

OST DIRECTIVES TRANSMITTAL SHEET

(Modified DI -416)

DOCUMENT IDENTIFICATION NUMBER	SUBJECT	RELEASE NUMBER
731 DS 23	Strong Authentication	14-07
FOR FURTHER INFORMATION		DATE
Information Resources		DEC 23 2014

EXPLANATION OF MATERIAL TRANSMITTED:

This policy establishes mandates, authorities, responsibilities, and compliance requirements for users who access the Office of the Special Trustee for American Indians (OST) network and systems in accordance with the Department of the Interior (DOI) regulations cited in the Authority Section of this policy. This policy applies to all users under the authority of OST, to include contractors, consultants, temporary employees, interns, volunteers, and tribal users who access the OST network and systems with Government-furnished equipment.


Acting Chief of Staff
Office of the Principal Deputy Special Trustee

FILING INSTRUCTIONS:

Remove: None

Insert: 731 DS 23

- 1.1 Purpose.** On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors,” which requires the development, and implementation of a mandatory, government-wide standard for secure, and reliable forms of identification (ID) for Federal employees, and contractors. This chapter establishes mandates, authorities, responsibilities, and compliance, in accordance with HSPD-12, and the Department of the Interior (DOI) guidance for users who interactively log on to the Office of the Special Trustee for American Indians (OST) network and systems.
- 1.2 Scope.** This policy applies to all users, both end users and privileged users, including but not limited to all functions under the authority of OST, including OST employees, contractors, consultants, temporary employees, interns, volunteers, and tribal users who interactively log on to the OST network and systems.
- 1.3 Policy.** All users shall adhere to the following access and two-factor authentication requirements. Two-factor authentication is a process utilizing two means of identification -- what you know and what you have -- to verify the identity of an entity trying to access services in a computer or network.

A. Access and Two-Factor Authentication.

- 1) If a user has an activated HSPD-12 compliant personal identification verification (PIV) card, they shall use this card at all times (including while in the office or teleworking) when accessing the OST network.
- 2) If a user does not have a PIV card and requires access into the OST network for more than 90 days, the user must make arrangements to have one issued.
- 3) If a temporary employee or contractor requires access into the OST network for a period not exceeding 90 days, user ID/password-based credentials will be issued. These credentials will automatically be disabled 91 days from the date they were created and issued.
- 4) If a PIV card is forgotten, a user may contact the OST Helpdesk (505-816-1007) or send an email to OST_ITHelp@OST.DOI.GOV and request the use of user ID/password-based credentials for up to 72 hours.
- 5) If a personal identification number (PIN) is forgotten, a user may contact the OST Helpdesk (505-816-1007) or send an email to OST_ITHelp@OST.DOI.GOV requesting the use of user ID/password-based credentials for no more than 10 business days to allow the user to continue working while the PIV card is retrieved and/or the PIN reset.
- 6) If a PIV card is damaged or lost, a user may contact the OST Helpdesk (505-816-1007) or send an email to OST_ITHelp@OST.DOI.GOV requesting the use of user ID/password-based credentials for no more than 30 calendar days to allow the user to continue working while making arrangements to replace the PIV card. In addition, the user must contact the OST USAccess Lead Sponsor to request that a new PIV card be issued.

- 7) All exceptions in excess of 30 calendar days must be approved by the Bureau Chief Information Security Officer (BCISO) and reported to the DOI Office of the Chief Information Officer (OCIO) in accordance with DOI guidance.
- 8) The OST Office of Information Resources (OIR) will review all non-PIV authorizations on a weekly basis and remove non-PIV access that has expired.

B. Prohibitions.

- 1) Users who access the OST network and systems shall not:
 - Provide or lend their PIV card and PIN or any other form of credentials to anyone for any reason.
 - Use access for any purpose that is prohibited by Section 2.6 of the Department's Policy on Limited Personal Use of Government Office Equipment, and Library Collections (410 DM 2).

1.4 Authority.

A. Regulatory.

- 1) HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, issued August 27, 2004
- 2) DOI DM 375, Chapter 19, Information Security Program, March 21, 2012
- 3) DOI DM 410, Chapter 2, Limited Personal Use of Government Office Equipment and Library Collections

B. Guidance.

- 1) Office of Management and Budget (OMB), Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 5, 2005
- 2) OMB, Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated February 3, 2011
- 3) National Institute of Standards and Technology (NIST), Federal Information Processing Standard 201-1 (FIPS 201-1), Personal Identity Verification of Federal Employees and Contractors, dated March 6, 2006
- 4) NIST, Special Publication 800-63-1, Electronic Authentication Guideline, December 2011
- 5) OCIO, Directive 2012-008, PIV Two-Factor Authentication for Virtual Private Network Remote Access

1.5 Responsibilities.

- A. **Supervisors** shall ensure that users, defined as employees, contractors, and other individuals who have been granted explicit authorization, to access, modify, delete, or utilize OST information, adhere to this policy.
- B. **The Assistant Director for Information Resources (ADIR)** and OIR staff are responsible for creating, and/or revising information technology policies, and ensuring that the information in this directive for the programs and functions within their authority, including references and citations, are accurate and up-to-date.
- C. **The BCISO** shall ensure that the policy, and processes in this directive conform to applicable statutes, regulations, Federal standards, and policies.
- D. **The OIR** shall review all non-PIV authorizations on a monthly basis, and remove non-PIV access that has expired.

1.6 Definitions.

- A. Access - the capability to enter into any OST workstation domain (desktop or laptop).
- B. Two-Factor Authentication is a combination of two elements:
 - 1) “Something you know,” defined as a PIN, and
 - 2) “Something you have,” defined as an HSPD-12 compliant PIV card.
- C. Privileged users – Users with elevated access rights beyond those granted to a general end user (e.g., system and network administrators, database administrators, etc.).
- D. Responsibilities of the OST ADIR as provided in **Paragraph 1.5** are executed by the Director, OIR.
- E. Responsibilities of the OST BCISO as provided in **Paragraph 1.5** are executed by the Office of Information Technology Services, OIR.