EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

July 3, 2003

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS OF DEPARTMENTS AND AGENCIES

FROM: Mark Forman
Administrator for E-Government and Information Technology

SUBJECT: Streamlining Authentication and Identity Management within the Federal Government

As we work to achieve the President's vision of creating a more responsive and cost-effective government, we must look for opportunities to improve processes and consolidate investments to deliver the kind of breakthrough results that citizens are looking to us to deliver. One such opportunity is in the area of e-authentication and identity management which is being led by the E-Authentication E-Gov Initiative. The Federal government is spending in excess of $160M in FY03 and FY04 on potentially inconsistent or agency-unique authentication and identity management infrastructure. Agencies also have inconsistent approaches to both physical security and computer security, which lead to increased risks to the Federal government and the people with whom it interacts. Finally, there is a burden on the public in interacting with the government by having to maintain multiple credentials and not being able to access the services they need using those credentials. It is clear that a cross-agency approach for authentication and identity management is a better alternative.

The purpose of this memorandum is to update agency CIOs on the next steps for the E-Authentication Initiative, and detail specific actions that agencies should undertake to support that plan by coordinating and consolidating investments related to authentication and identity management.

The Federal government has not only the opportunity, but also the legislative direction to drive true transformation in this area. We can achieve significant cost savings through aggregated acquisition planning and infrastructure consolidation, which is supported by Section 5113 of the Clinger-Cohen Act (P.L. 104-106) in its requirement for agencies to use common information technology solutions. We can facilitate information sharing while protecting government resources from unauthorized access by implementing common authentication and identity management processes, which is addressed by Section 3544(a) of the Federal Information Security Management Act (P.L. 107-347) in its requirement for agencies to provide information security protections for its physical and electronic resources. We can reduce the burden on the public when interacting with government by allowing citizens to use existing credentials to access government services and enabling new services that otherwise could not or would not have been available. These are addressed by Section 203 of the E-Government Act (P.L. 104-347) which requires agencies to ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director of OMB. This interoperable electronic

signature framework also removes a key barrier to agencies' implementation of and compliance with the Government Paperwork Elimination Act (P.L. 105-277).

Over the coming months, we will be executing several key actions based on cross-agency recommendations and are requesting your support and commitment in these endeavors. First, we are developing common policy for authentication and identity management, including the release of government-wide e-authentication and technical guidance from GSA and NIST. This includes the development of a common, comprehensive policy for the credentialing of Federal employees through the efforts of the newly created Federal Identity and Credentialing Committee (FICC). To ensure that your agency's requirements are accurately reflected in the forthcoming policy, **agencies should provide input into the policy and requirements efforts of the FICC in the areas of human resources, physical security, and IT security**.

Second, we are executing Federal-wide acquisitions of authentication technology, including smart cards, digital certificates, and other electronic credentials (e.g., PIN/password) to achieve cost savings in the near-term. **Agencies should support the execution of these Federal-wide acquisitions by refraining, to the maximum extent possible, from acquiring authentication or identity management technology without prior consultation with E-Authentication and the FICC**.

Finally, we are consolidating agency investments in credentials and PKI services. Shared service providers will be selected by the end of CY03, with agency migrations to those selected shared service providers occurring throughout FY04 and FY05. There will be no new funding in FY06 for authentication or identity management investments not related to the selected shared service providers. We will be providing additional guidance on the development of the business case for this initiative. **Agencies should develop migrations plans to the shared service with planning work beginning now and a final plan expected following the selection of the shared service providers**.

I appreciate your agency's assistance and continued cooperation on this critical Presidential E-Government initiative. We all desire a more effective and efficient government. Your leadership and commitment will empower the E-Authentication initiative to coordinate on-going efforts in this area and deliver benefits to both the citizens and the government. The OMB point of contact for this initiative is Jeanette Thornton, E-Authentication Portfolio Manager, jthornto@omb.eop.gov.