**Department of the Treasury Comments on DRAFT HSPD-12 Implementation Guidance for Federal Agencies as published in the Federal Register**

The Department of the Treasury thanks OMB and GSA officials for their efforts and appreciates the significant challenge of developing implementation guidance for implementing the requirements of HSPD-12. Treasury appreciates the opportunity to provide comments on this guidance. Overall, the DRAFT HSPD-12 Implementation Guidance provides clarification and is very useful. Our comments/questions are provided below:

**Comment/Question 1:** What is the definition of compliance for PIV I? Do we need to be putting all new employees and contractors through the new identity assurance process, or are we in compliance with the new requirements if we are using the new procedures to the maximum extent feasible by October 27, 2005?

**Comment/Question 2:** The NAC requirement appears to place a significant burden on agencies that do mass and seasonal hiring? For example, the IRS does seasonal hiring of hundreds of employees every tax year. The NAC portion of a background investigation can take several months to complete. As a result, requiring a NAC to be completed prior to credential issuance will have a large impact on the IRS mission. Consideration should be given to only requiring the favorable return of a fingerprint check for a credential to be issued? This process normally takes only a few days.

**Comment/Question 3:** During the two day meeting, it was stated that NIST FIPS PUB 201 requires a NACI to be updated every five years for credential re-issuance. It was later stated that there was no requirement for a NACI to be updated every five years. Can OMB provide clarification? The guidance indicates this must be done by October 27, 2005.

**Comment/Question 4:** NIST FIPS PUB 201 describes PIV 1 compliance in terms of processes and procedures being in place for an identity proofing and registration process and for a credential issuance and maintenance process. PIV 1 does not describe or imply the issuance of a PIV compliant credential to be issued. Two of the core objectives in FIPS PUB 201 Section 2.1 indicate that the credential issued must be rapidly authenticated electronically and is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation.

DISCUSSION:
Many of the badges currently issued in Treasury Bureaus do not contain chips needed for electronic authentication and do not contain the visual characteristics that would make the credential resistant to tampering, counterfeiting, etc. In order to comply with these two core objectives, agencies would be required to begin issuing new badges on or about October 28, 2005. Consideration should be given to the practicability and cost for agencies to issue new badges that satisfy these two core objectives in October 2005, knowing they must be issuing badges meeting PIV 2 requirements the following year, October 2006. Since there are no badges available on the market that meet the PIV 2 requirements today, this would force agencies to issue badges that must be replaced in a year or less.

RECOMMENDATION*:*
An erratum should be issued to the FIPS PUB 201 requiring the two core objectives mentioned above to be PIV 2 requirements and not a condition for PIV 1 compliance in October 2005. The OMB Implementation Template should be revised to clearly indicate that Control Objective B Statement 8 and 9 and Control Objective C Statements 10 and 11 apply to PIV 2 compliance only.

**Comment/Question 5:** The OMB Implementation Guidance requires the use of PIV cards for physical access to all federally controlled facilities, including Government space within commercial office buildings (Part 1.C. Federally Controlled Facilities). The Treasury Department believes this to be inconsistent with the intent of HSPD-12.

DISCUSSION:

a) During the FICC meeting on March 1, 2005, in which OMB and GSA officials presented draft implementation guidance to the Committee, it was abundantly clear from all members that the cost and resources needed to modify physical access control systems at tens of thousands of federal facilities was difficult to achieve in the current budget circumstances;
b) On its internet site, NIST has included its own clarification of FIPS 201 through a series of FAQ's (see: www.nist.gov/public_affairs/releases/piv_faqs.htm). Question #23: "Does compliance to FIPS 201 mean that every door in every federal building and every federal computer terminal must have a PIV card reader?" Answer: "As agencies develop their plans in accordance with HSPD-12, they should focus on the highest-risk facilities and systems for initial deployment of readers. Over time, this could expand to lower-risk systems and facilities";
c) HSPD-12 itself narrows the fiscal focus of the requirement to both "variations in quality and security of identification" and "access to secure Federal and other facilities where there is potential for terrorist attacks";
d) It should also be noted that the OMB appropriately recognizes the need to apply the limited available resources first to securing high risk information systems. See OMB Guidance, page 6, Part 2.E. System Access, which states: "Ideally (but not required) employee and contractor system access should make use of the identity credential as part of the system access protocol" and that "high impact systems under FIPS 199 should receive priority".

RECOMMENDATION:
The 2nd bullet under Part 1.C. Federally Controlled Facilities should be deleted. Replace the 1st bullet with: Federally owned or leased buildings, determined as high risk through agency implementation of HSPD-7, Interagency Security Committee standards, and other federal policies. Further implementation shall be accomplished as much as practicable. The GSA and FPS will coordinate, as much as practicable, the implementation of PIV card access to all leased space under their jurisdiction.

**Comment/Question 6:** The directive does not address federal law enforcement badging and credentialing. The guidance states that it applies to, "...employees and contractors who require long-term access to federally controlled facilities and/or information." In some cases, law enforcement officials may use their ID for this purpose, and hence the guidance would apply. In other cases, they also use their credentials to knock down doors and identify themselves away from federally controlled facilities and/or information. In this latter case, law enforcement officers tend to argue that they want to keep their current "visual identification" and not adopt any new standard credential. Every separate law enforcement entity issues its own unique badges and multi-part credentials that list the officers'/investigators' authorities. These badges and credentials have been counterfeited and stolen and found their way into criminals' hands. By applying the new standards to law enforcement badging and credentialing, OMB would improve identification control among a very large and diverse group of Federal employees.

Again, thank you for all of your efforts. I hope our comments are of value.