Smithsonian Institution
Office of the Inspector General

August 9, 2016

Via Electronic Transmission

Congressional Addressees:

Pursuant to the section 406 of the Cybersecurity Act of 2015 (Act), we are submitting the following information regarding the Smithsonian Institution's (Smithsonian) logical access controls and data security management practices. Section 406 requires that the Inspector General of each covered agency submit a report on such practices as they relate to covered systems.[1] A covered system is a national security system or a federal computer system that provides access to personally identifiable information (PII). A covered agency is an agency that operates a covered system.

As part of its information security program, the Smithsonian has identified 17 systems for Federal Information Security Management Act (FISMA) reporting that support a wide range of functions such as collections management, physical security, enterprise resource planning, and fundraising.[2] All 17 systems are categorized as moderate or low using the Federal Information Processing Standards (FIPS) 199 methodology. Examples of moderate data types include donor information, employee records, employee and customer financial accounts, and Smithsonian financial information. Since controls related to the 17 systems are defined by a central policy, this report covers all of them, regardless of the sensitivity of their data.

The following information describes the Smithsonian's policies, procedures, and system security plans. The Office of the Inspector General's (OIG) review of these documents consisted of identifying the requested information within the policies and procedures and then verifying that the controls were in place per the system security plan.[3] While OIG did not verify the effectiveness of the controls

---

[1] Smithsonian management does not believe that Section 406 applies to the Smithsonian because, in its view, the Smithsonian is not a covered agency. However, the OIG is submitting this report because the OIG believes that Section 406 may apply to the Smithsonian.

[2] The Smithsonian excludes from its FISMA program other systems, such as those run by the profit-generating Smithsonian Enterprises.

[3] The specific documents reviewed were Smithsonian Directive 920, *IT Life Cycle Management*; Technical Standards and Guidelines (TSG) IT-930-01, *Automated Information System Security Planning*; TSG IT-930-02, *Security Controls Manual*; TSG IT-930-TN37, *Securing IT Accounts*; and the system security plans for each of the 17 FISMA systems.

MRC 524
PO Box 37012
Washington DC 20013-7012
202.633.7050 Telephone
202.633.7079 Fax

through detailed testing, such testing is performed each year during the FISMA review.[4]

A. A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

i. Logical Access Controls

The Act defines logical access controls as "a process of granting or denying specific requests to obtain and use information and related information processing services." By policy, the Smithsonian has adopted controls from the National Institute of Standards and Technology Special Publication 800-53,[5] which is considered the baseline for non-national security systems. The Smithsonian's policies describe a variety of logical access controls as selected from that standard.

The primary method of controlling access to the Smithsonian's information systems is through username and password, which is present across all systems. User names are uniquely identifiable to an individual, with group and temporary accounts used only when specifically authorized. Passwords are enhanced by complexity requirements, which assist the user in selecting a strong password. Users are required to periodically change the password to guard against compromise and to ensure they are always using the most up-to-date complexity requirements. Individual systems store passwords in a secure manner using approved cryptographic modules.

The Smithsonian further limits each user's actions within the system based on his or her job responsibilities. Policies and procedures require that access be properly approved before being granted. Additionally, care is taken to separate actions that could allow the user to perform an entire transaction without oversight. This is known as separation of duties.

Each system's information technology (IT) representative is required to monitor accounts and determine if changes in access are necessary or if unauthorized access occurs. The representative should monitor for accounts that have not accessed the system in the last 90 days and for accounts related to individuals who have terminated employment or transferred departments. In addition,

---

[4] Smithsonian OIG, *Fiscal Year 2014 Independent Evaluation of the Smithsonian Institution's Information Security Program*, OIG-A-16-02, (Washington, D.C.: Dec 17, 2015).

[5] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Revision 4, (Washington, D.C.: April 2013)

systems should be configured to lock accounts after excessive login failures, which secures an account against repeated password guessing.

The Smithsonian also requires flow control to manage the data flow between systems. Flow control is the process of managing data traffic both within a system and between systems. The Smithsonian achieves flow control primarily through firewalls, which block network traffic unless specifically allowed. This allows the Smithsonian to partition the network infrastructure to protect critical systems. For example, users in publicly accessible areas are blocked from accessing internal business systems.

Three additional areas are centrally controlled by Smithsonian staff. First is the use of wireless access. By policy, connection of wireless access points to the Smithsonian network must be authorized and have a secure configuration that encrypts network traffic. Second is the central management of mobile devices. Mobile devices are required to have a secure configuration and enroll in centralized management tools, which allow remote data deletion if the mobile device is lost or stolen. Third is remote access, which is further discussed below under multifactor access controls.

ii. Multifactor Access Controls

Smithsonian policies and procedures do not broadly require multifactor access controls for systems. Almost all systems are accessed by using a single-factor username and password. With respect to the Act, this is classified as something the user knows.

The one exception is remote access. For a user to gain remote access to internal systems, he or she must use one of two authorized remote access systems. In both cases, a username and password is required, along with a personal identification number (PIN) number from a token. The token is something the user physically possesses, and thus this provides a second authentication factor. Smithsonian management is considering broader deployment of multifactor access controls but does not currently have an actionable plan backed by funding.

B. A description and list of the logical access controls and multifactor authentication used by the covered agency to govern access to covered systems by privileged users.

Privileged user access follows the same basic logical access controls as described above. While the type of access control does not vary, the underlying policy requirements differ somewhat from the standard controls. There are two main differences. First, privileged user accounts must have a longer password. Additional length requirements vary but are up to double the standard length requirement. The second difference is in how the accounts may be used. Policy

dictates that privileged accounts should not be used for day-to-day access. Instead, the account should only be used when such privilege levels are needed (e.g., for installing software). Although required by policy, this restriction is not enforced through automated controls.

C. If the covered agency does not use logical access controls or multifactor authentication to access a covered system, a description of the reasons for not using such logical access controls or multifactor authentication.

See appendix A for an explanation provided by the Smithsonian's Office of the Chief Information Officer.

D. A description of the following information security management practices used by the covered agency regarding covered systems:

> *i. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.*

The Smithsonian employs two methods of managing software inventory and licensing. First, by policy, the ability to install software (i.e., administrator access) is restricted to a subset of users that require this access for their job responsibilities. This allows designated IT support staff to monitor and verify that software is approved prior to installation. Second, the Smithsonian maintains a centrally approved list of allowed software. This allows the administrator to verify that software is authorized. In both cases, these controls are designed to prevent unauthorized and unlicensed software from entering the Smithsonian. Additional controls to monitor software after installation are limited.

While the Smithsonian has several centralized monitoring tools in place that are capable of tracking inventory and licensing, it has not yet incorporated the tools into day-to-day operations. There are some instances of centralized license tracking, but deployment varies across systems and is isolated to a small number of applications. In July 2016, the Smithsonian purchased an application to unify the existing monitoring tools and is working to incorporate it into their operations for ongoing monitoring and remediation.

> *ii. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including*
> *(I) data loss prevention capabilities;*
> *(II) forensics and visibility capabilities; or*
> *(III) digital rights management capabilities.*

None. The Smithsonian does not currently monitor for data exfiltration nor does it use data loss prevention or digital rights management tools.

> *iii. A description of how the covered agency is using the capabilities described in clause (ii).*

Not applicable, see above.

> *iv. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.*

See appendix A for an explanation provided by the Smithsonian's Office of the Chief Information Officer.

E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

The IT Life Cycle Management policy requires verification of contractor controls as part of the Smithsonian's system tailoring process. This process allows security staff to tailor security requirements to the needs of the system, which must be in place and verified before a system can enter production. Contractor systems and internally developed systems are treated the same way, with specific control requirements that are verified by security assessors. The same process is followed for both new and significantly changed systems. This process does not specifically call out data security management practices, but they would be considered based on the needs of the system.

For contractors that are performing services, rather than providing systems, there are two ways of ensuring data security management practices. First, policy requires that each contractor take computer security awareness training prior to being granted a user account. This provides a contractor with a basic foundation about applicable Smithsonian requirements related to computer security. Second, standard language about data security management practices is required to be inserted into contracts to ensure responsibilities are documented and communicated.

If you have any additional questions, please do not hesitate to call Epin Christensen, Counsel, at 202-633-7050.

Sincerely yours,

Cathy L. Helm

Cathy L. Helm
Inspector General

List of Addressees

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Roy Blunt
Chairman
The Honorable Charles E. Schumer
Ranking Member
Committee on Rules and Administration
United States Senate

The Honorable Candice Miller
Chairman
The Honorable Robert Brady
Ranking Member
Committee on House Administration
House of Representatives

The Honorable Lisa Murkowski
Chairman
The Honorable Tom Udall
Ranking Member
Subcommittee on Interior, Environment, and Related Agencies
Committee on Appropriations
United States Senate

The Honorable Ken Calvert
Chairman
The Honorable Betty McCollum
Ranking Member
Subcommittee on Interior, Environment, and Related Agencies
Committee on Appropriations
House of Representatives

The Honorable Lou Barletta
Chairman
The Honorable André Carson
Ranking Member
Subcommittee on Economic Development, Public Buildings and Emergency Management
Committee on Transportation and Infrastructure
House of Representatives

Smithsonian Institution

Appendix A

Office of the Chief Information Officer

Date: August 1, 2016

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

Cc: Al Horvath, Under Secretary for Finance and Administration / Chief Financial Officer
John Lapiana, Deputy Under Secretary for Finance and Administration
Joan Mockeridge, Office of Inspector General
Chuck Mitchell, Office of Inspector General
Juliette Sheppard, Director of IT Security
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: Management Response to IG Section 406 submission under the Cybersecurity Act of 2015 (Act)

Thank you for the opportunity to comment on this submission.

Smithsonian management does not believe that Section 406 of the Cybersecurity Act of 2015 applies to the Smithsonian. The report specified in Section 406 need only be submitted by an Inspector General of a covered agency, and in the view of Smithsonian management, the Smithsonian is not a covered agency. However, we are supportive of following government best practices wherever practicable and consistent with the Institution's mission.

The Smithsonian is currently in the process of formally analyzing all of its information security requirements, including those from federal regulations and best practices, against the existing IT Security Program and developing a comprehensive IT security architecture plan. This architecture planning includes controls discussed in the Section 406 report. Full implementation of the planned architecture improvements will be dependent on obtaining necessary funding.

In regards to the use of multi-factor access controls, the Smithsonian has implemented multifactor authentication for all remote access to the Institution's networks. Due to the relatively low risk nature of most Smithsonian systems, use of multifactor access controls on specific systems has previously not been a funded priority. However, due to evolving threats and best practices, and as part of the security architecture planning described above, the Smithsonian is assessing additional use of multifactor authentication in its computing environment. This includes determining policies for use of multifactor authentication, the selection of appropriate authentication technologies, and associated procedures.

In regards to the ability to monitor and detect exfiltration of data, this is an area where the Smithsonian has identified a need to enhance its capabilities and is planning for appropriate technologies and processes as part of the security architecture initiative described above. We have evaluated several data loss prevention solutions, forensics tools, and methods for improving visibility into our computing environment, and are working to determine which solutions would be most appropriate to include in our architecture. Additionally, funding for acquisition of a data loss prevention solution was included in our FY2017 congressional budget request.