OFFICE OF THE
INSPECTOR GENERAL
Smithsonian

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).

Memo

~~FOR OFFICIAL USE ONLY~~

Date: October 28, 2021

To: Doug Hall, Acting Under Secretary for Administration
Deron Burba, Chief Information Officer

Cc: Carmen Iannacone, Chief Technology Officer, Office of the Chief Information Officer (OCIO)
Juliette Sheppard, Director of Information Technology Security, OCIO

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

Subject: Information Security: Smithsonian Needs to Further Improve [redacted] (OIG-A-22-01)

Information technology 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 about $3.9 million; this study also found that organizations with formal incident response procedures experience lower data breach costs than organizations without such procedures.[1]

During summer 2020, the Smithsonian Institution's (the Smithsonian) [redacted][2] [redacted] In addition, although staff from the Smithsonian Office of the Chief Information Officer (OCIO) [redacted]

[redacted]

[1] Ponemon Institute LLC, *2020 Cost of a Data Breach Report* (Michigan: Ponemon Institute LLC, 2020).

[2] [redacted]

~~IMPORTANT NOTICE: This report is solely for the official use of the Smithsonian officials and stakeholders on a need-to-know basis to perform their duties. OIG will determine public availability of the document under Smithsonian Directive 807, *Requests for Smithsonian Institution Information*.~~

[redacted].[3] [redacted] (For the objective, scope, and methodology of this audit, see Appendix I.)

[redacted] see Table 1.

[redacted]

[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

BACKGROUND

The Smithsonian depends on information technology systems to carry out its programs and operations and to process essential data. But the risks to these systems are increasing—including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks. Rapid developments in new technologies, such as artificial intelligence, the Internet of Things, and ubiquitous Internet and cellular connectivity, can also introduce security issues. Additionally, because some information technology systems contain PII, the Smithsonian must protect the confidentiality, integrity, and availability of this information—and effectively respond to data breaches and security incidents.

[3] [redacted]

The Chief Information Officer is the senior official responsible for the Smithsonian's information systems and is the primary sponsor for the Information Technology Security Program. [redacted]

[redacted]

RESULTS OF THE AUDIT

[redacted] [5] [redacted]

[redacted]

[redacted]

[4] [redacted]

[5] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[6] [redacted]

[redacted]

[redacted].[7] [redacted]

[redacted]

[redacted]

[redacted][8] [redacted]

[7] [redacted]

[8] [redacted]

~~IMPORTANT NOTICE: This report is solely for the official use of the Smithsonian officials and stakeholders on a need-to-know basis to perform their duties. OIG will determine public availability of the document under Smithsonian Directive 807, *Requests for Smithsonian Institution Information.*~~

[redacted]

RECENT ACTIONS TAKEN

After an interim briefing on the results of [redacted] OCIO took the following actions:

- [redacted]
- [redacted].[9]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[9] [redacted]

CONCLUSION

The Smithsonian depends on information technology systems to carry out its programs and operations and to process essential data. In addition, the Smithsonian must protect the confidentiality, integrity, and availability of the sensitive personally identifiable information on some systems. Having effective information security controls can help to prevent, detect, and respond to security incidents.

[redacted]

In response to the findings in this report, OCIO took actions [redacted] Therefore, we are not making any recommendations.

MANAGEMENT RESPONSE AND OIG EVALUATION

OIG provided a draft of this report to Smithsonian management for review and comment. They provided written comments and concurred with our findings, which are found in Attachment I.

Appendix I

Objective, Scope, and Methodology

[redacted][10][redacted], [11] [redacted][12] [redacted]

[redacted]

[10] [redacted]

[11] [redacted]

[12] [redacted]

~~IMPORTANT NOTICE: This report is solely for the official use of the Smithsonian officials and stakeholders on a need-to-know basis to perform their duties. OIG will determine public availability of the document under Smithsonian Directive 807, *Requests for Smithsonian Institution Information.*~~

Table 2. Internal Control Components and Principles Significant to the Audit Objective

Control Activity Principles
• **Management should design control activities to achieve objectives and respond to risks.**
• **Management should design the entity's information system and related control activities to achieve objectives and respond to risks.**
• **Management should implement control activities through policies.**
Monitoring Principles
• **Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.**
• **Management should remediate identified internal control deficiencies on a timely basis.**

Source: OIG analysis.

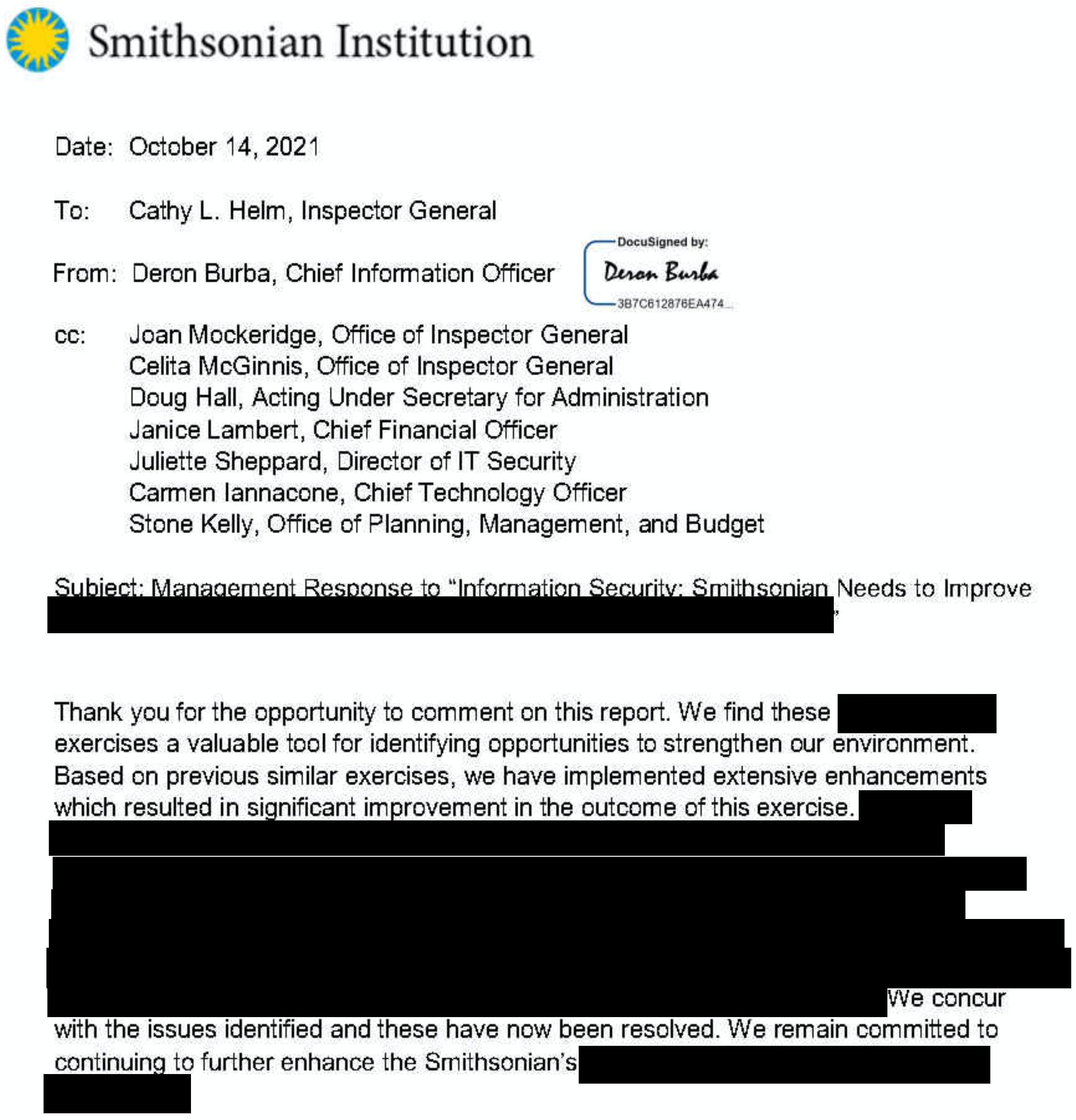
OIG conducted this performance audit in Washington, D.C., from June 2020 through October 2021 in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its 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.

~~IMPORTANT NOTICE: This report is solely for the official use of the Smithsonian officials and stakeholders on a need-to-know basis to perform their duties. OIG will determine public availability of the document under Smithsonian Directive 807, *Requests for Smithsonian Institution Information.*~~

~~FOR OFFICIAL USE ONLY~~

Attachment I

Management Response



Smithsonian Institution

Date: October 14, 2021

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

DocuSigned by:
Deron Burba
3B7C612876EA474...

cc: Joan Mockeridge, Office of Inspector General
Celita McGinnis, Office of Inspector General
Doug Hall, Acting Under Secretary for Administration
Janice Lambert, Chief Financial Officer
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Stone Kelly, Office of Planning, Management, and Budget

Subject: Management Response to "Information Security: Smithsonian Needs to Improve [redacted],"

Thank you for the opportunity to comment on this report. We find these [redacted] exercises a valuable tool for identifying opportunities to strengthen our environment. Based on previous similar exercises, we have implemented extensive enhancements which resulted in significant improvement in the outcome of this exercise. [redacted] We concur with the issues identified and these have now been resolved. We remain committed to continuing to further enhance the Smithsonian's [redacted]

~~IMPORTANT NOTICE: This report is solely for the official use of the Smithsonian officials and stakeholders on a need-to-know basis to perform their duties. OIG will determine public availability of the document under Smithsonian Directive 807, *Requests for Smithsonian Institution Information.*~~