Department of Energy
Washington, DC 20585

March 31, 2005

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: ROSITA O. PARKES
CHIEF INFORMATION OFFICER

GLENN S. PODONSKY
DIRECTOR
OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE

MICHAEL C. KANE
ASSOCIATE ADMINISTRATOR FOR MANAGEMENT AND ADMINISTRATION
NATIONAL NUCLEAR SECURITY ADMINISTRATION

SUBJECT: Department of Energy Implementation of Homeland Security Presidential Directive-12, Advisory No.1

The Chief Information Officer (CIO), Office of Security and Safety Performance Assurance (SSA), and Chief Financial Officer (CFO) are jointly sponsoring the Department's initiative to implement Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004.

HSPD-12 requires agencies to issue to their Federal and contractor employees "secure and reliable forms of identification" to be used for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems. Identification has to be rapidly authenticated electronically, strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation. This is a significant project that will engage resources throughout the Department of Energy (DOE) community and will require the cooperative spirit and dedication that consistently make DOE a leading-edge agency.

Timeframe

The Department of Commerce was tasked to develop Federal Information Processing Standard 201 (FIPS 201), *Personal Identity Verification for Federal Employees and Contractors*, to address the identification of Federal and contractor employees. The Federal departments and agencies shall meet the requirements of FIPS 201 no later than October 27, 2005 in accordance with the timetable specified in HSPD-12.

Project Management

DOE is establishing a Project Team (PT) with resources provided by SSA and the CIO, which will manage the overall implementation of HSPD-12. The CIO will administratively house the PT; Program Offices are requested to provide staffing for key positions. Representation from the Program Offices and the Laboratory environment is also highly encouraged. The PT will have primary responsibility for the engineering, design, procurement, coordination, deployment and support of a common solution for all DOE Elements, including the National Nuclear Security Administration, field sites and Management and Operations contractors. With the support of the DOE team, the PT will ensure a single solution is delivered economically and efficiently for the benefit of the whole DOE community.

Funding & Procurement

The initiative will be funded in accordance with Office of Management and Budget (OMB) direction to "Fund HSPD-12 using existing resources as necessary to meet deadlines established in the Directive." OMB has stated that the General Services Administration will be the Federal Government's centralized purchasing authority and executive agent for all HSPD-12 related items. Therefore, any pending or planned selection, purchase, major upgrade or acquisition of technologies, components or other technologies related to badging, physical access to facilities or logical access to information technology systems must be placed on hold until such a time as the PT has had an opportunity to determine requirements and issue subsequent guidance. All goals of the Department must continue to be met; therefore, if this procurement hold places other Departmental goals in jeopardy, Program Offices must assess and document the potential impact and provide findings to the PT for approval.

Next Steps

HSPD-12 requires agencies to interconnect badging, physical access and logical access systems to achieve electronic authentication and access control. In order to facilitate the work of the PT, a detailed inventory of the Department's infrastructure baseline will need to be performed expeditiously to ascertain current capabilities and "in-place" systems for the purposes of determining reusability and interfaceability. Accordingly, DOE Elements should expect to see a PT issued, DOE Enterprise Architecture Repository structured and facilitated data call in the near term. This data call will help the Department build a profile that includes site-by-site, building-by-building, vendor, and version specific information pertaining to hardware, software and systems used for badging offices, physical access control and logical access control.

Attached for information are the Plans of Action and Milestones for the four PT taskforces created to address immediate actions. If you or a member of your staff would like to participate on any or all of the taskforces, please contact the identified lead.

We appreciate the support of our DOE team in meeting the challenges of HSPD-12.

Questions should be directed to Mr. Bruce A. Brody, Associate CIO for Cyber Security at (202) 586-1090.

Attachments

cc: Susan Grant, ME-1

HSPD-12 POAM Points of Contact

3/25/05

TASK FORCE		ORG.	NAME	PHONE	FAX
A	**Lead**	CIO	John Rabb	202-586-4656	x1840
		SSA	Dan Young	202-586-2487	x5039
		NNSA	Kelly Stewart	202-586-6180	
	Support	ME			
		GC			
Action					
1. OMB Reporting					
2. Procurement Suspension					
3. Procurement Impact					
4. Policy Impact		CIO			
		SSA			
5. ID Mgt System (IDMS)					
6. IT System Impact					
7. Inventory		CIO			
		SSA			
8. Competitive Sourcing Impact		CIO			
		SSA			
B	**Lead**	SSA	Mitch McAllister	301-903-3022	x3086
		NNSA	Kelly Stewart	202-586-6180	
	Support	CIO			
		ME			
		GC			
Action					
1. Recredentialing Impact					
2. Foreign Born DOE Employees					
3. Card Layout					
4. Facility Impact					
C	**Lead**	ME	Cherylynne Williams	202-586-1005	x0576
		NNSA	Kelly Stewart	202-586-6180	
	Support	CIO			
		SSA			
		GC			
Action					
1. Personnel					
2. Privacy					
D	**Lead**	IG	TBD		
	Support	CIO			
		NNSA			
		SSA			
Action					
1. IG / Secretary Approval					

Plan of Action and Milestones
TASK FORCE A
Lead Organizations: CIO and SSA

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
1. OMB Reporting. As has been discussed at Federal Identity Credentialing Committee (FICC) meetings, it should be expected that a significant reporting requirement to OMB will be soon forthcoming. While the task is still TBD, it can be expected that OMB will want to know the DOE specifics on implementation, costs, timeframe, a POA&M, and related topics.	03/30/05	05/23/05		
2. Procurement Suspension. All of DOE, to include field sites, M&O contractors, and all other elements, must stop any pending or planned selection, purchase, major upgrade or acquisition of technologies, components and other technologies related to; badging, physical access control to facilities or logical access to information technology systems until such a time as the PMO has had an opportunity to determine requirements and issue subsequent guidance. Expenditure of funding could result in buying nonstandard or non-compliant technologies. OMB has stated that GSA will be the Executive Agent for all purchases related to PIV. Policy should include asking for a waiver to spend on physical access system upgrades. All desktop clients should include smart card keyboards. GSA will is setting up a large aggregate buy for cards, readers, etc.	03/30/05	04/06/05		
3. Procurement Impact. HSPD-12/FIPS 201 applies equally to contractors and contract employees. DOE Procurement must determine how to best deal with the requirements of HSPD- 12/FIPS 201 and how to impart those requirements and notifications into all DOE contracts.	03/30/05	04/11/05		

Plan of Action and Milestones
TASK FORCE A
Lead Organizations: CIO and SSA

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
4. Policy Impact. DOE must review all applicable Orders, Policy, Manuals, and related Guides pertaining to issuing ID badges, conducting background checks of personnel (employee and contractors) and hiring processes for the purposes of updating these documents to reflect the new requirements of FIPS 201, taking into account both PIV-I and PIV-II requirements. The review should produce proposed changes that will immediately go into effect and or produce new policy/guides, as required. Due to the short timeframe required by FIPS 201, implementation of these changes outside of REVCOM is recommended.	03/30/05	04/29/05		
5. Identification Management System (IDMS). Strongly implied in FIPS 201 is the need for a supporting IT system which manages the entire PIV process. This is separate from that which will control physical and logical access to facilities and IT systems. Without such an IDMS system, meeting the requirements of PIV-I and PIV-II will be difficult. The functions of this IDMS would be, but not be limited to, applicant monitoring, workflow, background check monitoring, ID issuance, revocation, update and maintenance. Any new supporting IT systems must consider the PIV-II requirements before being procured. The IDMS must interface with fingerprint readers, card printers and similar devices. The IDMS must be certified and accredited before it can be made operational. The CIO must analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts and perform the work required to determine the full extent of the requirements for this system, to see if such a system exists commercially, or if repurposing an existing capability could provide the services needed.	03/30/05	05/10/05		

Plan of Action and Milestones
TASK FORCE A
Lead Organizations: CIO and SSA

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
6. IT System Impact. FIPS 201 Table 6-3 correlates the Assurance Level requirement of a particular IT system (Level 2=SOME, Level 3=HIGH and Level 4=VERY HIGH) to the specific PIV authentication mechanism(s) required to be used to access the system. Therefore, if a system is deemed through a certification and accreditation process to require a Level 2, 3 or 4 Assurance Level, then the individual accessing the federal IT system must use a government issued PIV credential, even if they are non-employees or non-contractors. If the system is deemed to require only an Assurance Level of 1, then it can be presumed that the PIV is not required to be used because there is no identification proofing requirement for that particular system. The CIO's Office must review all of the DOE IT systems to list and quantify their individual respective required Assurance Level for the purposes of quantifying cost impacts to those systems to accept a PIV credential. This must include the use of PIV card in logon and applications.	03/30/05	05/02/05		

Plan of Action and Milestones
TASK FORCE A
Lead Organizations: CIO and SSA

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
7. Inventory. PIV-II requires agencies to interconnect badging, physical access and logical access systems to achieve electronic authentication and access control. In order to expedite this effort, the PMO will need a detailed inventory of the Department's infrastructure baseline to ascertain current capabilities and the potential reuse of "in-place" systems. A Department of Energy Enterprise Architecture Repository (DEAR) structured and facilitated data call must be performed. The data call will help the Department build a profile that includes site-by- site, building-by-building, vendor, and version specific information pertaining to hardware, software and systems used for badging offices, physical access control and logical access control. The CIO will analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts and perform the work required to resulting in a DEAR data call. This should include SBU and classified networks. It should include hardware (servers, clients, laptops, PDS's and other devices, RSA tokens or keyfobs, physical access doors, head ends and controllers, access cards) and operating systems.	03/30/05	05/31/05		
8. Competitive Sourcing Impacts. The IT Competitive Sourcing procurement that is currently on going may be greatly affected by HSPD-12 and FIPS 201. A workgroup should be formed of DOE experts to analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts and perform the work required to determine DOE's position on this topic.	03/30/05	04/29/05		

Plan of Action and Milestones
TASK FORCE B

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
1. Re-credentialing Impact. Certain DOE badges have been issued without the requisite FIPS 201 background checks. An example is the badge referred to as BAO (Building Access Only) which can be issued without a NAC. DOE must determine the impact of re-verifying and re-credentialing these individuals and what adjudication processes it wants to invoke if, when an FBI fingerprint check is done, a derogatory or criminal history is returned on the individual that was previously unknown to DOE.	03/30/05	04/29/05		
2. Foreign Born DOE Employees. DOE has a number of cases involving foreign born employees. DOE has to wrap the credentialing PIV process into this aspect of DOE workers.	03/30/05	04/29/05		
3. Card Layout. The format of and data elements for the DOE PIV smartcard need to be determined. FIPS 201 provides many optional features and agency specified zones which DOE has to select from and standardize upon. This activity, performed now, will dovetail into the determinations and requirements for the IDMS and for policy changes, such that if a certain DOE feature is invoked on the smartcard, the IDMS specification has knowledge of that requirement.	03/30/05	04/29/05		
4. Facility Impact. For determining physical access to a federally controlled facility by an employee, contractor, non-employee or non-contractor, physical access would be stipulated by that local facility's procedures, consistent with DOE policy.	03/30/05	04/29/05		

Plan of Action and Milestones
TASK FORCE C
Lead Organization: ME

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
1. Personnel. DOE federal employee personnel/HR processes will need to be examined and updated to incorporate the background check requirements into the hiring process before a badge is issued.	03/30/05	04/29/05		
2. Privacy. FIPS 201 contains many specific, implied and derived requirements which are solely allocated to the Senior Agency Official for Privacy (SAOP). This individual/office is required to perform many duties and to have life-cycle processes in place to support PIV. The magnitude of the actions allocated to the SAOP tends to indicate that the SAOP needs a staff, separate from the PMO, to perform the requirements. The SAOP should analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts to perform the work required and to determine subsequent costs required for SAOP PIV-related operations. Procurement should be included because it will impact contarcted employees/services and the way you acquire those services.	03/30/05	04/22/05		

Plan of Action and Milestones
TASK FORCE D

Action	Start Date	Estimated Completion Date	Status (Not Initiated, Ongoing, Completed)	Notes
1. Inspector General/Secretary Approval. FIPS 201 requires that the Agency IG must accredit the PIV-I process(es) stood up by the agency and certify that they meet FIPS 201. The Secretary must also approve the process in writing. A meeting has to be held with the OIG to inform them of their responsibility under FIPS 201.	TBD	TBD		

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: ROSITA O. PARKES
CHIEF INFORMATION OFFICER

GLENN S. PODONSKY
DIRECTOR
OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE

MICHAEL C. KANE
ASSOCIATE ADMINISTRATOR FOR MANAGEMENT AND ADMINISTRATION
NATIONAL NUCLEAR SECURITY ADMINISTRATION

SUBJECT: Department of Energy Implementation of Homeland Security Presidential Directive-12, Advisory No.1

The Chief Information Officer (CIO), Office of Security and Safety Performance Assurance (SSA), and Chief Financial Officer (CFO) are jointly sponsoring the Department's initiative to implement Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004.

HSPD-12 requires agencies to issue to their Federal and contractor employees "secure and reliable forms of identification" to be used for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems. Identification has to be rapidly authenticated electronically, strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation. This is a significant project that will engage resources throughout the Department of Energy (DOE) community and will require the cooperative spirit and dedication that consistently make DOE a leading-edge agency.

Timeframe
The Department of Commerce was tasked to develop Federal Information Processing Standard 201 (FIPS 201), *Personal Identity Verification for Federal Employees and Contractors*, to address the identification of Federal and contractor employees. The Federal departments and agencies shall meet the requirements of FIPS 201 no later than October 27, 2005 in accordance with the timetable specified in HSPD-12.

Concurrence

Rtg. Symbol	Initial/Sig.	Date
IM-31	A.Gardner	3/10/05
IM-30	C.Bales	3/10/05
IM-30	.Brody	3/10/05
IM-1	R.Parkes	3/10/05
NA-60	M.Kane	3/7/05
NA-65	L. WILBANKS	3/ /05
IM-1	GErrington	3/ /05
IM-1	R. Parkes	Date

SP-1
G. Podonsky
3/31/05

Project Management

DOE is establishing a Project Team (PT) with resources provided by SSA and the CIO, which will manage the overall implementation of HSPD-12. The CIO will administratively house the PT; Program Offices are requested to provide staffing for key positions. Representation from the Program Offices and the Laboratory environment is also highly encouraged. The PT will have primary responsibility for the engineering, design, procurement, coordination, deployment and support of a common solution for all DOE Elements, including the National Nuclear Security Administration, field sites and Management and Operations contractors. With the support of the DOE team, the PT will ensure a single solution is delivered economically and efficiently for the benefit of the whole DOE community.

Funding & Procurement

The initiative will be funded in accordance with Office of Management and Budget (OMB) direction to "Fund HSPD-12 using existing resources as necessary to meet deadlines established in the Directive." OMB has stated that the General Services Administration will be the Federal Government's centralized purchasing authority and executive agent for all HSPD-12 related items. Therefore, any pending or planned selection, purchase, major upgrade or acquisition of technologies, components or other technologies related to badging, physical access to facilities or logical access to information technology systems must be placed on hold until such a time as the PT has had an opportunity to determine requirements and issue subsequent guidance. All goals of the Department must continue to be met; therefore, if this procurement hold places other Departmental goals in jeopardy, Program Offices must assess and document the potential impact and provide findings to the PT for approval.

Next Steps

HSPD-12 requires agencies to interconnect badging, physical access and logical access systems to achieve electronic authentication and access control. In order to facilitate the work of the PT, a detailed inventory of the Department's infrastructure baseline will need to be performed expeditiously to ascertain current capabilities and "in-place" systems for the purposes of determining reusability and interfaceability. Accordingly, DOE Elements should expect to see a PT issued, DOE Enterprise Architecture Repository structured and facilitated data call in the near term. This data call will help the Department build a profile that includes site-by-site, building-by-building, vendor, and version specific information pertaining to hardware, software and systems used for badging offices, physical access control and logical access control.

Attached for information are the Plans of Action and Milestones for the four PT taskforces created to address immediate actions. If you or a member of your staff would like to participate on any or all of the taskforces, please contact the identified lead.

We appreciate the support of our DOE team in meeting the challenges of HSPD-12.

Questions should be directed to Mr. Bruce A. Brody, Associate CIO for Cyber Security at (202) 586-1090.

Attachments

cc: Susan Grant, ME-1

For Immediate Release
Office of the Press Secretary
The White House
August 27, 2004

August 27, 2004 Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

###

Source: The White House

This chart has been replaced by the 4 Separate task force PoA&Ms.
this chart should not be attached to memo. Thank you

Based on HSPD-12 & FIPS 201 requirements, the following actions are needed immediately by DOE

Action	Due By:	CIO	SSA	ME/ HR	ME/ SAOP	ME/ Procurement	IG	GC	NNSA
1. OMB Reporting. As has been discussed at Federal Identity Credentialing Committee (FICC) meetings, it should be expected that a significant reporting requirement to OMB will be soon forthcoming. While the task is still TBD, it can be expected that OMB will want to know the DOE specifics on implementation, costs, timeframe, a POA&M, and related topics.	AS REQ.	L	S		S		O		O
2. Procurement Cessation. All of DOE, to include field sites, M&O contractors, and all other elements, must stop any pending or planned selection, purchase, major upgrade or acquisition of technologies, components and other technologies related to; badging, physical access control to facilities or logical access to information technology systems until such a time as the PMO has had an opportunity to determine requirements and issue subsequent guidance. Expenditure of funding could result in buying nonstandard or non-compliant technologies. OMB has stated that GSA will be the Executive Agent for all purchases related to PIV.	3/31/05	S	S			L		O	O
3. Procurement Impact. HSPD-12/FIPS 201 applies equally to contractors and contract employees. DOE Procurement must determine how to best deal with the requirements of HSPD- 12/FIPS 201 and how to impart those requirements and notifications into all DOE contracts.	3/31/05	S	S			L	O	S	O
4. Inspector General/Agency Head Approval. FIPS 201 requires that the Agency IG must accredit the PIV-I process(es) stood up by the agency and certify that they meet FIPS 201. The Secretary must also approve the process in writing. A meeting has to be held with the OIG to inform them of their responsibility under FIPS 201.	3/31/05	S	S				L		O

L=Lead, S= Support, O=Optional

Based on HSPD-12 & FIPS 201 requirements, the following actions are needed immediately by DOE

Action	Due By:	CIO	SSA	ME/ HR	ME/ SAOP	ME/ Procurement	IG	GC	NNSA
5. Policy Impact. DOE must review all applicable Orders, Policy, Manuals, and related Guides pertaining to issuing ID badges, conducting background checks of personnel (employee and contractors) and hiring processes for the purposes of updating these documents to reflect the new requirements of FIPS 201, taking into account both PIV-I and PIV-II requirements. The review should produce proposed changes that will immediately go into effect and or produce new policy/guides, as required. Due to the short timeframe required by FIPS 201, implementation of these changes outside of REVCOM is recommended.	4/15/05	S	L	S	S	S	O	S	O
6. Re-credentialing Impact. Certain DOE badges have been issued without the requisite FIPS 201 background checks. An example is the badge referred to as BAO (Building Access Only) which can be issued without a NAC. DOE must determine the impact of re-verifying and re-credentialing these individuals and what adjudication processes it wants to invoke if, when an FBI fingerprint check is done, a derogatory or criminal history is returned on the individual that was previously unknown to DOE.	4/29/05	S	L	O	S	O	O	S	O
7. Foreign Born DOE Employees. DOE has a number of cases involving foreign born employees. DOE has to wrap the credentialing PIV process into this aspect of DOE workers.	4/29/05	S	L	S		S	O	S	O
8. Personnel. DOE federal employee personnel/HR processes will need to be examined and updated to incorporate the background check requirements into the hiring process before a badge is issued.	4/29/05	S	S	L	S		O	S	O

L=Lead, S= Support, O=Optional

Based on HSPD-12 & FIPS 201 requirements, the following actions are needed immediately by DOE

Action	Due By:	CIO	SSA	ME/ HR	ME/ SAOP	ME/ Procurement	IG	GC	NNSA
9. Privacy. FIPS 201 contains many specific, implied and derived requirements which are solely allocated to the Senior Agency Official for Privacy (SAOP). This individual/office is required to perform many duties and to have life-cycle processes in place to support PIV. The magnitude of the actions allocated to the SAOP tends to indicate that the SAOP needs a staff, separate from the PMO, to perform the requirements. The SAOP should analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts to perform the work required and to determine subsequent costs required for SAOP PIV-related operations.	4/29/05	S	S	S	L		O	S	O
10. Identification Management System (IDMS). Strongly implied in FIPS 201 is the need for a supporting IT system which manages the entire PIV process. This is separate from that which will control physical and logical access to facilities and IT systems. Without such an IDMS system, meeting the requirements of PIV-I and PIV-II will be difficult. The functions of this IDMS would be, but not be limited to, applicant monitoring, workflow, background check monitoring, ID issuance, revocation, update and maintenance. Any new supporting IT systems must consider the PIV-II requirements before being procured. The IDMS must interface with fingerprint readers, card printers and similar devices. The IDMS must be certified and accredited before it can be made operational. The CIO must analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts and perform the work required to determine the full extent of the requirements for this system, to see if such a system exists commercially, or if repurposing an existing capability could provide the services needed.	4/29/05	L	S	S	S	S	O		O

L=Lead, S= Support, O=Optional

Based on HSPD-12 & FIPS 201 requirements, the following actions are needed immediately by DOE

Action	Due By:	CIO	SSA	ME/ HR	ME/ SAOP	ME/ Procurement	IG	GC	NNSA
11. Competitive Sourcing Impacts. The IT Competitive Sourcing procurement that is currently on going may be greatly affected by HSPD-12 and FIPS 201. A workgroup should be formed of DOE experts to analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts and perform the work required to determine DOE's position on this topic.	4/29/05	L	S	S			O		O
12. Card Layout. Although not required until PIV-II, a cross-functional working group should be formed now to determine the format of and data elements for the DOE PIV smartcard. FIPS 201 provides many optional features and agency specified zones which DOE has to select from and standardize upon. This activity, performed now, will dovetail into the determinations and requirements for the IDMS and for policy changes, such that if a certain DOE feature is invoked on the smartcard, the IDMS specification has knowledge of that requirement.	4/29/05	S	L	S	S		O		O
13. IT System Impact. FIPS 201 Table 6-3 correlates the Assurance Level requirement of a particular IT system (Level 2=SOME, Level 3=HIGH and Level 4=VERY HIGH) to the specific PIV authentication mechanism(s) required to be used to access the system. Therefore, if a system is deemed through a certification and accreditation process to require a Level 2, 3 or 4 Assurance Level, then the individual accessing the federal IT system must use a government issued PIV credential, even if they are non-employees or non-contractors. If the system is deemed to require only an Assurance Level of 1, then it can be presumed that the PIV is not required to be used because there is no identification proofing requirement for that particular system. The CIO's Office must review all of the DOE IT systems to list and quantify their individual respective required Assurance Level for the purposes of quantifying cost impacts to those systems to accept a PIV credential.	4/29/05	L	S				O		O

L=Lead, S= Support, O=Optional

Based on HSPD-12 & FIPS 201 requirements, the following actions are needed immediately by DOE

Action	Due By:	CIO	SSA	ME/ HR	ME/ SAOP	ME/ Procurement	IG	GC	NNSA
14. Facility Impact. For determining physical access to a federally controlled facility by an employee, contractor, non-employee or non-contractor, physical access would be stipulated by that local facility's procedures, consistent with DOE policy.	4/29/05	S	L				O		O
15. Inventory. PIV-II requires agencies to interconnect badging, physical access and logical access systems to achieve electronic authentication and access control. In order to expedite this effort, the PMO will need a detailed inventory of the Department's infrastructure baseline to ascertain current capabilities and the potential reuse of "in-place" systems. A Department of Energy Enterprise Architecture Repository (DEAR) structured and facilitated data call must be performed. The data call will help the Department build a profile that includes site-by- site, building-by-building, vendor, and version specific information pertaining to hardware, software and systems used for badging offices, physical access control and logical access control. The CIO will analyze this issue, determine the full extent of HSPD-12/FIPS 201 impacts and perform the work required to resulting in a DEAR data call.	5/31/05	L	S				O		O

L=Lead, S= Support, O=Optional