Smithsonian Institution **Memo**
Office of the Inspector General

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

Date: October 10, 2018

To: Albert Horvath, Chief Operating Officer and Under Secretary for Finance and Administration (OUSFA)

Cc: Mike McCarthy, Deputy Under Secretary for Finance and Administration
Deron Burba, Chief Information Officer
[redacted]
Juliette Sheppard, Director of Information Technology Security, Office of the Chief Information Officer
[redacted]

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

Subject: Actions Needed to Enhance Protection of Sensitive Information (OIG-A-19-01)

In fiscal year 2017, federal agencies reported more than 35,000 cybersecurity incidents, a 14 percent increase from the previous year. Such incidents resulted in, among other things, thousands of federal employees and taxpayers having their personal information compromised.[1] According to the Department of Homeland Security, "Cyber threats constantly evolve with increasing intensity and complexity."[2] The prevalence and constant evolution of cybersecurity threats demonstrates the need for, but difficulty of, maintaining effective prevention, detection, and response capabilities.

The Smithsonian Institution's (Smithsonian) Office of the Inspector General (OIG) conducted this performance audit to test the Smithsonian's capabilities to prevent, detect, and respond to information security incidents. The methodology involved [redacted]

[redacted]

[1] Office of Management and Budget, *Federal Information Security Modernization Act of 2014: Fiscal Year 2017 Annual Report to Congress*, (Washington, D.C.).
[2] Department of Homeland Security, *Cybersecurity Questions for CEOs* (Washington, D.C.: February 2013).
[redacted]

[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 includes 19 museums, the National Zoological Park, and nine research centers. Research is conducted in the museums and other facilities throughout the world. In fiscal year 2016, the public made more than 29 million visits to the Smithsonian museums and the zoo, and more than 134 million people visited the Smithsonian's public websites. In addition to federal appropriations, the Smithsonian receives private support, external grants and contracts, income from investments, and income from various business activities. Business activities include Smithsonian magazines and other publications; online catalogs; and entertainment, retail shops, and food services. In February 2018, the Smithsonian announced completion of a fundraising campaign that involved more than 535,000 donors.

The Office of the Chief Information Officer manages the Smithsonian's information security program and technology infrastructure. The Office of Protection Services has overall responsibility for the physical security of the Smithsonian. 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

[5] US-CERT defines a data breach as "The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information."

[redacted]

RESULTS OF THE AUDIT

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

CONCLUSION

[redacted]

RECOMMENDATIONS

1. [redacted]

2. [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 the recommendations that OIG made in its draft report. OIG evaluated management's response and determined that the planned actions address the intent of the recommendations.

Attachment I

MANAGEMENT RESPONSE

Smithsonian Institution Memo

Date: September 21, 2018

To: Cathy L. Helm, Inspector General

From: Albert Horvath, Chief Operating Officer and Under Secretary for Finance and Administration
Deron Burba, Chief Information Officer, Office of Chief Information Officer
[redacted]

Cc: Michael McCarthy, Cindy Zarate, Joan Mockeridge, [redacted] Juliette Sheppard, [redacted]

Subject: Management Response to Office of Inspector General Draft for [redacted]
Actions Needed to Enhance Protection of Sensitive Information

This response is submitted on behalf of the Chief Information Officer (OCIO) and [redacted] Thank you for the opportunity to provide additional context.

1. **Recommendation No. 1.** [redacted]

Management Response: *Management concurs with this recommendation.* [redacted]

2. **Recommendation No. 2.** [redacted]

Management Response: *Management concurs with this recommendation.* [redacted]

PO Box 37012, CC 350, MRC 1200
Washington, DC 20013-7012
202.633.7290 Telephone
202.633.7319 Fax