United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

SEP 29 2014

Memorandum

To: Heads of Bureaus and Offices

From: Sylvia Burns
Chief Information Officer

Subject: Guidance on the Use of Electronic and Digital Signatures

A number of information systems across the Department of the Interior (DOI) provide for and may eventually require, the use of electronic[1] and digital signatures.[2] This memorandum notifies Bureaus and/or Offices that DOI workstations, desktops, laptops, and other Personal Identity Verification (PIV) capable devices must meet all software and hardware configuration requirements to enable effective use of electronic and digital signatures via PIV cards. Bureaus and/or Offices must support use of electronic or digital signatures by December 31, 2014.

The new Enterprise Forms System currently being implemented is an enterprise-wide shared service that will support and require the use of electronic and digital signatures for Bureau and/or Office forms. As such, in order to take advantage of this new service, all Bureaus and/or Offices need to ensure that employees have the ability to generate electronic or digital signatures compliant with *Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors.*[3] The HSPD-12 specifies requirements for a common identification standard for Federal employees and contractors utilizing PIV cards.

We appreciate your cooperation and collaboration as we work together to promote and advance the use of electronic and digital signatures. It is incumbent upon Bureaus and/or Offices to ensure compliance by the due date of December 31, 2014. If a Bureau and/or Office is unable to

---

[1]An electronic signature or e-signature is any electronic means that indicates a person adopts the contents of an electronic message, or more broadly, that the person who claims to have written a message is the one who wrote it (i.e., the message received is the one that was sent).

[2]A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and other cases where it is important to detect forgery or tampering.

[3]http://www.dhs.gov/homeland-security-presidential-directive-12.

support this requirement by December 31, 2014, please notify John Montel at John_Montel@ios.doi.gov in writing by November 3, 2014. If there are any questions regarding implementation of the HSPD-12 requirements, please contact the Chief Information Security Officer (CISO), Lawrence Ruffin at (202) 208-5419 or Lawrence_Ruffin@ios.doi.gov. All other questions should be directed to John Montel at (202) 208-3939 or John_Montel@ios.doi.gov.

Attachment

cc: Bureau and Office Deputy Directors
Rachel Spector, Office of the Solicitor
Faye Iudicello, Director of the Office of the Executive Secretariat
Bureau and Office Assistant Directors for Information Resources
Bureau Chief Information Security Officers
Bureau and Office FOIA Officers
Bureau and Office Privacy Act Officers
Bureau and Office Records Officers
Bureau and Office Forms Managers

National Institute of Standards and Technology Publication References

The following National Institute of Standards and Technology (NIST) publications outline the overall guidance and security requirements for HSPD-12:

- NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations:* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
- NIST Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication:* http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf.
- Federal Information Processing Standard Publication 186-3, *Digital Signature Standard (DSS):* http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.
- NIST Special Publication 140-2, Federal Information Processing Standard, *Security Requirements for Cryptographic Modules*: http://www.nist.org/nist_plugins/content/content.php?content.48.
- NIST Special Publication 201, Federal Information Processing Standard, *Personal Identity Verification (PIV):* http://www.nist.org/nist_plugins/content/content.php?content.49.