OFFICE OF THE
INSPECTOR GENERAL

Memo

Smithsonian

Information requiring protection from public dissemination has been redacted from this report in accordance with 5 U.S.C. § 552(b)(5) and (7)(E), and Smithsonian Directive 807, Requests for Smithsonian Institution Information, Exemption 2.

Date: July 2, 2019

To: Mike McCarthy, Acting Under Secretary for Finance and Administration

Cc: Deron Burba, Chief Information Officer
Carmen Iannacone, Chief Technology Officer, Office of the Chief Information Officer
Juliette Sheppard, Director of Information Technology Security, Office of the Chief Information Officer

From: Cathy L. Helm, Inspector General Cathy L Helm

Subject: Information Security: The Smithsonian Needs to Enhance Protection of Sensitive Information (OIG-A-19-06)

Information technology (IT) security is a top risk for organizations. Security breaches cost money, disrupt operations, and erode public trust. In a recent study, researchers estimated that an average breach costs almost $4 million.[1]

From October 22, 2018, through November 11, 2018, the Smithsonian Institution's (the Smithsonian) [redacted]

[1] Ponemon Institute LLC, *2018 Cost of a Data Breach Study* (Michigan: Ponemon Institute LLC, 2018).

[redacted]

OIG conducted this audit to assess the Smithsonian's IT security capabilities [redacted] The methodology involved [redacted] The OIG contractor conducted its work from October 22, 2018, through November 11, 2018. [redacted] The scope of the audit did not include systems that the Smithsonian hosts on behalf of two other organizations.

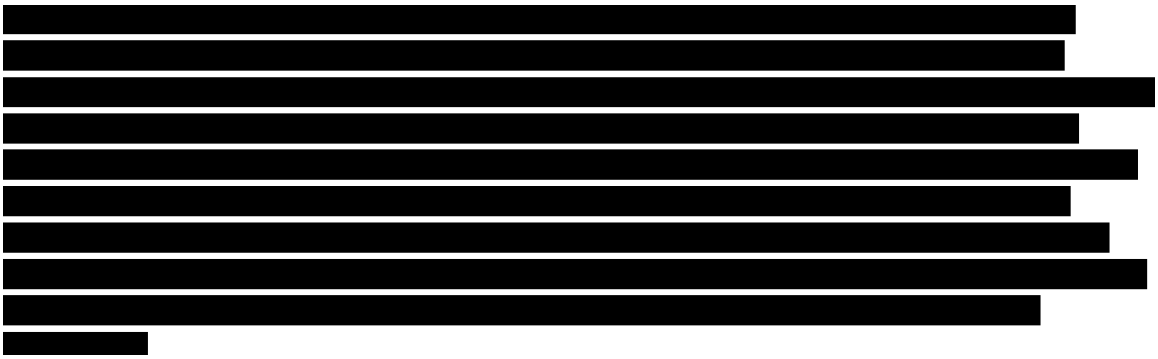
OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on its audit objective.

BACKGROUND

The Smithsonian's Chief Information Officer (CIO) is the senior official responsible for the Institution's information systems and is the primary sponsor for the Smithsonian's IT security program. The Office of the Chief Information Officer (OCIO) manages the technology infrastructure, known as the Smithsonian Institution Network (the network).

[redacted]

The network contains business systems including desktop computers, electronic file storage, and software applications for day-to-day operations.



The Smithsonian's IT security program includes processes like security assessment, monitoring, and incident response.[6] OCIO is primarily responsible for conducting all three processes. IT security assessment lets OCIO review a system to identify and manage related security risks. Monitoring helps OCIO identify security incidents by watching users and systems. Incident response allows OCIO to take action when a security incident is identified.

The Privacy Office is responsible for setting the Smithsonian's privacy policy, working with units to ensure that adequate safeguards are in place for sensitive information, and coordinating the Smithsonian's response to suspected or confirmed privacy breaches. The Smithsonian's privacy policy requires that personally identifiable information "shall be protected by technological and/or physical means commensurate to its sensitivity level and risk of harm to the individual" if the personally identifiable information is compromised.

The Office of Protection Services (OPS) has overall responsibility for the physical security of the Smithsonian and for managing background investigations. OPS stores the sensitive background investigation information in the Identity Management System and Personnel Security Case Management System.

[6] NIST defines security incidents as, "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

RESULTS OF THE AUDIT

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

In October 2018, OIG reported similar results [redacted][8] [redacted]

[redacted]

[redacted]

[8] Actions Needed to Enhance Protection of Sensitive Information (OIG-A-19-01, October 10, 2018).

CONCLUSION

IT security is a high risk because security breaches cost money, disrupt operations, and erode public trust. [redacted]

In response to an OIG recommendation from the previous audit, OCIO is [redacted] and OCIO is incorporating the results of this audit [redacted]. As a result, OIG is not making a recommendation in this report. [redacted]

MANAGEMENT RESPONSE AND OIG EVALUATION

OIG provided a draft of this report to Smithsonian management for review and comment. They provided written comments, which are found in Attachment I. They concurred with OIG's findings and stated that they are working to resolve the findings as a high priority.

Attachment I

MANAGEMENT RESPONSE

Smithsonian Institution

Office of the Chief Information Officer

Date: June 28, 2019

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

CC: Mike McCarthy, Acting Undersecretary for Finance and Administration
Greg Bettwy, Chief of Staff
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Joan Mockeridge, Office of Inspector General
Chuck Mitchell, Office of Inspector General
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: Management Response to "Information Security: Smithsonian Needs to Enhance Protection of Sensitive Information"

Thank you for the opportunity to comment on this report. Management concurs with the findings. OCIO developed a remediation plan to resolve the findings from both the 2017 and 2018 [redacted] conducted by the Office of the Inspector General. OCIO has treated implementation of the plan as a high priority. [redacted] actions in the plan have now been completed [redacted]

Page 1