Smithsonian Institution

SMITHSONIAN DIRECTIVE 224,
November 27, 2019

IDENTITY MANAGEMENT PROGRAM

1. PURPOSE

The Smithsonian's Identity Management Program encompasses identity and documentation validation, background investigation, credentialing, physical access to Smithsonian Institution (SI) facilities, and logical access to SI computer systems.

This program is consistent with the Institution's responsibility for the safety, security, and privacy of visitors and employees and for the care of the national collections and SI assets. This program is intended to determine whether employees and persons selected for employment or association with SI are trustworthy, reliable, and of good character, and whether their employment or association might in some way pose a threat to the Institution and its visitors, staff, collections, or assets.

2. BACKGROUND

Although the SI is not an Executive Branch agency, we support the general policies and procedures of the Homeland Security Presidential Directive (HSPD-12), an initiative that called for increased security across Government agencies.

The Smithsonian strives to meet as much of the guidelines as appropriate for our unique mission. In 2008, the Office of Protection Services (OPS) began to move toward adoption of personal identity verification through the implementation of our Identity Management System. The system enables SI to create enrollment and security processes that meet the intended goal by validating the identity of federal, trust and affiliated persons. This is done through identity validation and background investigations.

With the increased risk to SI computers and systems, this directive has been expanded to include requirements for logical access, and OPS and the Office of the Chief Information Officer (OCIO) have implemented appropriate risk mitigation measures for logical access.

3. DEFINITIONS

Affiliated Persons: Individuals other than employees who perform duties for the Smithsonian Institution or operate on Smithsonian property, including but not limited to:

- Contractors (paid with federal or trust funds) who perform work similar to Smithsonian employees, such as temporary help firms' employees, and other contractors, such as construction contractors and food service contractors' employees
- Interns, as defined in SD 709, Smithsonian Institution Internships
- Fellows, as defined in SD 701, Smithsonian Institution Fellows
- Emeriti, as defined in SD 206, Emeritus Designations
- Friends of the National Zoo (FONZ) employees and contractors
- Research associates, as defined in SD 205, Research Associates
- Smithsonian Early Enrichment Center (SEEC) employees
- Visiting researchers, including scientists, scholars and students
- Volunteers, as defined in SD 208, Standards of Conduct Regarding Smithsonian Volunteers
- Employees of federal, state, and local agencies working with SI employees at SI facilities
- Regents and advisory board members.

Employee: Smithsonian federal employees, as defined in Title 5 *United States Code* (U.S.C.) 2105, and Smithsonian trust employees.

Homeland Security Presidential Directive 12 (HSPD-12): HSPD-12 is the policy for Executive Branch agencies for a common identification standard for federal employees and contractors. It was issued on August 27, 2004. The primary goals of the directive are to enhance security, reduce identity fraud, protect personal privacy and leverage logical (computer) and physical (building access) security through one identification card.

Smithsonian-Controlled Facilities: For the purposes of this directive, SI-controlled facilities shall be considered Smithsonian-owned buildings or leased spaces, SI-controlled commercial space shared with non-Smithsonian tenants, and SI-owned contractor-operated facilities,

3. DEFINITIONS (continued)

including laboratories and educational institutions (collectively, SI-controlled facilities). (Please click on the link to the *SI Identity Management Handbook*, which is available at the Office of Protection Services [OPS] webpage on Prism, for additional information on this type of property, as well as for examples of SI facilities that meet these criteria.)

Smithsonian-Controlled Computer (IT) System accounts: For purposes of this directive, SI-controlled computer (IT) system accounts shall include SI network and email accounts, and Remote Access/Citrix accounts. Please click on the *OCIO Accounts and Access* website for further information.

Sponsor: A sponsor is defined as a federal or trust employee who requires an employee or affiliated person to accomplish a particular SI-related task or project. Additionally, to be eligible to be a sponsor, the employee must have a current SI credential and completed background investigation.

4. POLICY

Physical Access

The SI Identity Management Program will be consistent with the control objectives of HSPD-12. All employees and other affiliated persons associated with the Smithsonian will receive an appropriate background investigation and SI credential under the following conditions:

- their association with SI is for more than 30 calendar days, and they require unescorted access to staff-only areas of SI-controlled facilities; or

- they are considered vendors, provide regular delivery services or recurring services (as a contractor), or are other individuals who require intermittent unescorted physical access to SI facilities for more than 30 calendar days

The level of background investigation may vary based on the position risk level and/or required level of access. However, all employees and affiliated persons will receive a pre-appointment screening prior to their association with the Smithsonian and prior to the issuance of an SI credential. Compliance with this policy is a condition of an employee's or affiliated person's employment or association with the Smithsonian Institution.

All SI employees and affiliated persons must wear their SI credential at all times while in non-public areas of SI-controlled facilities and property areas. When a facility is closed to the public, staff will visibly wear the SI credential at all times throughout both public and staff areas of the facility.

4. POLICY (continued)

Individuals will not receive a background investigation and SI credential if they are associated with the Smithsonian Institution for less than 30 days. The 30-day period begins the first day the individual is affiliated with the Smithsonian and ends exactly 30 days later, no matter the frequency or duration of the activity (e.g., one or five days per week).

Individuals without an SI credential must be escorted by a credentialed employee or credentialed affiliated person when entering staff-only areas of SI-controlled facilities. Non-credentialed individuals must access SI-controlled facilities via a screening system (where appropriate), display an SI visitor credential at all times, and be escorted at all times.

The risk at a particular facility may be low enough so that a credential and/or appropriate background investigation may not be necessary for some affiliated persons. However, the requirement for issuance of an SI credential or completion of an appropriate background investigation can only be waived by the Director, OPS. Generally, waivers would only be approved for groups of persons (by labor category or location) and not for individuals. These requirements cannot be waived for any SI employees (federal or trust). Employees in labor categories must receive an appropriate background investigation and SI credential if their official association with the Smithsonian Institution is longer than 30 days.

There are several identification badges that are issued without a background investigation. These badges are an unofficial form of identification and do not grant the bearer unescorted access to staff-only areas of SI facilities. Specific guidance for these badges is addressed in the *SI Identity Management Handbook*.

Any misuse, tampering, or unauthorized reproduction of SI credentials is in direct violation of §499 and §701, Title 18, U.S.C., and is subject to criminal charges.

Logical Access

All employees and other affiliated persons who require an SI-controlled computer (IT) system account will receive an appropriate background investigation if their association with SI is for more than 30 calendar days.

The level of background investigation may vary based on the position risk level and/or required level of access. However, all employees and affiliated persons will receive a pre-appointment screening prior to receipt of an SI-controlled computer (IT) system account, regardless of their need for physical access or an SI credential. Reference Technical Note IT-960-TN12 for account request procedures.

Any deviations from this policy can only be waived by the Smithsonian Chief Information Officer for OCIO or his/her designee.

4. POLICY (continued)

Further details of the Identity Management Program policy and procedures can be found in the *SI Identity Management Handbook*. The handbook captures the complete process for applicant identification and identifies the required steps for issuance and use of SI credentials and access control procedures. The *SI Identity Management Handbook* briefly describes the background investigation process, but further details and requirements can be found in Chapter 731, Personnel Security, of SD 212 (for federal employees) and the corresponding chapter in SD 213 (for trust employees).

5. ROLES AND RESPONSIBILITIES

Office of Protection Services (OPS)

OPS is responsible for administering the Identity Management Program and reserves the right to deny or revoke issuance of an SI credential at any time for just cause during the investigative process or thereafter. Only specific qualified individuals from OPS have the authority to issue, deny, or revoke SI credentials; to access control cards; to initiate background investigations; and to approve or deny requests for reconsideration (appeals).

Office of the Chief Information Officer (OCIO)

OCIO is responsible for ensuring that SI employees and affiliated persons provide confirmation of a favorable pre-employment background investigation prior to receiving an SI-controlled computer (IT) system account, and developing (in consultation with OPS) protocols for background investigations beyond pre-appointment screening.

Unit Directors

SI unit directors are responsible for the daily oversight and enforcement of the Identity Management Program policies and procedures within their units.

Sponsors

All sponsors of new employees or affiliated persons are responsible for ensuring that all background investigation and credential request paperwork is properly completed in a timely manner. When SI employees or affiliated persons depart the Smithsonian, the sponsor shall account for Smithsonian personal property, materials, and credentials assigned to and/or controlled by the individual. SI property is defined in SD 315, *Personal Property Management*.

5. ROLES AND RESPONSIBILITIES (continued)

Employees and Affiliated Persons

All SI employees and affiliated persons are responsible for complying with the standards, policies, and guidance contained in this directive and in the associated handbooks.

6. REFERENCES

The authorities relied on for the SI Identity Management Program are as follows:

- Title 5, *Code of Federal Regulations* (CFR), Part 731: Suitability
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
- U.S. Office of Personnel Management Memorandum, “Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12”
- Chapter 731, Personnel Security, in SDs 212, *Federal Personnel Handbook*, and 213, *Trust Personnel Handbook*
- SD 931 — Use of Computers, Telecommunications Devices and Networks
- IT-960-TN12 — Active Directory Account and Password Requests
- IT-930- TN01— IT Security Waivers and Exceptions

SUPERSEDES:	SD 224, October 13, 2016
INQUIRIES:	Office of Protection Services (OPS), Smithsonian Facilities (SF)
RETENTION:	Indefinite. Subject to review for currency 36 months from date of issue

---