Social Security Administration Detailed Comments on
OMB Draft Implementation Guidance for HSPD-12

Item 1. D. Federally Controlled Information Systems
• Applicability for the access of Federal systems by remote access is a department or agency decision (e.g. researchers up-loading data through a secure website).

SSA Comment: Is all remote systems access discretionary (e.g. wireless networks)?

Item 2. What is the schedule for implementing the directive?

SSA Comment: Section A refers to a Department of Commerce item due 6/25/05 titled "Release of reference implementation to aid agency implementation." What is the relationship between this item and the Agency milestone "6/27/05 Submit implementation plan?" It would seem that the release of a reference implementation would provide limited usefulness in aiding the development of the Agency implementation plan with only two days separating their respective due dates. If the Agency implementation plan is to be based upon previous OMB guidance then what additional information will be provided by the Department of Commerce reference implementation?

Section B gives dates for Federal Information Processing Standard (FIPS) 201 Parts 1 and 2 that are clearly stated in the FIPS standard, but which do not reflect the "to the maximum extent practicable" language in HSPD-12 itself.
Item 3, "How should I implement the directive," does give latitude in implementation by restricting the requirement due on October 27, 2005 to "all new identity credentials issued to employees and contractors." The GSA handbook (section 2.3, page 12) goes on to say agencies may continue to use their current identification after October 27 as long as the issuance process complies with Privacy Impact Assessment (PIA) 1. Due to budget constraints, SSA needs this kind of latitude in implementation time frames, which we will reflect in the implementation plan due to OMB in June. Also, all documents should be consistent in addressing such details.

For SSA to meet the new identity proofing requirements for new hires, we must to conduct and adjudicate background investigations before an individual is given either physical and/or logical access. This process will have to be completed before an individual begins work at SSA. To accomplish this, SSA will likely have to initiate the background investigation process 60 to 90 days before an individual begins work to allow sufficient time to conduct and favorably adjudicate the required background investigation. Thus, the manner in which SSA hires employees and enters them on duty will be impacted. Hiring officials must allow considerably more lead time to begin the hiring process, and it would seem that Full Time Equivalent allocations will have to be made available considerably earlier than is currently the process. Further, background investigation workloads will increase, as some number of prospective hires may decline job offers after the investigation has been initiated, preferring to find other employment because of the delay.

Therefore, we suggest that some form of temporary credentialing be considered for an employee's first 90 days of employment prior to the required National Agency Check (NAC) and ultimately the NAC and Inquiry. Our past experience indicates that, in most instances, a favorable adjudication can occur within a 90-day period. Thus, the credential would automatically become permanent. Our view is that this would pose little risk as SSA currently verifies the identity of the individuals being hired even though a background investigation has not been initiated at the time of hiring. If potentially disqualifying information is discovered during the 90-day period, appropriate action to address the issue can be initiated or the temporary credentialing period extended for good and sufficient reason.

For current employees, SSA has thousands of long-term employees for whom background investigations were completed when they were hired; conceivably 30 to 40 years ago. It is possible that because of the passage of time, neither SSA nor the Office of Personnel Management (OPM) maintain data on these background investigations; OPM only maintains database records for 15 years. The manual review of Official Personnel Folders to determine whether an investigation was conducted will create a huge workload for SSA. As a result, we would strongly recommend that individuals who have been employed in excess of 15 years be grandfathered for credentialing purposes. This would, in our estimation, eliminate much of the workload and pose little risk to SSA since these are long-term employees whose identities are well known. This would make it possible for SSA to use automated databases to ensure that employees with 15 years or less service have investigations on file.

An additional impediment to timely implementation is the need to conduct impact and implementation bargaining for our bargaining unit employees. While we have not identified any specific obligations under the Labor-Management Relations Statute to coordinate this pre-decisional process, the implementation of this guidance will affect conditions of employment for bargaining unit employees. Therefore, once decisions are made, we would appreciate the opportunity to further review them, prior to implementation, to determine whether they may have any impact on the bargaining unit that would trigger any labor-management obligations under the statute.

Item 3. C Include language implementing the Standard in applicable contracts.

SSA Comment: Agencies must comply with this section on October 27, 2005. The GSA due date given in Item 2 to issue a Federal Acquisition Regulation (FAR) amendment is the same October 27, 2005 date. If agencies are to include HSPD-12 language in contracts, GSA will need to issue the FAR amendment considerably in advance of the October 27 date.

Item 3. D Complete the privacy requirements listed in section 5 of this guidance.

SSA Comment: Please see our comments below in section 5.

Item 3. Departments and agencies whose identity credentials can be verified electronically must:

E. **Rapidly authenticate –** Have mechanisms in place to take advantage of this capability in a manner that enables rapid authentication of the credential. Rapid authentication is the ability to check if the identity credential is valid without undue delay.

SSA Comment: The term "undue delay" is subjective. We suggest that a minimal acceptable time be provided (e.g. xx hours).

Part 2: Government-wide Uniformity and Interoperability

E. **System access–**

Compliance with the Standard requires the activation of at least one digital certificate on the identity credential for access control, the requirement to use this capability for access control to specific agency networks and systems should be based on the department's or agency's authentication risk assessments, required by OMB Memorandum M-04-04 dated December 16, 2003, "E-Authentication Guidance for Federal Agencies**." Ideally (but not required) employee and contractor system access should make use of the identity credential as part of the system access protocol.** Systems categorized as high-impact systems under FIPS-199 Standards for Security Categorization for Federal Information and Information Systems should receive priority integrating identity credentials into system access processes.

SSA Comment: The above paragraph appears to contain contradictory guidance. Are digital certificates required for System Access control or is their use discretionary?

Item 5. How must I consider privacy in implementing the directive?

When implementing the directive, you are already required under the Privacy Act, the E-Government Act of 2002 and OMB policy to satisfy privacy and security requirements. See section 2.4 of the standard for a summary of the privacy requirements. In addition, **prior to identification issuance or by October 27, 2005 you must:**

A. Ensure that personal information collected for employee identification purposes is handled consistent with the Privacy Act of 1974.

SSA Comment: SSA will only collect the necessary information for the specific purposes contemplated for employee/contractor identification, issuing badges and providing systems access. Once the decision is made as to whom the identification applies SSA will follow the tenets of the Privacy Act in collecting information and issuing badges and allowing systems access to the appropriate people. This means that SSA will comply with all aspects of the Privacy Act by providing adequate notice to all affected individuals of the information collection, and

- the reasons for the collection;

- expected uses;
- the impact of providing/not providing information;
- avenues of redress, amendment, correction, etc.; and
- the steps the Agency will take to protect the confidentiality, integrity and quality of the data.

SSA will not use the information in ways that are incompatible with employees'/contractors' understanding of how it will be used.

B. Assign an individual to be responsible for overseeing the privacy-related matters associated with implementing this Directive.

SSA Comment: SSA already has a Senior Official for Privacy and an SSA Privacy Officer to oversee privacy-related matters associated with implementing this Directive in place. Staff in the Office of the General Counsel, Office of Public Disclosure will provide staff support.

C. Prepare and submit to OMB a comprehensive PIA of your HSPD-12 program, including analysis of the information technology systems used to implement the Directive. The PIA must comply with section 208 of the E-Government Act and OMB M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. You must periodically review and update the PIA. Email your completed PIA to pia@omb.eop.gov.

SSA Comment: PIA preparation is dependent on many activities that have yet to be defined and undertaken by SSA. These activities cover everything from budgetary needs and systems requirements to personnel and contractor background checks. Once system design and preparation is started, we would be able to prepare a PIA. SSA will be able to prepare a PIA after the systems requirements and design phases of the system life cycle are completed. Given all these preliminary steps which must be accomplished it does not appear that the PIA can be accomplished by the due date posed by OMB.

D. Update pertinent employee-identification systems of records (SOR) notice(s) to reflect any changes in the disclosure of information to other Federal agencies (i.e. routine uses), consistent with Privacy Act of 1974, 5 U.S.C. 552(a) and OMB Circular A-130, Appendix 1.

SSA Comment: The SOR preparation, like the PIA, is dependent on other activities that are yet to be defined and completed. SSA's present SORs for employee access to building should be sufficient in the interim. SSA's Office of Public Disclosure has volunteered to work closely with OMB staff to draft language for use in SORs across the Government.

F. Develop, implement and post in appropriate locations (e.g., agency intranet site, human resource offices, regional offices, etc.) your agency's identification privacy policy, complaint procedures, appeals procedures for those denied identification or whose

identification credentials are revoked, sanctions for employees violating agency privacy policies).

SSA Comment: We will post all pertinent information on SSA's Intranet and appropriate internet websites once completed.

G. Adhere to control objectives in section 2.1 of the Standard. Your agency may have a wide variety of uses of the credential and its components not intended or anticipated by the Directive.

SSA Comment: Any other uses must be appropriately covered by the SORs and PIA.

Editorial comments from SSA's Office of General Counsel follow:

Pages 3 and 4: In the responses to question 1, "To whom does the directive apply?," the draft includes six references to either "the directive" or "this Directive." To ensure clarity in a document that refers in various places to "guidance," "Standard," "section," "Part" and "Directive," we suggest that each of the references to "the directive" or "this Directive" be replaced with "HSPD-12." We further suggest replacement of "the directive" with "HSPD-12" in each of the five questions that appear on page 3.

Page 5: Question 3 should be revised to read as follows: "How should I implement HSPD-12?" In the paragraph describing Part 1, "the Directive" should be replaced with "HSPD-12" to read as follows: "The minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12, including the personal . . . "

Under Part 1, a comma should be added after the date. That is, the introductory clause should read as follows: "By October 27, 2005, all . . . ."

In Part 1 A, we suggest adding a footnote following the word "Standard." The new footnote would be number "4" and read as follows: "As used in this guidance, "the Standard" refers to Federal Information Processing Standard 201. See note 1, *supra*."

In Part 1 B, the word "employee" in the second sentence should be changed to "employees."

In Part 1 C, the two commas in the first complete sentence are unnecessary and should be deleted.

Page 6: Under Part 2, a comma should be added after the date. That is, the introductory clause should read as follows: "By October 27, 2006, all . . . ."

In Part 2 B, the word "standard" in the second sentence should be capitalized, assuming that it refers to Federal Information Processing Standard 201.

In Part 2 C, the word “standard” in the first sentence should be capitalized, assuming that it refers to Federal Information Processing Standard 201.

In Part 2 D, the word “part” in the first sentence should be capitalized, as it is elsewhere in the guidance.

In Part 2 E, we suspect the first comma should be replaced with a semicolon to read as follows: “Compliance with the Standards requires the activation of at least one digital certificate on the identity credential for access control; the requirement to use this capability . . . .” The second sentence is missing a comma and should read as follows: “Ideally (but not required), employee and contractor access . . .” The footnote at the end of this Part will now be note 5.

Page 7: To ensure clarity, the first sentence of the response to question 4, “What acquisition services are available?” should be revised to read as follows: “To ensure government-wide interoperability, GSA will preapprove products and services procured by departments and agencies as meeting the standard.” The beginning of the second sentence should read as follows: “In partnership with the Department of Commerce, GSA will establish a process . . .”

In 4 B, “GSA Services,” the reference to “the Directive” at the end of the first sentence should be replaced with “HSPD-12.”

In 4 C, “Agency Customization,” the first use of the word “standard” should be capitalized.

In question 5 and in the first line of the response, “HSPD-12” should replace the two references to “the directive.” The word “standard” in the second sentence of the response should be capitalized. In the response to question 5 identified as “B,” “HSPD-12” should replace the reference to “this Directive.”

Page 8: In the response to question 5 identified as “C,” “HSPD-12” should replace the reference to “the Directive.” The next line, beginning “The PIA must comply. . .,” requires a comma after the date, i.e., “September 26, 2003, OMB Guidance. . .”

In the response to question 5 identified as “D,” a comma should follow the “i.e.” within the parentheses to read as follows: “(i.e., routine uses).”

In the response to question 5 identified as “G,” “HSPD-12” should replace the reference to “the Directive.” Similarly, in the responses to question 6 identified as “A” and “B,” “HSPD-12” should replace the three references to “the directive” or “this directive.”

In the response to question 7 identified as “A,” “HSPD-12” should replace the reference to “the Directive.”

Page 9: In the response to question 7 identified as “B,” the word “agencies” in the second sentence should have a possessive mark to read as follows: “This reporting will be incorporated into your agencies’ annual report . . “

In the response to question 7 identified as “C,” the topic sentence is missing a verb. It should read as follows: “Impact of Future Technical Guidance to be Issued by the Department of Commerce --”. The last sentence of the paragraph identified as “C” needs a comma to read as follows: “If you agency has a large scale deployment, you can use . . .”

In the response to question 7 identified as “D,” “HSPD-12” should replace the reference to “this directive.” The comma also should be deleted, and the sentence should read as follows: “Agencies with employees who serve undercover shall implement HSPD-12 in a manner consistent with maintenance of the cover and to the extent consistent with applicable law.”