

**POLICY ISSUE
(Information)**

November 21, 2008

SECY-08-0181

FOR: The Commissioners

FROM: Darren B. Ash
Deputy Executive Director
for Corporate Management
Office of the Executive Director for Operations

SUBJECT: HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 UPDATE

PURPOSE:

The purpose of this paper is to inform the Commission of a change in the staff's plan for implementing Homeland Security Presidential Directive-12 (HSPD-12). NRC's current strategy is to obtain its HSPD-12 compliant credentials through a shared services provider (SSP). The NRC's SSP is the General Services Administration (GSA). Since our current strategy was developed, NRC's Managed Public Key Infrastructure (MPKI) has been upgraded to work with the Federal Public Key Infrastructure (PKI) Bridge that allows all PKI vendors that are connected to the bridge to cross-certify each others' certificates. Smartcards are now being produced at NRC using this technology. Therefore, because of the high cost of integration and maintenance using GSA's USAccess system, staff plans to leverage use of the existing in-house VeriSign PKI to continue implementation of HSPD-12. This change will not impact NRC's existing schedule for completing full implementation of the HSPD-12 physical access requirements by October 27, 2009. This plan does not include any new commitments or resource implications.

BACKGROUND:

The President issued HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," on August 27, 2004. That policy required all Federal Executive

CONTACT: Andrew Pretzello, ADM/DFS/FSB
(301) 415-7404

Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors for access to Federal facilities and information systems, and to designate the major milestones for implementation. Since issuance of HSPD-12, the Office of Management and Budget (OMB) has issued several memoranda requiring agencies to meet specific deadlines for the HSPD-12 program. The first memorandum, M-05-24, was issued on August 5, 2005, and specified the use of PKI digital certificates for accessing government resources. The memorandum required that agencies work toward using the card for access to information and network resources and physical access to facilities. On January 11, 2007, OMB issued a second memorandum, M-07-06, that required agencies to complete HSPD-12 actions by a given list of dates. On October 23, 2007, OMB sent a third memorandum, M-08-01, to remind agencies to complete background investigations and issue credentials as required for the implementation of HSPD-12.

In accordance with the OMB memorandum, M-07-06, NRC met the October 27, 2006, deadline for all departments and agencies to begin issuance of activated identity credentials for all new employees and contractors compliant with Parts 1 and 2 of the Federal Information Processing Standard 201. NRC also met OMB's October 27, 2007, deadline for all departments and agencies to complete background checks for employees with 15 years or fewer of service. NRC has informed OMB that 1) as of October 27, 2008, NRC had completed background checks for all employees and contractors; and 2) by October 27, 2009, NRC will issue HSPD-12-compliant credentials to all employees and contractors.

DISCUSSION:

In order to meet HSPD-12 requirements, staff entered into an agreement with GSA in 2006 for GSA to serve as NRC's SSP and provide access to GSA's USAccess system. An SSP provides the information technology (IT) system, including the software used to store information from background investigations, process fingerprints and pictures, produce badges, and issue PKI certificates. The PKI certificates enhance security and enable Federal agencies to use standardized credentials to obtain access to information and network resources and physical access to facilities. GSA uses Entrust as its PKI provider. While staff identified interface concerns regarding GSA's use of Entrust and NRC's use of VeriSign as its PKI provider, GSA assured staff that integration costs associated with implementing an interface between the Entrust and VeriSign PKIs would not be prohibitive. Initial cost estimates from GSA were approximately \$30,000.

Two events have caused staff to reevaluate our strategy and change direction. First, the U.S. Department of Treasury (Treasury) began to work with GSA in 2007 to develop an interface between its internal Entrust PKI and the GSA Entrust PKI. Treasury has already incurred in excess of \$450,000 to program the interface between the internal and external Entrust PKIs. The considerable cost of developing this interface has led several agencies to reconsider their options, and GSA has advised Federal agencies to plan and budget for a minimum cost of \$450,000. Under GSA's program, NRC's costs would be significantly higher as NRC utilizes VeriSign's PKI. Second, after entering into the agreement with GSA, the staff determined that several mission critical business applications, such as the Electronic Information Exchange System, Criminal History Program System, and National Source Tracking System, would require digital certificates to enhance security of the information contained in the various applications. Therefore, NRC is upgrading the current internal PKI infrastructure utilizing VeriSign to cross-certify certificates with other vendors across the Federal Bridge. The existing

NRC staff certificates will be replaced with the new Federal Bridge certificates as they expire. The change to cross-certification of these PKI certificates now allows NRC to leverage the internal PKI infrastructure for the HSPD-12 program.

An independent contractor conducted a review of NRC's HSPD-12 and Identity and Access Management strategy in June 2008, and recommended that, because NRC is hosting an in-house MPKI, the HSPD-12 personal identification verification card production should be brought in-house as part of the HSPD-12 solution. Consistent with this recommendation and because of the high cost of integrating multiple NRC systems with the GSA USAccess system, staff plans to leverage use of the existing in-house VeriSign PKI infrastructure to continue implementation of HSPD-12. This change will not impact NRC's existing schedule for completing full implementation of the HSPD-12 physical access requirements by October 27, 2009.

In addition, NRC will upgrade the current physical access control system (PACS) to the latest HSPD-12-compliant version. The agency began the Headquarters, Region III, and Technical Training Center PACS upgrades in October 2008. The Technical Training Center upgrade will be completed by December 2008; Region III will be completed by April 2009; Region I will be completed by August 2009; Headquarters will be completed by October 2009; and Regions II and IV will be completed as part of their moves to new locations, dates to be determined. Following implementation of the HSPD-12 physical access requirements at Headquarters, appropriate arrangements will be made for NRC first responders and senior staff to exchange their GSA USAccess badge with the NRC HSPD-12 badge.

NRC is also developing plans to implement the infrastructure to support the use of the HSPD-12 compliant cards for access to NRC information and network resources. This involves building on the work that was completed to implement the MPKI infrastructure that is currently utilized to support access to critical business applications, such as the Electronic Information Exchange System, Criminal History Program System, and the National Source Tracking System. Additional hardware and software will be implemented to enable the PKI certificate on the HSPD-12 compliant cards to provide the access to NRC information and network resources. This capability will be implemented by October 31, 2010. Additional work to update NRC applications for "single sign-on" will be on-going with December 31, 2010 as the target date to provide this capability for the first application.

In summary, once all HSPD-12-compliant cards are issued and systems requiring authenticated users have been upgraded, employees and contractors will use the same HSPD-12 credential for access to NRC information and network resources and physical access to NRC facilities. By contracting directly with VeriSign and a systems integrator rather than utilizing GSA as a third-party provider, NRC will avoid significant integration costs between GSA's Entrust PKI and NRC's VeriSign MPKI. In addition, this approach leverages the MPKI foundation currently being developed, and ensures that the program is entirely managed by NRC staff. Thus, issuing and replacing credentials will occur at NRC locations as opposed to staff travelling to GSA locations. This strategy also permits NRC to manage its own stored PKI certificates and utilize the full capabilities of the card, as NRC deems appropriate.

The Commissioners

- 4 -

COORDINATION:

The Office of the General Counsel has reviewed this package and has no legal objection. The Chief Financial Officer reviewed this package and determined that there is no financial impact.

/RA/

Darren B. Ash
Deputy Executive Director
for Corporate Management
Office of the Executive Director for Operations