In Brief

Fiscal Year 2024 Audit of the Smithsonian's Security Incident Prevention, Detection, and Response Capabilities

OIG-A-26-05, March 26, 2026

Background

In recent years, cultural institutions like the Smithsonian Institution (Smithsonian) have been victims of serious information technology (IT) and physical security incidents. For example, within the last three years: a national library experienced a significant cyber-attack; a major museum software provider suffered a ransomware attack; and a shooting took place outside a museum in the Washington, D.C., area. Incidents like these show IT and physical security are increasingly important.

What OIG Did

The Office of Inspector General (OIG) conducted an audit to assess the Smithsonian's capabilities to prevent, detect, and respond to IT and physical security incidents. As a part of the audit, the OIG contracted with a firm to conduct a covert physical and IT security assessment, which included vulnerability testing.

What Was Found

The OIG identified eight physical security goals and four IT security goals for the OIG contractor to accomplish (e.g. accessing certain non-public information/areas). The OIG contractor accomplished two of the eight physical security goals, but did not accomplish any of the IT security goals.

Security Vulnerabilities Identified

During the initial assessment, the OIG contractor conducted an unsuccessful phishing campaign to gain access to the Smithsonian network. The OIG then assisted the contractor by providing internet network access to test the Smithsonian's detection and response processes. The Smithsonian was unable to fully prevent, detect, or respond to all of the security incidents simulated by the contractor. Although Smithsonian staff detected one attack on the Smithsonian's computer network, they were unable to stop other staged attacks, including physical breaches at three Smithsonian facilities and a network breach originating from the internet. The simulated attacks allowed the OIG contractor to obtain access to non-public information and areas.

What Was Recommended

To strengthen physical security controls, OIG recommended that the Director, Office of Protection Services, take the following actions:

1. Update the relevant handbook, to incorporate a procedure on identified physical security threats.

To strengthen IT security controls, OIG recommended that the Chief Information Officer take the following actions:

2. Assess how to reduce the risk of security vulnerabilities for certain websites and determine which features must remain publicly accessible for required functionality.

3. Implement appropriate encryption technologies or formally document a risk-based exception.

Management concurred with these three recommendations. As of the date of this report, OIG has closed recommendations two and three.

The full audit report is not posted on the OIG website because it contains information that, if disclosed, may adversely affect the Smithsonian's IT and physical security. For additional information, please submit a records request to the OIG.