HSPD-12 Implementation Guidance (Draft) Comment Matrix

Item Number	Source (Organization and/or Agency)	Section and Line Number	Comment	Proposed Change
1	Department of State (IRM/OPS/ITI/SI)	Section 1A, third bullet	The waiver for just DoD retirees, family members, and non-military eligible beneficiaries overlooks all other Federal Departments. While the military has the greatest number of people in this category, there are other Federal Departments that allow continued access to facilities and information systems by individuals in these categories, including retired annuitants, immediate family members living with/visiting employees overseas, and similar individuals.	Expand this proforma waiver to other Departments, especially the Department of State. Revise the text to read: "Within the Departments of Defense (DoD) and State (DoS), the directive applies to members of the Armed Forces, Foreign Service, and DoD and DoS Civil Service employees (including both appropriated fund and nonappropriated fund employees). This directive does **not** apply to retirees, family members, and other eligible beneficiaries."
2	Department of State (IRM/OPS/ITI/SI)	Section 1C, third bullet	The waiver for just academic locations overlooks contractor facilities who also conduct activities on behalf of departments or agencies or at which Federal employees may be hosted. It also does not bind the hosting activity to allow or accommodate the necessary physical requirements.	Expand this waiver to include contractor facilities meeting the same general criteria as academic locations. Revise the text to read: "Does **not** apply to academic or contractor locations who conduct activities on behalf of departments or agencies or at which Federal employees may be hosted unless specifically designated by the sponsoring department or agency, and included in contractual arrangements.
3	Department of State (IRM/OPS/ITI/SI)	Section 1D, second bullet	This allowance for remote access potentially opens up a significant hole in the overall security of information systems; in that if there are no controls at the distant end, then the Government has no real control over who may be accessing its networks.	Revise the text to read: "Applicability for the access of Federal systems by remote access is a department or agency decision, so long as that access meets the minimum Federal standards for networked systems or such access is limited to specific stand-alone systems and/or local area networks (LAN)
4	Department of State (IRM/OPS/ITI/SI)	Section 2A, third entry, and 2B, first entry	There appears to be a disconnect between the prescribed dates in these tables. Specifically, the "reference implementation to aid agency implementation" is released only two calendar days (Saturday & Sunday) before the deadline for agencies to "submit implementation plans." Having the reference implementation guidance appears critical to the development of a feasible and satisfactory plan.	Review this timeline and adjust accordingly

HSPD-12 Implementation Guidance (Draft) Comment Matrix

Item Number	Source (Organization and/or Agency)	Section and Line Number	Comment	Proposed Change
5	Department of State (IRM/OPS/ITI/SI)	Footnote #2	This document makes reference to draft NIST Special Publications that were not yet released at the time this draft document was released. It is now two weeks after the fact, and SP 800-73 is not yet released, and SP 800-76 is unlikely to be released prior to the mandated response date for this document. Further, this footnote implies, by omission, that these Special Publications are final.	Revise the text to reflect the reality of the situation that the two referenced NIST Special Publications were not released as indicated, and that they are still in draft.
6	Department of State (IRM/OPS/ITI/SI)	Section 3, Part 1E	This requirement is technologically impossible. It requires agencies to have interoperable e-authentication mechanisms "in-place" by October 27, 2005. The networking infrastructure absolutely required to support this capability does not yet exist. Further, the interoperable credential (i.e., the PIV Card) is not required until one year later.	Move the requirement to "Rapid Authenticate" to Section 3, Part 2.
7	Department of State (IRM/OPS/ITI/SI)	Section 3, Part 2B	This establishes a requirement to begin phasing-in the PIV Card for current employees and contractors on or about October 27, 2006 but establishes no completion date (reasonable or unreasonable). Agencies must be able to establish start/stop dates for budget submissions, to guide implementation plans, and measure progress.	Establish criteria for the phase-in and completion of PIV Card issuance to existing (as ov 10/27/06) employees, such as "upon end of lifecycle of existing non-PIV credential."
8	Department of State (IRM/OPS/ITI/SI)	Section 3, Part 2C	This requirement is directly tied to the requirement in Section 3, Part 1E (see comment #6 above). While reducing/eliminating reliance on visual authentication is an excellent goal, it presumes that there is a communications infrastructure in-place to support non-visual authentication and credential validation. This is not the case, and is unlikely to be the case by 102706.	Provide for the creation of the communications infrastructure to support the requirements of Section 3, Part 1E and Part 2C.
9	Department of State (IRM/OPS/ITI/SI)	Section 3, Part 2D	The text does not make clear that "identity proofing" means 100% Federal compliance with the provisions of PIV Phase 1.	Revise the text to read: "By September 30, 2007, identity proofing in accordance with PIV Phase 1 shall be on record for all current employees and contractors.

HSPD-12 Implementation Guidance (Draft) Comment Matrix

Item Number	Source (Organization and/or Agency)	Section and Line Number	Comment	Proposed Change
10	Department of State (IRM/OPS/ITI/SI)	Section 4, Parts 4A abd 4B	These two paragraphs establish an arbitrary list of preferred vendors, and grant GSA a monopoly on negotiating for products and services. Although mandating that products be tested to meet an established standard is necessary, the presumption that the products of this list of vendors are the best technology and the best price is unsupported in fact. It assumes that every agency's business case is identical to every other agency's business case in every situation. It also prohibits agencies from procuring a card that not only meets the standards, but may provide additional agency-specific capabilities at the best possible price. Finally, it places GSA in the unenviable position of monitoring agency compliance by requiring that GSA, in effect, report who is/is not using a "branded" card, and how well they are doing based on card purchases.	Review these requirements, and revise the text of Part 4B to read: "GSA Services—GSA is hereby…by the Directive. GSA will report to OMB annually on the activities undertaken as an executive agent. GSA will establish several procurement services for optional agency use including the use of Multiple Aware Schedules and blanket purchase agreements. Departments and agencies are encouraged to use the acquisition services developed by GSA; or may contract directly for products that meet agency-specific business case requirements, provided those products and services are compliant with the Standard and have demonstrated that the extablished criteria for interoperability are met. By March 15, 2005, GSA, in partnership..."
11	Department of State (IRM/IA)	FIPS 201	The method used for identity verification in the new ID card involves the use of biometrics and radio frequency identification (RFID). There may be issues concerning interception of sensitive data transmissions using RFID.	OMB may want to review or analyze this technology further.
12	Department of State (IRM/IA)	Question 5, page 7 of the Guidance	OMB does not make adequate provision in the guidance for protecting the sensitive information on users to be stored by the Department (reference Section 2.4 of FIPS 201).	Add details in the guidance as to what specific security controls are necessary for the storage, protection, retention, and destruction of the sensitive information to be used in implementing the ID process.
13	Department of State (IRM/IA)	Section 1D, page 4 of the Guidance	This section states that the applicability of remote access is a Department decision. This loose guidance may lead to users incorrectly electing to use COTS computers for remote access while the FIPS guidance is requiring two factor authentication (smart card and biometric devices) not normally found in COTS equipment.	Recommend the guidance be changed to require the use of GFE (government furnished equipment) for all remote access.

HSPD-12 Implementation Guidance (Draft) Comment Matrix

Item Number	Source (Organization and/or Agency)	Section and Line Number	Comment	Proposed Change
14	Department of State (DS/ST/FSE/DME)	Section 3, Part 2B	The first sentence infers that there is a different ID proofing process for Parts I & II	Change the text of the first sentence to read: Require the use of identity creditials for all new employees and contractors.
15	Department of State (DS/ST/FSE/DME)	Section 4, C.	The second sentence allows for card customization in limited circumstances with the approval of OMB. It does not, however, define the allowed circumstances nor the approval process	OMB needs to list the allowable circumstances and develop an approval process.