OFFICE OF THE
INSPECTOR GENERAL

Smithsonian

Memo

FOR OFFICIAL USE ONLY

Date: September 26, 2024

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: Nicole L. Angarella, Inspector General

Subject: Information Security: Smithsonian Needs to Improve Its Security Incident Prevention, Detection, and Response Capabilities (OIG-A-24-09)

In 2023, [redacted] was the most popular method used by attackers to gain initial access to networks—about 80 to 95 percent of breach attacks.[1] OIG conducted this audit to assess the effectiveness of the Smithsonian Institution's (Smithsonian) information technology (IT) security capability in preventing, detecting, and responding to an attack. The methodology involved using an IT security company (OIG contractor) to simulate a real-life adversary attempting to breach the Smithsonian's computer network to access sensitive information. Smithsonian staff did not have advance notice of this test except for two senior-level managers. OIG specified one primary and two secondary goals for the OIG contractor to pursue within 4 weeks. The primary goal was to access the internal network through external attacks. The secondary goals were to (1) demonstrate the ability to distribute ransomware to the environment (privileged access) and (2) obtain access to Endpoint Detection and Response (EDR) management.[2] The OIG contractor gained access to the Smithsonian's network without advanced knowledge of Smithsonian systems. For additional background information, see Attachment I. For a detailed description of OIG's objectives, scope, and methodology, see Attachment II.

RESULTS OF THE AUDIT

During early 2023, the OIG contractor began the staged attack by conducting online research to identify staff member information such as names, roles, login information, and phone numbers. The contractor then carried out multiple social engineering attacks using the information collected from the staff members. The OIG contractor used [redacted] to deliver malware that, once signed, provided the OIG

[1] Comcast Business, 2023 Comcast Business Cybersecurity Threat Report, https://business.comcast.com/community/browse-all/details/2023-comcast-business-cybersecurity-threat-report

[2] EDR management tools are used to identify suspicious activity on laptops desktop, servers, etc.

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*.

contractor with access to the users' devices. This access enabled them to identify the names of Smithsonian domains and servers. Next, the OIG contractor attempted to add a new computer to one of the Smithsonian's [redacted] domains; however, the incident response staff of the Office of the Chief Information Officer (OCIO) detected the OIG contractor and ultimately terminated their access.

Using a [redacted] campaign, the OIG contractor was able to gain access to the Smithsonian's [redacted] environment. This enabled the OIG contractor to identify [redacted] and obtain access to more than 400 Smithsonian [redacted] servers. OCIO's incident response staff did not identify this breach; therefore, the OIG contractor's access to the [redacted] environment was left intact.

In the [redacted] environment, OCIO detected the OIG contractor's staged attack. However, OIG determined that OCIO could have better mitigated the risks associated with insufficient detection and response capabilities in its [redacted] environment. In addition, OIG determined that OCIO could better mitigate risks associated with the availability of [redacted] on the network. The OIG contractor met the primary goals established for this audit but did not meet the two secondary goals, as shown in Table 1.

Table 1: Primary and Secondary Goals for the OIG Contractor's Simulated Attack and Whether They Were Met

Type and Description of Goal	Did the OIG Contractor Meet the Goal?
Primary Goal	
Access the internal network through external attacks	Yes
Secondary Goals	
Demonstrate the ability to distribute ransomware to the environment (privileged access)	No
Obtain access to EDR management	No

Source: OIG analysis.

OCIO Detected the OIG Contractor's Staged Attack on the [redacted] Environment but not on the [redacted] Environment

In early 2023, the OIG contractor, without any advanced knowledge of Smithsonian systems, used various attack methods, such as [redacted] and [redacted] campaigns, to capture credentials and access the Smithsonian's [redacted] and [redacted] environments. [redacted] is the use of social engineering, such as using emails and [redacted] to persuade people to reveal information. [redacted] is another form of [redacted] using [redacted] Although OCIO detected and removed the OIG contractor from the [redacted] environment, the OIG contractor maintained its [redacted] connection.

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.*

During the engagement, the Smithsonian IT security team identified malicious behavior originating from [redacted] servers in the network and provided evidence that they had identified suspicious activity before the OIG notification. Specifically, OCIO identified that a computer had been added to the network without the staff member's knowledge and removed the computer immediately.

[redacted] *Configuration Could be Improved*

OCIO's configuration for [redacted] was vulnerable to the [redacted] configuration. The [redacted] configuration enabled the OIG contractor to perform a privileged escalation attack that targeted this [redacted] environment. The OIG contractor escalated its privileges from a low-level [redacted] to [redacted] access. They then exploited this [redacted] environment. Although the OIG contractor was able to escalate their privileges, OCIO did identify the suspicious activity generated by this compromised account. Nevertheless, OCIO is still reviewing the [redacted] configuration that enabled this to happen. In June 2024, OCIO staff said that they were addressing this vulnerability.

Insufficient Configurations of the [redacted] Environment

OCIO could improve its configuration of the [redacted] systems to prevent the OIG contractor from gaining access, escalating privileges, and using them as a base of operations for follow-on attacks. The OIG contractor used [redacted] to orchestrate attacks in the [redacted] environment.[3] They also identified several gaps in [redacted] configurations, such as [redacted] OCIO configured Smithsonian's [redacted] environment using the recommended [redacted] However, the Smithsonian security team did not detect the OIG contractor's access to the [redacted] servers, enabling them to access data and conduct other exploitation operations without detection.

In addition, the Security Operations Center (SOC) team stated that the [redacted] team changed the [redacted] for the accounts that the OIG contractor exploited. The SOC team said that OCIO also was taking the following actions:

- establishing [redacted] audit logs to enhance monitoring of servers,
- evaluating a new tool to support central account administration and monitoring, and
- creating tasks to address hardening and monitoring of the [redacted] environment.

[3] An IP address identifies devices connected to the internet. This enables computers and other internet-connected devices, such as laptops, to communicate.
[4] The [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.*

Insufficient system hardening can hinder the effectiveness of security operations, providing an attacker with less risk of detection and the ability to escalate privileges.[5] Therefore, the OIG contractor was able to reside within the [redacted] environment, avoid eviction, and achieve their attack objectives.

OCIO Allows the Storage of [redacted]

The OIG contractor found two [redacted] stored within the Smithsonian's [redacted] environment, and, after notification, OCIO removed these [redacted] from the system. [redacted]

Smithsonian Directive 931, *Use of Computers, Telecommunications Devices, and Networks,* states that users must protect data from loss, misuse, modification, and unauthorized access. This includes [redacted] In addition, [redacted] OCIO Technical Note IT-930-TN37, *Securing IT Accounts*, states that personnel must take reasonable precautions to avoid exposing their account information. In addition, any documented [redacted] must be encrypted when stored electronically. Nevertheless, the OIG contractor still found [redacted] stored in local file systems.

Storing [redacted] offers attackers easy lateral movement and privilege escalation options to other systems and the wider [redacted] domain.

Smithsonian Staff [redacted]

The OIG contractor searched online for information about Smithsonian people, processes, and technology and created a list of employees to target for social engineering campaigns. In addition, Smithsonian usernames, passwords, and domain information were shared in [redacted] public repository.

Smithsonian Staff is [redacted]

[redacted]

[redacted]

[5] Hardening is the process of eliminating a means of attack by patching vulnerabilities and turning off nonessential services.

[6] Two staff members were targeted in both the [redacted] and [redacted] campaigns.

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]

The OCIO security team identified some security incidents but did not determine the full scope and extent of the breach. OCIO provided evidence that they detected malicious activity on [redacted]

OCIO's IT security staff took additional steps to educate users who fell victim to [redacted] For example, in February 2023, OCIO included an article, "Beware of Malicious [redacted]" in the IT Security Awareness Newsletter. It included a tip sheet and video link on how [redacted] via [redacted] works. OCIO hired a training staff member dedicated to improving the Smithsonian's IT security program. This staff member is responsible for improving awareness, including providing one-on-one training to users who fall victim to cyberattacks.

OCIO Technical Standard and Guideline IT-930-05, *Computer Security Training and Awareness,* provides Smithsonian IT training requirements. OCIO uses Computer Security Awareness Training, IT Awareness newsletters, and [redacted] exercises to develop awareness of identifying suspicious messages. OIG understands that social engineering attacks are becoming more sophisticated and more difficult to identify, and that people will always be susceptible to social engineering and [redacted] attempts.

Smithsonian Information was Disclosed in the [redacted]

The OIG contractor identified data such as [redacted][7] Initially, the OIG contractor shared a sample of four [redacted] and OCIO promptly deleted them. After further review, OIG found a list of [redacted] and shared the list with OCIO. The OCIO SOC team stated that the SOC developer and [redacted] administrators are working through the list.

[7] Programming source code is a set of instructions in a computer language.

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.*

Although any one piece of information may not be useful, an attacker could combine some or all of the pieces to inform more complex attacks—[redacted]

RECENT MANAGEMENT ACTIONS

After OIG brought these issues to OCIO's attention, OCIO took the following actions:

- To remediate the vulnerability of [redacted] to the [redacted] configuration OCIO [redacted] as recommended by [redacted] A [redacted] The [redacted] provides admins and users a way to view, install and remove [redacted] on devices. Therefore, we will close recommendation one as of the date of this report.

- To address the risk of Smithsonian staff [redacted] OCIO submitted changes to the CSAT training vendor for the FY 2025 CSAT course. A bullet point was added informing staff that they should never electronically store unencrypted passwords. Furthermore, a change was made to clarify that staff should not automatically trust an email from a SI address or trusted third party such as [redacted] These changes are expected to be implemented prior to the beginning of the FY 2025 training cycle (October 1, 2024). OCIO also discussed the use of [redacted] and other attack vectors for [redacted] attacks in IT Notice emails and IT Security Awareness Newsletters which are distributed Institution wide. Therefore, in October 2024 we will verify that these changes have been implanted and will close the recommendation at that time.

CONCLUSION

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

The Smithsonian uses [redacted] to enable staff access to a wide range of IT systems. The Smithsonian's [redacted] is more widely used by staff; therefore, OCIO has dedicated more resources to its configuration and auditing capabilities. As a result, OCIO detected and removed the OIG contractor from the [redacted] environment during this engagement. However, [redacted] of Smithsonian [redacted] systems enabled the OIG contractor to access these systems, escalate their privileges, and use them as a base of

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.*

operations for follow-on attacks. Establishing more effective [redacted] configuration settings and auditing capabilities for the Smithsonian's [redacted] environment can help facilitate the management of risk to those IT systems as well.

Smithsonian's policy requires users to secure [redacted] however, OCIO has configured the [redacted] environment in a way that allows the storage of [redacted] Securing [redacted] protects data from loss, misuse, modification, and unauthorized access.

The vast majority of cyber incidents begin with [redacted] like those used by the OIG contractor, which [redacted] Any one piece of data found online about an organization may not be useful; however, an attacker could combine some or all of the data to create more believable [redacted] or to begin building a picture of an organization's internal network. Smithsonian [redacted] in [redacted] If [redacted] are necessary, access to shared data should be made private to reduce the likelihood of secret exposure to unintended parties. Because the attack was simulated, no sensitive data were released outside the Smithsonian.

RECOMMENDATIONS

To strengthen security controls, OIG recommends that the Chief Information Officer take the following actions:

1. Develop and Implement a plan to mitigate the risk caused by the [redacted] vulnerability.

2. Finalize and implement additional [redacted] to decrease the risk of exploitation of the network caused by [redacted]

3. Develop and implement a procedure to enforce Smithsonian policy disallowing the [redacted].

4. Update the computer security awareness training to include additional communication channels and mechanisms for [redacted]

5. Identify and remove [redacted] such as [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.*

FOR OFFICIAL USE ONLY

MANAGEMENT RESPONSE AND OIG EVALUATION

OIG provided the Smithsonian a draft of this report for review and comment, and Smithsonian management provided written comments, which are reproduced in their entirety in Attachment III. In its written comments, management concurred with all of the recommendations and outlined actions planned to address them.

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 I

BACKGROUND

The Chief Information Officer (CIO) is the senior executive responsible for the Smithsonian's information systems. The CIO serves as the primary program sponsor for the Smithsonian's Information Technology Security Program and ensures compliance with all Smithsonian IT security policies and procedures. The Director of Information Technology oversees the selection and assessment of security controls in Smithsonian IT systems, oversees the implementation and operation of common security controls, and tracks IT security control weaknesses and remediation efforts across the Smithsonian enterprise. The Data Center Operations & Network Server Administration Division is responsible for establishing and maintaining operating system baselines and patching.

The Information Technology Security staff maintains the Smithsonian-owned security infrastructure, performs vulnerability scanning, and audits all controls on an ongoing basis. They are responsible for enforcing compliance and determining appropriate enforcement action, including removing non-compliant [redacted] servers from the network. Also, they manage the [redacted] logging application.

Criteria

Smithsonian SD 931, *Use of Computers, Telecommunication Devices, and Networks,* provides the rules for using Smithsonian computers, telecommunication devices, and networks appropriately, and the user's role in protecting these resources from unauthorized use.

OCIO Technical Standard and Guideline IT-930-05, *Computer Security Training and Awareness,* provides the Smithsonian's IT training requirements.

OCIO Technical Note IT-930-TN37, *Securing IT Accounts*, establishes policy for securing accounts and privileges for access to Smithsonian IT systems.

Executive Order No. 14028, 86 F.R. 26633 (2021) requires federal agencies to advance toward a Zero Trust Architecture. The Smithsonian is not required to comply with this Executive Order because it is not an executive branch agency; however, the Smithsonian is taking steps to apply zero trust policies to its information security program as a best practice to the extent practicable and consistent with its mission.

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 the Smithsonian's IT security capability in preventing, detecting, and responding to an attack. The methodology involved [redacted] Smithsonian staff did not have advance notice of this test except for two senior-level managers. OIG specified one primary goal and two secondary goals for the OIG contractor to pursue within 4 weeks. The primary goal was to access the internal network through external attacks. The secondary goals were to (1) demonstrate the ability to distribute ransomware to the environment (privileged access) and (2) obtain access to Endpoint Detection and Response (EDR) management.[8] The OIG contractor conducted its work from January 23, 2023, through February 23, 2023. They met the primary goal but did not meet the secondary goals. When the OIG contractor completed its work, OIG compared its results with the Smithsonian's response to determine if the Smithsonian's security controls and processes could prevent, detect, and respond to the simulated attack.

In planning and performing this audit, we identified two internal control components and five underlying principles that were significant to the audit objectives, as shown in Table 2.

Table 2: Internal Control Components and Principles Significant to the Audit Objectives

Control Activities 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.

We conducted our audit from January 2023 through September 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on our audit objectives.

[8] EDR management tools are used to identify suspicious activity on laptops desktop, servers, etc.

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: August 30, 2024

To: Nicole Angarella, Inspector General

From: Deron Burba, Chief Information Officer

DocuSigned by:
Deron Burba
3B7C612876EA474...

CC: Joan Mockeridge, Assistant Inspector General for Audits
Celita McGinnis, Office of Inspector General
Meroe Park, Deputy Secretary and Chief Operating Officer
Greg Bettwy, Chief of Staff
Ron Cortez, Under Secretary for Finance and Administration / Chief Financial Officer
Jennifer McIntyre, Chief Legal Officer
Porter Wilkinson, Chief of Staff to the Regents
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Catherine Chatfield, Enterprise Risk Program Manager

Subject: Management Response to "*Information Security: Smithsonian Needs to Improve Its Security Incident Prevention, Detection, and Response Capabilities*"

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

Recommendation 1: Develop and Implement a plan to mitigate the risk caused by the [redacted] vulnerability.

Management Response: Management concurs with this recommendation. We have enabled the [redacted] requirement on the [redacted] to mitigate the risk. Management considers this recommendation completed.

Recommendation 2: Finalize and implement additional [redacted] to decrease the risk of exploitation of the network caused by [redacted]

Management Response: Management concurs with this recommendation. We performed an audit of all [redacted] that didn't adhere to our policies. [redacted] We also enabled [redacted] starting with [redacted]. [redacted] Additionally, we are implementing [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]. We expect this work to be completed by February 28, 2025.

Recommendation 3: Develop and implement a procedure to enforce Smithsonian policy disallowing the [redacted].

Management Response: Management concurs with this recommendation. We will develop and implement a process to [redacted]. We will investigate potential policy violations and remediate [redacted]. We expect this work to be completed by August 31, 2025.

Recommendation 4: Update the computer security awareness training to include additional communication channels and mechanisms for [redacted].

Management Response: Management concurs with this recommendation. While the training (including CSAT, newsletters, and other awareness materials) already covers [redacted] and other channels, we have added additional content including specific mention of [redacted] to the course for FY 2025 and have included additional content about [redacted] and other channels in the security awareness newsletter and other communications. Additionally, [redacted] and related topics have been added to custom outreach training. Management considers this recommendation completed.

Recommendation 5: Identify and remove [redacted], such as [redacted].

Management Response: Management concurs with this recommendation. We will implement a process to remove [redacted]. We expect this work to be completed by August 31, 2025.

We appreciate the opportunity to learn from this audit and your assistance in identifying opportunities to enhance the security of our computing environment.

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.*

OFFICE OF THE INSPECTOR GENERAL

Smithsonian

OIG's Mission	Our mission is to promote the efficiency, effectiveness, and integrity of the Smithsonian Institution's programs and operations through independent and objective audits and investigations and to keep stakeholders fully and currently informed.
Reporting Fraud, Waste, and Abuse to OIG Hotline	OIG investigates allegations of waste, fraud, abuse, gross mismanagement, employee and contractor misconduct, and criminal and civil violations of law that have an impact on Smithsonian Institution programs and operations. If requested, anonymity is assured to the extent permitted by law. Although you may remain anonymous, we encourage you to provide us with your contact information. The ability to gather additional information from you may be the key to effectively pursuing your allegation. To report fraud and other serious problems, abuses, and deficiencies, you can do one of the following: Call 202-252-0321. Send an email to: oighotline@oig.si.edu. Visit OIG's website: https://www.si.edu/oig. Write to: Office of the Inspector General Smithsonian Institution P.O. Box 37012, MRC 524 Washington, D.C. 20013-7012.
Obtaining Copies of Reports	To obtain copies of our reports, go to OIG's website: https://www.si.edu/oig or the Council of the Inspectors General on Integrity and Efficiency's website: https://oversight.gov.