From: David Sulser [mailto:david@sulser.org]
Sent: Monday, April 25, 2005 11:09 PM
To: FN-OMB-Eauth
Subject: Comments on OMB Draft Guidance for HSPD-12 of April 8, 2005

To: Jeanette Thornton, Office of E-Government and Information Technology
From: David Sulser, CISSP, CISM
Information Security Consultant
david@sulser.org
April 13, 2005

OMB released for public comment on April 8, 2005 the "DRAFT HSPD-12 Implementation Guidance for Federal Departments and Agencies" ("Draft").
My personal comments and questions on the draft follow.

Section 2.A. should be updated to include NIST SP 800-78.

Section 2.B. What is the anticipated publication date for the separate OMB guidance memorandum on the agency implementation plan that is due to OMB June 27, 2005? Announcing that guidance is forthcoming can have the effect of freezing agency plan development until the guidance is available.

Section 3, Part 1, paragraph B. Will there be any guidance forthcoming on how to accredit a process? Federal certification and accreditation as we know it from OMB Circular A-130, Appendix III and NIST SP 800-37, is aimed at major information technology systems (major applications and general support systems) not processes that are primarily human interaction as is the case with PIV-I. Of the recommended controls in SP 800-53, many of the management controls might apply, some of the operational controls might apply, but very few of the technical controls would be likely to apply.

Section 3, Part 1, paragraph E. Does the requirement for credentials that can be verified electronically (under PIV-I) extend to legacy proximity and contact cards? For agencies that currently do not verify cards electronically at entrance points, this would add an additional burden and require them to deploy additional readers that will be obsolete in 2006-2007.

Section 3, Part 2, paragraph D. Consider adding language similar to paragraph E such that persons in very sensitive positions should receive priority in replacing their credentials so that their older, less counterfeit-resistant ID cards may be destroyed.

Section 4, paragraph A. Is there today, or will there be before October, a smart card available that is guaranteed to be upgradeable to FIPS-201 specifications when they are all finalized? Or should agencies defer any new smart card purchases rather than lose their investment?

Section 4, paragraph B. What is the estimated cost for budgetary purposes of a fully FIPS-201 compliant card? If the recommended GSA acquisition services only become available July 31 as indicated in the Draft, that leaves agencies less than three months to acquire, integrate, test, certify and accredit their technology before the

October 27 deadline for new employee cards. Will there be an earlier date for a list of pre-approved products before acquisition services are complete? What is the anticipated date for products to emerge from the planned NIST FIPS 201 conformance validation facility?

Section 5, paragraph G. Are there any other criteria for determining what legitimate uses of the PIV credential are not covered by HSPD-12? On this question, paragraph 7A of the draft refers back to this section (5). Is there an example of a credential use not covered by the Directive?

Section 7, paragraph C. Title appears to have word missing, "Guidance to <
be> Issued..." In determining whether an agency has or has not
be> "implemented a
large scale deployment of identity credentials" is there a distinction among existing deployments of photo ID only, electronic, (proximity or contact) and ICC (smart) card credentials? If an agency is compelled or wishes to implement PIV-II and SP 800-73 prior to October 27, 2005 will there be sufficient compliant products available for purchase and integration into agency systems?

Thank you,
David Sulser
david@sulser.org