews.

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](https://www.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](https://www.nsf.gov/research-security)

NSTC Policy and Regulation Updates

Describes updates to research security policies under NSPM-33.
[nsf.gov/research-security](https://www.nsf.gov/research-security)

Frequently asked questions

What is NSTC NSPM-33 used for?

NSTC NSPM-33 establishes requirements and guidelines to protect U.S. federally funded research from foreign government interference and exploitation. The memorandum aims to safeguard the integrity of research environments, mitigate security risks, and promote responsible information sharing across research institutions.

Is compliance with NSTC NSPM-33 required for organizations?

Yes, compliance with NSPM-33 is mandatory for organizations receiving federal research funding in the United States. Federal agencies have incorporated the memorandum's requirements into grant, contract, and cooperative agreement terms with recipient organizations.

What entities or research activities does NSTC NSPM-33 apply to?

NSTC NSPM-33 applies to universities, research institutions, and federal contractors receiving federal funding for research projects. The requirements cover activities involving sensitive or controlled research, particularly those at risk of foreign influence, regardless of the research domain.

What are the key concepts and artifacts required by NSTC NSPM-33?

Key concepts in NSPM-33 include research security programs, foreign talent program disclosures, conflict of interest disclosures, and standardized risk assessment processes. Required artifacts include documented security policies, training materials, and comprehensive disclosure forms from researchers and staff.

How do organizations implement NSTC NSPM-33 requirements?

Organizations must establish or enhance research security programs that align with NSPM-33 directives, including developing policies, processes for risk identification, security training programs, and ongoing monitoring mechanisms. Implementation typically involves collaboration among compliance, security, research administration, and IT teams.

How does NSPM-33 relate to other research security frameworks?

NSPM-33 complements existing federal regulations such as the National Industrial Security Program (NISPOM) and Controlled Unclassified Information (CUI) requirements. It fills research-specific gaps by standardizing disclosure and security expectations across federally funded projects, creating a unified baseline.

What are the ongoing compliance requirements under NSTC NSPM-33?

Ongoing compliance includes maintaining up-to-date disclosure records, conducting periodic research security training, performing regular program reviews, and promptly reporting potential risks or breaches. Organizations must also continuously monitor and update their research security controls as federal guidance evolves.

How would SmartSuite support NSTC NSPM-33?

SmartSuite can help organizations manage NSTC NSPM-33 compliance by enabling configurable workflows for risk tracking, documenting and reviewing security controls, collecting and centralizing researcher disclosures, and supporting evidence collection for audits. Automated task management, comprehensive reporting, and centralized document repositories support ongoing audit readiness and help demonstrate compliance to federal agencies.

License included / downloadable: Yes NSPM-33 is publicly available via official White House/NSTC government publications. License included with platform

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