

**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: 12/1/2008	
Agency/Department Name: U.S. Nuclear Regulatory Commission (NRC)	
Agency HSPD-12 Point of Contact: Karen Cudd	
Phone Number: 301-415-6554	Email: Karen.cudd@nrc.gov

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? <i>(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."))</i>	Yes/ No	If no, then include planned date of completion (this is the date from your agency/OMB agreed-upon HSPD-12 Implementation Plan):
	Y	
a) What are the key milestones and dates, in your plan, for implementing the use of PIV credentials for physical and logical access control?	LACS: Deploy card readers/middleware – 7/1/2010 Complete LACS implementation – 12/31/2010 PACS: Complete PACS installations for all locations – 10/30/2009	
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:
	Y	
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: 12/31/2011
	N	
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:
	Y	
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:
	Y	
5) In developing your plan and transition strategy, is your agency leveraging the "Federal Enterprise Architecture Practice	Yes/ No	

Guidance?"	Y	
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: <i>(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.)</i>		
a) Number of Level I facilities identified as requiring access using the electronic capabilities of PIV credentials:	0	
Planned date of completion for using PIV credentials to access Level I facilities:	N/A	
b) Number of Level II facilities identified as requiring access using the electronic capabilities of PIV credentials:	2	
Planned date of completion for using PIV credentials to access Level II facilities:	10/30/2009	
c) Number of Level III facilities identified as requiring access using the electronic capabilities of PIV credentials:	9	
Planned date of completion for using PIV credentials to access Level III facilities:	10/30/2009	
d) Number of Level IV facilities identified as requiring access using the electronic capabilities of PIV credentials:	2	
Planned date of completion for using PIV credentials to access Level IV facilities:	10/30/2009	
e) Number of Level V facilities identified as requiring access using the electronic capabilities of PIV credentials:	0	
Planned date of completion for using PIV credentials to access Level V facilities:	N/A	
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:
	Y	
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:
	Y	
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?
	Y	
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:

	Y		
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:
	Y		
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:
	Y		
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:
	Y		
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:
	Y		
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:
	Y		
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:
	Y		
Comments:			