Performance Audit of U.S. National Science Foundation's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2026

REPORT PREPARED BY CASTRO & COMPANY, LLC



U.S. NATIONAL SCIENCE FOUNDATION
Office of Inspector General

November 03, 2026
OIG 27-02-001

At a Glance

Performance Audit of U.S. National Science Foundation's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2026
OIG 27-02-001 | November 03, 2026

AUDIT OBJECTIVE

The U.S. National Science Foundation Office of Inspector General engaged Castro & Company, LLC (Castro) to conduct a performance audit of NSF's Information Security Program for fiscal year 2026, as required by the Federal Information Security Modernization Act of 2014 (FISMA, Pub. L. No. 113-283). The audit, which was conducted in accordance with the performance audit standards established by Generally Accepted Government Auditing Standards (GAGAS), included an assessment of the corrective actions taken by NSF in response to the FY 2025 FISMA audit.

AUDIT RESULTS

Castro found that NSF's security controls were effective in six of the ten FISMA metric domains. However, NSF's security controls were not effective in the remaining four domains, which resulted in a not effective rating for NSF's overall Information Security Program for FY 2026 in accordance with the applicable Inspector General FISMA Reporting Metrics. Castro determined that two prior year findings were closed and that NSF has not fully implemented corrective actions to address the remaining eight prior year findings. Castro identified one new finding for FY 2026. Castro is responsible for the Performance Audit and the conclusions expressed in the report. NSF OIG does not express any opinion on the conclusions presented in Castro's audit report.

RECOMMENDATIONS

The auditors included one new finding in the report related to the Protect function with associated recommendations for NSF to address weaknesses in information technology security controls.

AUDITEE RESPONSE

NSF agreed with the finding and recommendations in the report and plans to incorporate information gained and lessons learned from the review to continue making improvements in its information security program.

CONTACT US

For congressional, media, and general inquiries, email OIGPublicAffairs@nsf.gov.

National Defense Authorization Act General Notification

Pursuant to Pub. L. No. 117-263 § 5274, business entities and non-governmental organizations specifically identified in this report have 30 days from the date of report publication to review this report and submit a written response to NSF OIG that clarifies or provides additional context for each instance within the report in which the business entity or non-governmental organization is specifically identified. Responses that conform to the requirements set forth in the statute will be attached to the final, published report.

If you find your business entity or non-governmental organization was specifically identified in this report and wish to submit comments under the above-referenced statute, please send your response within 30 days of the publication date of this report to OIGPL117-263@nsf.gov, no later than December 06, 2026. We request that comments be in .pdf format, be free from any proprietary or otherwise sensitive information, and not exceed two pages. Please note, a response that does not satisfy the purpose set forth by the statute will not be attached to the final report.

About Us

NSF OIG was established in 1989, in compliance with the *Inspector General Act of 1978* (5 USC 401-24). Our mission is to provide independent oversight of NSF to improve the effectiveness, efficiency, and economy of its programs and operations and to prevent and detect fraud, waste, and abuse.

Contact Us

Address:
U.S. National Science Foundation Office of Inspector General
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Phone: 703-292-7100

Website: oig.nsf.gov
Follow us on X: https://x.com/nsfoig

Congressional, media, and general inquiries: OIGPublicAffairs@nsf.gov
Freedom of Information Act inquiries: FOIAOIG@nsf.gov

Report Fraud, Waste, or Abuse

Report violations of laws, rules, or regulations; mismanagement; and research misconduct involving NSF operations or programs via our Hotline:

- File online report: oig.nsf.gov/contact/hotline
- Anonymous Hotline: 1-800-428-2189
- Mail: Randolph Building, 401 Dulany Street, Alexandria, VA 22314 ATTN: OIG HOTLINE

Have a question about reporting fraud, waste, or abuse? Email OIG@nsf.gov.

Whistleblower Retaliation Information

All NSF employees, contractors, subcontractors, awardees, and subawardees are protected from retaliation for making a protected disclosure. If you believe you have been subject to retaliation for protected whistleblowing, or for additional information on whistleblower protections, please visit oig.nsf.gov/whistleblower.