Performance Audit of the National Science Foundation's Information Security Program for FY 2023

REPORT PREPARED BY KEARNEY & COMPANY, P.C.

NATIONAL SCIENCE FOUNDATION
Office of Inspector General

November 9, 2023
OIG 24-2-001

NATIONAL SCIENCE FOUNDATION
Office of Inspector General

At a Glance

Performance Audit of the National Science Foundation's Information Security Program for FY 2023

November 9, 2023 | OIG 24-2-001

AUDIT OBJECTIVE

The National Science Foundation Office of Inspector General engaged Kearney & Company, P.C. (Kearney) to conduct a performance audit of NSF's Information Security Program for fiscal year 2023, 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 2022 FISMA audit.

AUDIT RESULTS

Kearney found that NSF's security controls were effective in seven of the nine FISMA metric domains and that NSF's Information Security Program was effective for FY 2023 in accordance with the U.S. Department of Homeland Security's *FY 2023 Inspector General FISMA Reporting Metrics*. Kearney determined that NSF corrective actions remediated two prior year findings and that NSF is in the process of implementing corrective actions to address the remaining four prior year findings. Kearney identified one new finding for FY 2023. Kearney 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 Kearney's audit report.

RECOMMENDATIONS

The auditors included one new and four modified repeat findings in the report with associated recommendations for NSF to address weaknesses in information technology security controls.

AGENCY RESPONSE

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

About NSF OIG

We promote effectiveness, efficiency, and economy in administering the Foundation's programs; detect and prevent fraud, waste, and abuse within NSF or by individuals who receive NSF funding; and identify and help to resolve cases of research misconduct. NSF OIG was established in 1989, in compliance with the *Inspector General Act of 1978* (5 USC 401-24). Because the Inspector General reports directly to the National Science Board and Congress, the Office is organizationally independent from the Foundation.

Connect with Us

For further information or questions, please contact us at OIGpublicaffairs@nsf.gov or 703-292-7100. Follow us on Twitter at @nsfoig. Visit our website at https://oig.nsf.gov/.

Report Fraud, Waste, Abuse, or Whistleblower Reprisal

- File online report: https://oig.nsf.gov/contact/hotline
- Anonymous Hotline: 1-800-428-2189
- Mail: 2415 Eisenhower Avenue, Alexandria, VA 22314 ATTN: OIG HOTLINE
- For general inquiries about reporting fraud, waste, and abuse: Email oig@nsf.gov

National Defense Authorization Act (NDAA) 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 organizations 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 14, 2023. 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.