OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

The U.S. Department of the Interior's Cyber Threat Detection and Defense Controls

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

AUG 10 2022

Memorandum

To: June Hartley
Acting Chief Information Officer

From: Kathleen Sedney
Assistant Inspector General for Audits, Inspections, and Evaluations

Subject: Closeout Memorandum – *The U.S. Department of the Interior's Cyber Threat Detection and Defense Controls*
Report No. 2020–ITA–067

In October 2020, we initiated an evaluation of the U.S. Department of the Interior's cyber threat detection and defense controls. Our objective was to determine whether the Department deploys and operates a secure infrastructure for its public-facing internet systems in accordance with guidance provided by the National Institute of Standards and Technology, Department policy, and industry best practices. Specifically, we conducted penetration testing of the Department's public-facing systems. We found that the Department detected our simulated attacks and responded in accordance with actions agreed upon by the Office of the Chief Information Officer (OCIO) and the Office of Inspector General, as defined in our Rules of Engagement.[1] We are closing this evaluation because we are satisfied with the Department's response to our technical tests.

To assess security weaknesses with the Department's public-facing systems, we conducted technical tests from May 1, 2021, to November 2, 2021. The scope of this evaluation included all of the Department's on-premise public-facing systems.[2] First, we used software tools to test the Department's systems for vulnerabilities. Vulnerabilities are software flaws or system misconfigurations that can be exploited to gain access to or control of an information system. Vulnerability scanners are specialized software tools that automate the vulnerability detection process. Second, we used ethical hacking tools to simulate malicious activity and reviewed the Department's incident tracking system and incident response tools to evaluate whether the Department detected and responded to our simulated malicious activity. We provided the results of our tests to the Department for vulnerability confirmation and mitigation.

[1] "Rules of Engagement" is an agreement that defines detailed guidelines and constraints for executing information security testing. The agreement is established before starting a security test and gives the test team authority to conduct defined activities without the need for additional permissions.
[2] On-premise systems are those physically hosted inside a Department or bureau data center.

We conducted similar reviews of incident handling and vulnerability detection and mitigation practices in 2015 and 2018.[3] Our 2015 evaluation reported critical vulnerabilities on public-facing systems, and our 2018 evaluation found that many of the alerts generated from our simulated malicious activity went unnoticed by the Department. In this project, we determined that the Department demonstrated improvement since the 2015 and 2018 evaluations were performed. In particular, our review of the Department's incident tracking system demonstrated that information technology staff identified our simulated attacks. Moreover, the Department mitigated confirmed technical vulnerabilities identified by our technical tests.

We are encouraged by this improvement but advise the Department to remain vigilant. The Department has many public-facing internet systems that face a variety of other vulnerabilities that should be considered and addressed. Our technical testing was broad in scope and did not mimic adversaries who may have the time and resources to focus their attacks.

Because we are not offering recommendations, we do not require a response. We will notify Congress of our findings and include information regarding this work in our next *Semiannual Report to Congress* as required by law. We will also post a public version of this report on our website.

If you have any questions, please contact me at 202–208–5745.

[3] *Security of the U.S. Department of the Interior's Publicly Accessible Information Technology Systems* (Report No. ISD–IN–MOA–0004–2014), issued July 15, 2015, and *Interior Incident Response Program Calls for Improvement* (Report No. 2016–ITA–020), issued March 12, 2018.

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

REPORT FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

The Office of Inspector General (OIG) provides independent oversight and promotes integrity and accountability in the programs and operations of the U.S. Department of the Interior (DOI). One way we achieve this mission is by working with the people who contact us through our hotline.

If you wish to file a complaint about potential fraud, waste, abuse, or mismanagement in the DOI, please visit the OIG's online hotline at **www.doioig.gov/hotline** or call the OIG hotline's toll-free number: **1-800-424-5081**

Who Can Report?

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement involving the DOI should contact the OIG hotline. This includes knowledge of potential misuse involving DOI grants and contracts.

How Does it Help?

Every day, DOI employees and non-employees alike contact the OIG, and the information they share can lead to reviews and investigations that result in accountability and positive change for the DOI, its employees, and the public.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act, and other applicable laws protect complainants. Section 7(b) of the Inspector General Act of 1978 states that the Inspector General shall not disclose the identity of a DOI employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the course of the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-DOI employees who report allegations may also specifically request confidentiality.