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

SENSITIVE INFORMATION

Date: March 31, 2023

To: Ron Cortez, Under Secretary for Administration
Deron Burba, Chief Information Officer

Cc: 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

Subject: Information Security: Enhancements Needed to Improve [redacted] (OIG-A-23-05)

Information technology security is a top risk for organizations. The Smithsonian depends on IT 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, [redacted] For additional background information, see Attachment I.

OIG conducted this audit to assess the effectiveness of Smithsonian's information technology (IT) [redacted] The methodology involved using an [redacted] For a detailed description of OIG's objectives, scope, and methodology, see Attachment II.

[1] [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*~~.

Results of the Audit

During summer 2021, [redacted]

[redacted]

Table 1. [redacted]

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

Source: OIG analysis.

[redacted]

[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]

[redacted]

[redacted]

- [redacted]

- [redacted]

  [redacted]

[3] [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]

- [redacted]

  [redacted]

- [redacted]

  [redacted]

[redacted]

[4] OCIO Technote [redacted]

[5] [redacted]

[6] OCIO Technical Note [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[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]

[redacted]

[redacted]

[redacted]

[redacted]

Recent Management Action

In response to issues identified in this audit OCIO took the following actions:

- [redacted]
- [redacted]
- [redacted]

Conclusions

The Smithsonian depends on IT systems to carry out its programs and operations and to process essential data. [redacted]

Recommendations

To mitigate the risks associated [redacted] the Chief Information Officer should take the following actions:

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]

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 III.

Attachment I

Background

To protect its information, Smithsonian uses [redacted] OCIO has established [redacted]

[redacted] is a long-standing problem and a growing national security threat. According to one estimate they accounted for almost [redacted] in 2022.[9] In addition, it has been reported that [redacted][0] [redacted][1] The most common way that [redacted][2]

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

[redacted]

[redacted]

[9] [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*.~~

Attachment II

Objective, Scope, and Methodology

OIG conducted this audit to assess the effectiveness of Smithsonian's information technology (IT) [redacted] The methodology involved using an [redacted]

In planning and performing this audit, OIG identified two internal control components (control activity and monitoring) and five underlying principles as significant to the audit objective, as shown in Table 2. OIG assessed the design, implementation, and operating effectiveness of the internal controls significant to the audit objective.

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.

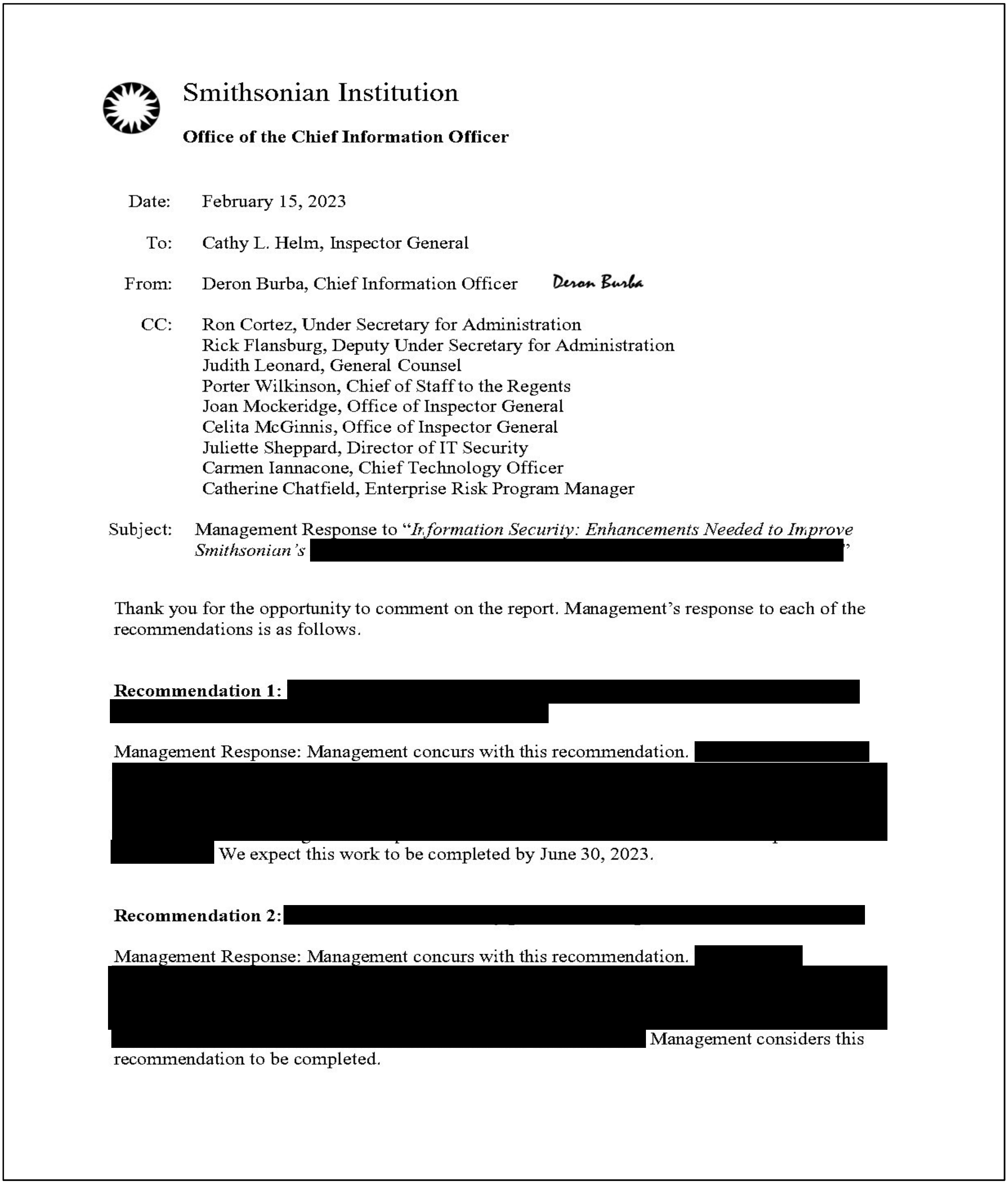
Source: OIG analysis.

OIG conducted this performance audit in Washington, D.C., from June 2021 through March 2023 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.

[13] [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*.~~

Attachment III



Smithsonian Institution

Office of the Chief Information Officer

Date: February 15, 2023

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer Deron Burba

CC: Ron Cortez, Under Secretary for Administration
Rick Flansburg, Deputy Under Secretary for Administration
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Joan Mockeridge, Office of Inspector General
Celita McGinnis, Office of Inspector General
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Catherine Chatfield, Enterprise Risk Program Manager

Subject: Management Response to "*Information Security: Enhancements Needed to Improve Smithsonian's* [redacted]"

Thank you for the opportunity to comment on the report. Management's response to each of the recommendations is as follows.

Recommendation 1: [redacted]

Management Response: Management concurs with this recommendation. [redacted] We expect this work to be completed by June 30, 2023.

Recommendation 2: [redacted]

Management Response: Management concurs with this recommendation. [redacted] Management considers this recommendation to be completed.

~~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.*~~

Recommendation 3: [redacted]

Management Response: Management concurs with this recommendation. [redacted] Management considers this recommendation to be completed.

Recommendation 4: [redacted]

Management Response: Management concurs with this recommendation. [redacted] We expect this work to be completed by April 30, 2023.