External Penetration Testing of the NSF and U.S. Antarctic Program Networks

REPORT PREPARED BY MAX CYBERSECURITY, LLC

NATIONAL SCIENCE FOUNDATION
Office of Inspector General

CUI Contact: cui@nsf.gov

November 15, 2023
OIG 24-6-001

At a Glance

External Penetration Testing of the NSF and U.S. Antarctic Program Networks

October 17, 2023 | OIG 24-6-001

WHY WE ISSUED THIS REPORT

As part our ongoing efforts to assess the National Science Foundation (NSF) information security program, we engaged Max Cybersecurity, LLC (Max Cyber) to perform external penetration testing of the NSF and U.S. Antarctic Program (USAP) external network segments, systems, and applications as well as the research.gov domain in support of OIG's *Federal Information Security Modernization Act* (FISMA, Pub. L. No. 113-283) evaluation for FY 2023. The objective of the testing was to identify and attempt to exploit network vulnerabilities in NSF's and USAP's external security architecture. The external penetration testing sought to provide a practical demonstration of the security controls' effectiveness and to provide an estimate of each network's susceptibility to exploitation and data breaches.

OVERALL OBSERVATIONS

The NSF and USAP networks present a medium-risk attack surface. Multiple vulnerabilities were identified during the penetration testing, including security flaws and instances of data leakage, which may contribute to unauthorized access, network disruption, and pose a significant risk to NSF's and USAP's information systems. Max Cyber is responsible for the testing and the conclusions expressed in the report. NSF OIG does not express any opinion on the conclusions presented in Max Cyber's report.

RECOMMENDATIONS

Max Cyber recommended that NSF remediate the vulnerabilities identified through the penetration testing using NSF's vulnerability management procedure.

AGENCY RESPONSE

NSF agreed with all findings in the report. NSF's response is attached in its entirety to the report as Appendix One.

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, to OIGPL117-263@nsf.gov, no later than December 20, 2023. We request that comments be in .pdf format, be free from any proprietary or otherwise sensitive information, and not exceed 2 pages. Please note, a response that does not satisfy the purpose set forth by the statute will not be attached to the final report.