EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

May 23, 2008

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator E-Government and Information Technology

SUBJECT: Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation

To assist agencies with their implementation activities for HSPD-12, we are providing the attached guideline. This guideline includes questions agencies should have considered when planning for the use of Personal Identity Verification (PIV) credentials with physical and logical access control systems.

If your agency has not already completed its plan for incorporating the use of PIV credentials with physical and logical access control systems, we ask you to ensure these plans are developed as soon as possible and in coordination with officials from your agency's personnel, physical security, budget, and other appropriate offices. Additionally, agencies should continue to follow the requirements of Office of Management and Budget (OMB) policy, such as A-130, "Management of Federal Information Resources" and A-11, "Preparation, Submission and Execution of the Budget," when developing plans.

The attached guideline is provided to assist you with your planning efforts and the status of these items and your HSPD-12 plans should be available to your oversight organizations (e.g. OMB, General Accountability Office, and your Office of Inspector's General) upon request. If you have questions, please contact Carol Bales, Senior Policy Analyst, Office of Management and Budget at (202) 395-9915 or eauth@omb.eop.gov.

Attachment
Guidelines for Addressing Physical and Logical Access Controls in the Agency's HSPD-12 Implementation Plan

GUIDELINES FOR ADDRESSING
PHYSICAL AND LOGICAL ACCESS CONTROLS
IN THE AGENCY'S HSPD-12 IMPLEMENTATION PLAN

This document serves as a guideline to assist agencies in preparing or refining plans for incorporating the use of Personal Identity Verification (PIV) credentials, to the maximum extent practicable, with physical and logical access control systems.

I. General Information	
Guideline Completion Date:	
Agency/Department Name:	
Agency HSPD-12 Point of Contact:	
Phone Number:	Email:

II. Physical and Logical Access Control			
1) Does your agency have a documented plan for incorporating the use of Personal Identity Verification (PIV) credentials for both physical and logical access control? *(As part of the planning process, agencies must continue to follow all existing OMB policy requirements (e.g. OMB Circular A-130, "Management of Federal Information Resources.")*	**Yes/ No**		If no, then include planned date of completion (this is the date from your agency/OMB agreed-upon HSPD-12 Implementation Plan):
a) What are the key milestones and dates, in your plan, for implementing the use of PIV credentials for physical and logical access control?			
2) Does your agency have policy, implementing guidance and a process in place to track progress towards the appropriate use of the PIV credentials?	**Yes/ No**		If no, then include the date this will be completed:
a) Does your plan include a process for authorizing the use of other agency PIV credentials to gain access to your facilities and information systems?	**Yes/ No**		If no, then include the date this will be completed:
3) In developing your plan, has your agency prioritized the implementation of PIV credentials with physical access control systems based on the "Facility Security Level Determinations for Federal Facilities – An Interagency Security Committee Standard" for facilities security?	**Yes/ No**		If no, then include the date this will be completed:
4) In developing your plan, has your agency prioritized the implementation of PIV credentials for logical access based on the NIST FIPS 199 (Standards for Security Categorization of Information and Information Systems), NIST Special Publications (SP) 800-53 (Recommended Security Control for Information Systems) and 800-63 (E-authentication Guidance), as well as other relevant NIST FISMA guidelines and OMB guidance?	**Yes/ No**		If no, then include the date this will be completed:
5) In developing your plan and transition strategy, is your agency leveraging the "Federal Enterprise Architecture Practice Guidance?"	**Yes/ No**		

Physical Access Control			
6) Planned completion date for implementing the use of PIV credentials with all physical access control systems, as determined necessary based on risk assessments and policy requirements: *(If physical access control is controlled by the GSA Public Building Service (PBS) then agencies are to provide requirements to GSA PBS for them to address in the GSA PBS plan.)*			
a) Number of Level I facilities identified as requiring access using the electronic capabilities of PIV credentials:			
Planned date of completion for using PIV credentials to access Level I facilities:			
b) Number of Level II facilities identified as requiring access using the electronic capabilities of PIV credentials:			
Planned date of completion for using PIV credentials to access Level II facilities:			
c) Number of Level III facilities identified as requiring access using the electronic capabilities of PIV credentials:			
Planned date of completion for using PIV credentials to access Level III facilities:			
d) Number of Level IV facilities identified as requiring access using the electronic capabilities of PIV credentials:			
Planned date of completion for using PIV credentials to access Level IV facilities:			
e) Number of Level V facilities identified as requiring access using the electronic capabilities of PIV credentials:			
Planned date of completion for using PIV credentials to access Level V facilities:			
7) Has your agency completed a full inventory of its physical access controls systems, including readers?	**Yes/ No**		If no, then include the date this will be completed:
8) Has your agency identified all physical access points where you intend to require access using the electronic capabilities of the PIV credentials?	**Yes/ No**		If no, then include the date this will be completed:
9) Has your agency reviewed and considered the PIV functionality features and assurance levels /recommendations outlined in NIST 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)"?	**Yes/ No**		If you answered yes, when does your agency intend to begin implementing the NIST recommendations?
10) Has your agency performed the analyses to identify the changes that must be made to upgrade its systems' capabilities to support use of the electronic capabilities of the PIV credentials for physical access?	**Yes/ No**		If no, then include the date this will be completed:

Logical Access Control				
11) Planned completion date for implementing the use of PIV credentials for all logical access control systems, as determined necessary based on risk assessments and policy requirements:				
a) Has your agency identified all of its high impact systems (based on FIPS 199 and SP 800-63) in which it intends to require access using the electronic capabilities of the PIV credentials?	**Yes/ No**		If no, then include planned completion date:	Include date all of these high impact systems will be leveraging PIV credentials:
b) Has your agency identified all of its moderate impact systems (based on FIPS 199 and SP 800-63) in which it intends to require access using the electronic capabilities of the PIV credentials?	**Yes/ No**		If no, then include planned completion date:	Include date all of these moderate impact systems will be leveraging PIV credentials:
c) Has your agency identified all of its low impact systems (based on FIPS 199 and SP 800-63) in which it intends to require access using the electronic capabilities of the PIV credentials?	**Yes/ No**		If no, then include planned completion date:	Include date all of these low impact systems will be leveraging PIV credentials:
12) Is your agencies' plan for integrating use of PIV credentials for logical access control aligned with its plan for implementing two-factor authentication and encryption in accordance with OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information?"	**Yes/ No**		If no, why not:	
13) Does your agency intend to leverage the electronic capabilities of the PIV credentials as the primary means of meeting the requirements of OMB Memorandum 06-16, "Protection of Sensitive Agency Information?"	**Yes/ No**		If no, why not:	
14) Have you reviewed your agency's E-authentication Ramp-up Plan to identify all E-Government, and other E-authentication applications, to be PIV-enabled to provide access for authorized federal employees and contractors using their PIV credentials?	**Yes/ No**		If no, why not:	
Comments:				