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) Office of the Chief Information Officer (OCIO) ²

In addition, although staff from the Smithsonian OCIO


2
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.

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

Table 1.
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.

RESULTS OF THE AUDIT
RECENT ACTIONS TAKEN

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

• [redacted]

• [redacted]

• [redacted]

• [redacted]

• [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.

In response to the findings in this report, OCIO took actions 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.
Table 2. Internal Control Components and Principles Significant to the Audit Objective

<table>
<thead>
<tr>
<th>Control Activity Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Management should design control activities to achieve objectives and respond to risks.</td>
</tr>
<tr>
<td>• Management should design the entity’s information system and related control activities to</td>
</tr>
<tr>
<td>achieve objectives and respond to risks.</td>
</tr>
<tr>
<td>• Management should implement control activities through policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Management should establish and operate monitoring activities to monitor the internal control</td>
</tr>
<tr>
<td>system and evaluate the results.</td>
</tr>
<tr>
<td>• Management should remediate identified internal control deficiencies on a timely basis.</td>
</tr>
</tbody>
</table>

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.
Management Response

Date: October 14, 2021

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

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 Iannaccone, Chief Technology Officer
    Stone Kelly, Office of Planning, Management, and Budget

Subject: Management Response to "Information Security: Smithsonian Needs to Improve"

Thank you for the opportunity to comment on this report. We find these 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. We concur with the issues identified and these have now been resolved. We remain committed to continuing to further enhance the Smithsonian's...