HSPD-12 Public Meeting
Karen Evans Remarks
8:40-9:10

On behalf of the Office of Management and Budget, the General Services Administration, and the Department of Commerce, I'd like to welcome you to a public meeting on the Common Identification Standard for Federal Employees and Contractors.

As OMB's Administrator of E-Gov and IT, it is my job to promote effective and efficient information technology, security and privacy --- a delicate balancing act.

The Federal government was directed by the President to strengthen identification issued to employees and contractors. We know the thought of a standardized ID card causes some angst. This is why we are having this meeting—we want to get advice on how we can meet the President's Directive AND provide identification designed to protect privacy. When the first meeting filled up within days of the Federal Register notice, we immediately scheduled a second meeting. The afternoon session soon filled up. We still have turned some away. This is when thousands of people are coming into DC for the inaugural festivities, and others are in the process of fleeing as fast as they can to beat the traffic.

Today's conversation is important and necessary. Leading up to this meeting, the Department of Commerce hosted two industry and one government workshop to seek input. These meetings were focused on the technology --now its time to discuss policy and privacy. Today you'll hear the views and recommendations of recognized experts on issues associated with the Directive. The information will inform future OMB guidance to Federal agency heads. Staff members responsible for drafting the standard from the Department of Commerce are also in attendance.

Let me start off by talking about the history behind the Directive and some of the work already completed. I want to also spend time talking about the delicate balance of privacy and security.

We operate in a world where the capabilities of technology are rapidly expanding. At the same time, we must ensure the government addresses security needs without eroding privacy.

In February of 2003, the National Strategy to Secure Cyberspace was released. The strategy asked agencies to ensure people on government systems are who they say they are and are doing what they are authorized to do.

To follow the strategy, in July of 2003, the Office of Management and Budget recognized millions of dollars were invested annually for incompatible processes and systems, some with questionable value and performance. We recognized some IDs currently issued by Federal agencies could be forged or stolen. This would allow access by unauthorized individuals. We recognized there was no minimum standard across the government to allow us to trust each others identification. We recognized it was time for agency computer security, physical security, and human resource experts to work together on a unified approach.

Standardized identification has the potential to significantly improve the process of verifying the identity of people accessing federal buildings and computer systems, especially when used in combination with other technologies. In 2003, we formed a group of agency experts called the Federal Identity Credentialing Committee to develop a common policy for the credentialing of Federal employees.

The President told us to be more aggressive with the work we were doing. As I'm sure most of you know, on August 27, 2004 the President signed the Homeland Security Presidential Directive titled "Policy for a Common Identification Standard for Federal Employees and Contractors." The objective is to ensure the identification for government employees and contractors is reliable and can be easily verified, visually by a security guard at the front desk and electronically.

As a result, the Federal Government has developed and will implement a government-wide standard for secure and reliable forms of identification. This identification is for employees and contractors who work at Federal facilities. This identification should eliminate inconsistent approaches to facility security and computer security.

This directive established extremely tight deadlines which the government will meet. The Department of Commerce is required to issue the standard by February 27th. The draft Commerce posted for public review in early November received over 1900 comments from over 90 individuals, agencies and public interest groups. I understand from Commerce a number of changes to the public

draft have been made in response to comments, which are posted on the Commerce's website.

On the agency side, Agencies must complete their implementation plans by the end of June. By October of this year (not next year), agencies have to require use of IDs that meet the Standard.

A common standard makes sense from an efficiency standpoint. We have a history of requiring our Federal facilities to be secure, going back to an Executive Order issued by the Eisenhower Administration. Too often government resources are wasted, when agencies try to customize to meet their needs. A common standard will eliminate this inconsistency. Today, many Federal employees who have to visit multiple locations wear multiple ID cards around their necks. One agency may not trust an ID issued by another agency.

We gain efficiencies in operating as one government --- we don't want each agency to go it alone.

But, with efficiency comes a need for limits and strict guiding principles. The key question is how we strike the balance between protecting our Federal

resources and protecting the privacy and security of those who come to work for us everyday. We want our valued employees and contractors to be confident the government will use technology appropriately. Sounds good, right? But as you know the devil is in the details. As many of the industry members in the audience will tell you, the capacity of identification and identity management technology is constantly growing. When agencies implement this directive, the privacy of your Federal employees and contractors must be protected.

Today we are looking for your views on specific issues.

You are about to hear about specific actions we can take to address privacy and security in the development of the standard and implementation guidance. We want to build privacy enhancing technologies into the card. We want to ensure uses of the card are appropriately controlled. We want to ensure employees and contractors receive the necessary training to properly secure their cards.

Card holders must have a clear understanding what personal information is being collected from them and why. Agency security personnel must be appropriately trained. We want to put in place protective measures to ensure personal information stored on a card can't be accessed inappropriately.

These requirements are based on a longstanding policy framework enforced by OMB. Agencies must ensure consistency with existing privacy and security law and policies. The Privacy Act, E-Government Act, and other OMB policies, are a few examples, which I expect our speakers to address in their remarks.

Some of today's speakers will address the use of smart cards, both those with "contact" chips, and those employing wireless or RFID type technology.

You'll hear about the benefits and privacy concerns associated with biometrics. Most Federal employees on their first day of work are fingerprinted – this is often done with paper and ink and not electronically. Since we are moving to an electronic system of fingerprint capture, we need to prevent the reading of this information without the knowledge or consent of the individual.

You can't have a discussion on identification without talking about ID numbers. I hope to hear how we can design numbering systems to protect privacy and minimize the linkage to a particular individual. We need to ensure this number doesn't become persistent and follow someone from job to job.

I'm sure these are only some of the issues you'll hear discussed.

Closing

In closing, I'd like to thank all of you for coming. Your questions and comments will help inform the discussion and our policy decisions.

I'd also like to say how pleased I am to see how many industry members are here today. Its good to see you take the initiative to address privacy concerns and incorporate these considerations into your products and services.

Privacy is a critical issue for the Office of Management and Budget and the Federal Government as a whole. Today, represented here are representatives from both large and small Federal agencies, including many agency privacy officers. To address privacy we need to work as a team, and I promise to play my part.

We have an impressive list of speakers, so it is now time to hear what they have to say. Thank you. I now turn it back to John who will introduce the first speaker.