Record of Public Meeting Addressing Privacy and Policy Issues in a Common Identification Standard for Federal Employees and Contractors

January 19, 2005

On Wednesday, January 19, 2005 the Office of Management and Budget (OMB) and the General Services Administration (GSA) co-sponsored an all day meeting to hear and collect public comments regarding Homeland Security Presidential Directive-12 (HSPD-12). HSPD-12 mandates the issuance of a standard identification card to all federal employees and contractors doing long-term business with the federal government. The meeting was held at the Potomac Center Plaza, 550 12th Street, Southwest Washington, D.C.

Session One

The morning session began at 8:40 a.m. and was attended by approximately 200 people.

Overview of Agenda/Logistics

John Sindelar, Deputy Associate Administrator, Office of Governmentwide Policy, General Services Administration

Mr. Sindelar welcomed everyone and gave an overview of the morning agenda. He indicated there would be six speakers who would provide their comments regarding several issues surrounding the implementation of HSPD-12. Mr. Sindelar stated that Ari Schwartz, Pam Dixon and Dr. Amitai Etzioni would comment on the privacy implications of the directive then Jim Byrne, Daniel Chenok and Dr. Robert D. Atkinson would comment on the potential technologies to be used to implement the standard ID cards.

Opening Remarks

Karen S. Evans, Administrator E-Gov and IT, Office of Management and Budget

Before the speakers started their presentations, Mr. Sindelar introduced Karen Evans and indicated she would make opening remarks. Ms. Evans introduced Jeanette I. Thornton, Policy Analyst, Executive Office of the President, OMB, as a key staff member.

Ms. Evans indicated that the meeting was being held to get advice on how the government could meet the President's Directive to provide a standardized ID card and protect privacy. She indicated that the Department of Commerce had held two workshops seeking input on the technology involved in the implementation of HSPD-12 but that it was time to discuss policy and privacy. Ms. Evans indicated that HSPD-12 established extremely tight deadlines that require the Department of Commerce to issue the standard by February 27th and agencies to complete implementation plans by the end of June and implement use of IDs that meet the standard by October 2005.

Ms. Evans indicated that a common standard will eliminate inconsistency and the waste of government resources. She acknowledged that with efficiency comes a need for limits and strict guiding principles. Ms. Evans indicated the key question is how to strike the balance between protecting our federal resources and protecting the privacy and security of those who come to work for the government everyday. She assured the audience that the government wants to build privacy enhancing technologies into the standard ID card and ensure that card use is appropriately controlled. She further stated that the government wants to put in place protective measures to ensure that personal information stored on a card can't be accessed inappropriately. Ms. Evans indicated that the expert speakers would address the use of smart cards (those with contact chips and those employing wireless or RFID type technology), the benefits and privacy concerns associated with biometrics (particularly the electronic system of fingerprint capture), and designing a numbering system to protect privacy.

Ms. Evans ended by acknowledging the presence of representatives from both large and small federal agencies, including many agency privacy officers.

(*See Attachment 1, a copy of Karen Evans' prepared remarks)*

Privacy Policy Principles
Ari Schwartz, Associate Director, Center for Democracy and Technology

Mr. Sindelar returned to the podium and introduced the first invited presenter, Mr. Ari Schwartz. *His comments closely followed his PowerPoint slide presentation on "Privacy and Other Policy Issues in Common ID for Federal Employees and Contractors."*

Mr. Schwartz indicated there is a need for a common ID standard because the current system does not adequately protect security or privacy. Mr. Schwartz voiced several concerns. His primary concern is that technical standards are being set before a policy framework is established. He emphasized that policy discussions need to come first. He stated that security and privacy require equal weight to people, process and technology but, thus far, there has been a heavy emphasis on technology. Mr. Schwartz is also concerned that there are no policies to limit misuse and overuse of standard ID cards. He stated that HSPD-12 is silent on the use of backend data and that cards must be used in the right way to avoid insider user fraud.

Finally, he stated his specific technical concerns with: the storage of actual fingerprint images instead of templates; contactless chips; and persistent use of the ID. He recommended that detailed privacy sensitivity and other policy training be provided but indicated it hasn't been built into the plan. He also stated that Privacy Impact Assessments (PIAs) are needed immediately even for agencies that are exempt under the E-Government Act if they are changing cards. He concluded by reiterating that the development of policy should have happened earlier in the process and that mission creep must be avoided at all costs.

(*See Attachment 2, copy of PowerPoint slide presentation of Ari Schwartz)*

Privacy Policy Principles
Pam Dixon, Executive Director, World Privacy Forum

Ms. Pam Dixon was introduced as the next invited presenter. *There were no substantive variations between her comments and her PowerPoint slide presentation on "The New Federal ID Card: Privacy Implications."*

Ms. Dixon stated there were many privacy risks associated with the use of a standard ID card (mission creep; card ID number would be subject to same abuses as SSNs; length and manner of storage/access for original source documents such as birth certificates; personally identifiable information (PII); transactional data mining; real time tracking; unauthorized use, access, disclosure, disruption, modification or destruction; data matching; inability to limit use by private sector; background check implementation and application across agencies; proposed use of the card for press members; use of live test data by vendors; lack of appeal and redress procedures; lack of a specific plan for audit, access control, protocols, training; lack of substantive PIA, Privacy Act compliance).

Ms. Dixon felt that privacy impact assessments (PIA) should be done immediately by the lead agency and applied to all affected agencies. She outlined the required elements of a PIA (what information s to be collected; why the information is being collected, intended uses of the data; with whom the information will be shared; what opportunities individuals have to decline to provide; how information will be secured; whether a system of records is being created under the Privacy Act).

Ms. Dixon concluded by stating there are other questions and issues involved with the implementation of HSPD-12 including security risks with the card relating to the technology; legislation to strictly limit the use of the card; employee privacy training; Privacy Officer dedicated to this issue.

(*See Attachment 3, copy of Pam Dixon's PowerPoint slide presentation)*

Privacy Policy Principles
Dr. Amitai Etzioni, Founder and Director of the Communitarian Network

Dr. Etzioni spoke extemporaneously. He told the audience he was concerned with safety and the lack of progress in this area between the first and second attack on the World Trade Center. He indicated that the documentary film, "The Dirty War," dramatizes the importance of a standard ID. He said that agencies must share information with each other. He noted that when people try to enter federal buildings with fake ID's, they are successful. They can even enter safe houses with false ID's. The best way to reconcile concern for privacy is to increase accountability, and supervise the use of a standard ID. He recommended that an Independent Review Board be established.

Dr. Etzioni indicated that mission creep should be looked at as a collateral gain. He noted there is no right to have a false ID. If a national ID card were used, you would be required to have it with you at all times and the police could stop you at anytime and ask you to identify yourself. The standard ID is for use in a specific area. The system can be abused but the notion that the system cannot be used for other purposes should be reviewed. Dr. Etzioni stated that driver's licenses are used to establish ID in the private sector (for instance to board airplanes) but this is a joke in the aftermath of 9/11. He informed the audience that in late 2002 and early 2003, GAO agents were able to enter the United States using counterfeit driver's licenses without being stopped 25 out of 25 times yet the airlines are opposed to a standard ID. Dr. Etzioni said that IDs and birth certificates are easy to fake. He also stated that "States don't even check the validity of SSNs" and "Standard IDs should be adopted for state use". Dr. Etzioni ended by asking the audience, "How far do you go with protecting privacy" and "When should security concerns receive priority over privacy concerns".

Dr. Etzioni provided the audience with a copy of a recent article from *The Washington Post*, "It's Not Just A Driver's License Anymore," dated May 16, 2004 and referred them to his book, "How Patriotic is the Patriot Act?"

Following Dr. Etzioni's comments, there was a fifteen minute break.

(*See Attachment 4, copy of Dr.Amitai Etzioni's presentation notes)*

Technology and Privacy

Jim Byrne, Co-Chair, Information Technology Association of America's Identity Management Task Group

Mr. Byrne was the first presenter after the break. He spoke from prepared notes. Mr. Byrne described himself as the industry evil guy. He informed the audience that he represented a trade association and there were 400 companies participating in the Identity Management Task Group. He indicated that they want a more secure environment for federal workers and believe it is important to put policy in place before technology. The issue of security as it relates to privacy was Mr. Byrne's focus. He stated that technology questions related to security need to be addressed as it relates to policy; not "how to do it" but "what to do" is the question. Security is the enabler of privacy. The decision to add more security may increase privacy solutions.

Mr. Byrne felt that the proposed standards do not include sufficient level of detail to allow industry to make any substantial assessment. A policy on whether contact or contactless cards should be used has not been established. He indicated that industry has been building solutions with government for many years and given timelines and level of detail required to implement HSPD-12, a cooperative effort between government and private industry is necessary.

He stated that the issue is not whether technology exists but whether technology supports policy. Many elements need to be addressed: information capture, retention, biometrics, image vs templates, centralization, contact vs contactless, and encryption. Mr. Byrne stated that without policies, questions about technology cannot be answered. It's not a "does technology exist" question but "how do you want to use the technology?" The industry around smart cards has evolved exponentially over the last few years. Technology can support just about anything but policy has not been established.

Mr. Byrne concluded by stating that we have to design a card where data on the card is not being kept in other places. He noted that HSPD-12 has aggressive timelines especially since technology is being designed without policies in place.

(*See Attachment 5, copy of Jim Byrne's presentation notes)*

Technology and Privacy

Daniel J. Chenok, Vice President and Director, Policy and Management Strategies, SRA International, Inc.

Mr. Chenok's comments did not vary substantively from his PowerPoint presentation ("Privacy Issues in HSPD-12 Implementation: Principles for the Government to Consider").

Mr. Chenok stated that policies must come first. He noted that privacy and security are two of the most important factors in the implementation of the systems that implement the standard; that technology media can be managed well or poorly from a privacy and security perspective; that the overall architecture of the system and the policies that govern data collection, data uses, data storage and retention will be integral to the effectiveness of the system; and that agencies should consider privacy and security issues across the entire identity management system across its life cycle.

Mr. Chenok focused on four principles for privacy protection: transparency, minimization, architecture and life cycle. He stated that transparency must be provided for individuals whose credentials are stored based on the standard (individuals must know how cards are to be used). He also stated that we must minimize data collection, use and storage in card implementation (need to develop policy that controls and limits use of ID cards beyond primary purpose for which they are created. If there is less mandatory information on card, privacy is increased). He recommended that the government consider architecture options that do not centralize collection and storage of personal information and that privacy considerations are incorporated in all phases of system development and implementation. Mr. Chenok also recommended that general Privacy Impact Assessment be adopted for all government agencies but that the PIA should be tailored for each agency.

(*See Attachment 6, copy of Dan Chenok's PowerPoint slide presentation)*

Technology and Privacy

Robert D. Atkinson, Vice President and Director of the Technology and New Economy Project, Progressive Policy Institute

The last presenter during the morning session was Dr. Atkinson who spoke on the issue of technology and privacy.

Dr. Atkinson stated that we need to modernize the state driver's license system and the federal ID system. He felt some of the issues raised on privacy are really red herrings designed to scare people; these issues are raised by people who are scared of technology. He thought there may be a few legitimate issues:

- Privacy issues regarding federal employees already exist.

- How would employees be protected if smart cards are lost or stolen? A card with biometrics can't be used by someone else.

- Need for appeal is necessary if more stringent background checks are required to get ID and they can lose their job if they can't get a card.

- Storage of birth certificate is irrelevant since they are already being stored by the state. Storage of private documents in and of itself is not a privacy issue.

- Cards would be issued to employees, not citizens, so the numbers are not a privacy issue.

- Mission creep is not a bad thing. Increasing functionality of the cards is good. The chip for metro card can be included on the federal ID card. That means federal employee doesn't have to carry two cards. Smart cards should be designed for both federal and private use. In Europe, smart cards can be used to get out of a garage. You should be able to use smart cards to get into a hotel room. Other applications should be placed on federal ID cards.

- The Federal ID card is not a National ID card. We need mandatory state driver's license with biometrics and chips on them anyway.

- Contact vs contactless cards is not really a privacy issue.

- We oppose putting fingerprint on card. This is over the line. It's much better to have a template rather than actual fingerprint.

- Unencrypted data on a contactless card would be a mistake and raises significant privacy concerns.

- Tracking employees with new technology is not a legitimate concern. An employer has a right to know where employees are during work hours.

He ended by referring the audience to "Technological Innovation without Big Brother", an article that asserts that privacy issues are not a legitimate concern.

(*See Attachment 7, copy of Robert D. Atkinson's presentation notes)*

Questions and Answers

The morning session concluded with an "open microphone" period during which audience members directed questions to the presenters as follows:

Question: Are there levels of security protection that can be used in contact-less cards?
James B. Sheire, Manager, Government Programs, Philips Electronics North America Corporation, Washington, D.C. (202) 962-8550

Answer: I think we're talking about major risks. This is a controversial issue in card technology that's not worth the risk. We are recommending that it not move forward. Authentication of readers is necessary.
Ari Schwartz, Associate Director, Center for Democracy and Technology

Follow-up: Philips would be happy to provide a briefing on contact-less features for these cards.
James B. Sheire

Question: Has there been a survey of federal employees to determine how they feel about the card?
Vera Stevenson, National Labor Relations Board

Answer: There has not been a survey. OMB is in the process of determining how it will implement the standard.
Jeanette I. Thornton, Policy Analyst, Executive Office of the President, OMB

Question: {paraphrased} Have we been doing a PIA on policies being put forward.
Zaida Candelario,Privacy Program Analyst, Office of the Privacy Advocate, IRS, Washington, D.C. (202-927-6785)

Answer: Policy needs to be evaluated on an ongoing basis.
Jeanette I. Thornton

Question: I'm a private investigator and a reporter. We're on extremely dangerous ground. Privacy in America is a myth. I've made my living invading people's privacy. This is a precursor to a National ID card which is dangerous to people's liberty. The privileged elite will have access to federal facilities that people have paid for. Buildings do not belong to the government. We should have the ability to use

them. You have legitimate need to limit access to buildings where there are weapons. The federal ID is reprehensible. The federal ID card will affect federal employees, contractors, members of the press and a wide variety of members of the public. Why should we require these intrusive measures to have access to what we have paid for. We recognize that the War on Terror requires some stricter measures . Use of cards will dramatically expand to areas all across the United States. It will be like living in Russia. I got in this building today. I wasn't checked for anything and I don't have a pass. Security always fails with minimum wage rent-a-cops. A more thoughtful approach is needed. Ramifications of what you are doing will affect America for a long time. I was taught at a Police Academy that when you begin to surrender your civil liberties, the terrorists have won. Bin Laden has won this war.
Patrick M. Clawson, Private Investigator, Flint, MI (810-730-5110)

Answer: None required.

Question: We need a common sense approach to security; not privacy. What happened on 9/11 was a security problem, not a privacy problem. HSPD-12 mandate to make electronic ID is a foolish idea. Computer assisted, hardware-software is not a substitute for security. Smart cards can't support security. The 9/11 terrorists were smarter than people charged with protecting us. Artificial intelligence is not better than people intelligence. There is no balance between security and privacy. Security is like pregnancy. You can't be a little bit secure. Nuclear weapons are not being used because countries have secure systems.
Dr. Dmitry A.Novik, Digital Imaging General, DIMAGE, Inc., Washington, D.C. (202-333-8956)

Answer: None required.

Question: There is a need to involve actual employees who will be using the cards in the formulation and implementation issues. Unions would like to be consulted before issuance of guidelines by OMB. Policies need to recognize use of authorized pseudonyms. ID cards must be issued in the name of pseudonyms that have been authorized for employee protection. We are concerned about use of cards to track employee movement in buildings. We don't want cards used to track employees improperly. Cards for long-term visitors should be analyzed. Who's paying for these cards? Timelines don't seem realistic. How are privacy concerns expressed here today going to be addressed? Will GSA or OMB answer questions?

Barbara A. Atkin, Deputy General Counsel, National Treasury Employees Union, Washington, D.C. (202-572-5500 x7005)

Answer: Transcripts of meeting will be posted on website. Those involved in drafting standards are present and will insure that comments are incorporated. OMB is in the process of developing guidance and will obtain input from federal agencies.
Jeanette I. Thornton

Follow-up: I hope employees at federal agencies will be allowed an opportunity for comment.
Barbara Atkin, NTEU

Question: I participated in national and international standards efforts. There was widespread participation of federal and private sector. I want to address the storage of templates on cards instead of images. Standards that have been developed for image storage require that data be encrypted whether it is image or template data. When there is storage of templates instead of images, in many cases it is not a difficult task to take a stored template and produce a similar template. Storing templates is not the right solution. Encrypting data is the right solution.
Jim Cambiara, Meridien

Answer: None required.

Question: Will this be limited to federal employees and contractors within DC?
David Y. Lee, Program Analyst, Office of Inspector General, Department of Commerce, Washington, D.C. (202-482-5322)

Answer: All federal employees and contractors will be affected. Agencies will be required to go through a funding process.
Jeanette I. Thornton

Question: Our agency has already prepared the Exhibit 300 and submitted its budget. What will be done to redirect those funds?

Answer: I can’t comment on budget issues.
Jeanette I. Thornton

Question: I am a former federal employee and contractor. There are a lot of privacy concerns that can be addressed by policy. This is not the first time the government has issued ID cards. When barcodes first came out, everyone was upset. DOD used smart cards 10 years

ago but called it “The Marc” which upset many people. They renamed their cards and it is a very good program for controlling access. A driver’s license is similar to a National ID card so it would be better to have one that is built with better technology. You need to explain contact-less technology; it’s not the same as RFID. Contact-less cards have chips but are designed to track only a few feet. We need to look at what technology is a threat and what technology is not a threat to allay concerns of people.
Jeremy Grant, VP, Maximus, Rockville, MD (240-306-6018)

Answer: None required.

Question: We have talked about biometrics. My company does fingerprinting. Technology can protect privacy. Technology can provide benefits and counter risk. You must evaluate how you want to use technology. You cannot know by looking at a fingerprint how a person looks, how old he is or where he comes from. But a driver’s license gives you a picture, age and address. When you show your passport at the airport, the airport personnel knows more about you. Biometrics is a more secure method.
Teresa Wu, Marketing Specialist, SAGEM MORPHO, Inc., Alexandria, VA (702-797-2666)

Answer: None required.

Question: I need clarification on who will be required to have the card. Define contractor. Will a Congressional staffer need a card? What impact will the new card have on cards currently in use? Will Department of Defense personnel have to have these new cards when 4 million employees at DOD have already been issued cards?
Tim Kaufman, Federal Times

Answer: You may want to set up a separate interview, but briefly, cards will be issued beginning August 2005. Standards have specific guidelines for who will be issued cards. Contractors who need to be in a federal building for a long period of time, will be issued cards. Agencies that have card program in place, like DOD have been contacted to determine their experience. Cards are not designed for Executive Branches (Congress members or congressional staffers).
Jeanette I. Thornton

Question: I sell products to military installations internationally. To get on these bases, we have to have IDs. We need a different tag for

each military base. Is it possible that contractors can be issued one card to enter multiple military installations around the world?
Allen Burton, American Logistics Association

Answer: Access control is still the purview of each agency's Director.
Jeanette I. Thornton

Session Two

The afternoon session began promptly at 1:00 p.m. and was attended by approximately 175 people.

Overview of Agenda/Logistics

Jeanette Thornton, Policy Analyst, Office of Management and Budget

Ms. Thornton provided an overview of the agenda for the afternoon session indicating there would be presentations from six invited speakers. Ms. Thornton concluded with an introduction of Glenn Schlarman who provided opening remarks.

Opening Remarks

Glenn Schlarman, Branch Chief, Information Policy and Technology, Office of Management and Budget

Mr. Schlarman provided the opening remarks verbatim from prepared notes.

Mr. Schlarman acknowledged that he was repeating the remarks made by Karen Evans during the morning session. He began by saying that promoting effective and efficient information technology, security and privacy requires a delicate balancing act, then he reiterated the points made earlier by Ms. Evans.

He stated the meeting was being held to get advice on how the government could meet the President's Directive to provide a standardized ID card and protect privacy. He indicated that the Department of Commerce had held two workshops seeking input on the technology involved in the implementation of HSPD-12 but that it was time to discuss policy and privacy. Mr. Schlarman indicated that HSPD-12 established extremely tight deadlines that require the Department of Commerce to issue the standard by February 27th and agencies to complete implementation plans by the end of June and implement use of IDs that meet the standard by October 2005.

Mr. Schlarman indicated that a common standard will eliminate inconsistency and the waste of government resources. He acknowledged that with efficiency comes a need for limits and strict guiding principles. He indicated the key question is how to strike the balance between protecting our federal resources and protecting the privacy and security of those who come to work for the government everyday. He assured the audience that the government wants to build privacy enhancing technologies into the standard ID card and ensure that uses of the card are appropriately controlled. He further stated that the government wants to put in place protective measures to ensure that personal information stored on a card can't be accessed inappropriately. Mr. Schlarman indicated that the expert speakers would address the use of smart cards, those with contact chips and those employing wireless or RFID type technology, the benefits and privacy concerns associated with biometrics (particularly the electronic system of fingerprint capture) and designing a numbering system to protect privacy.

Mr. Schlarman ended by acknowledging the presence of representatives from both large and small federal agencies, including many agency privacy officers.

Privacy Policy Principles

Frannie Wellings, Policy Analyst, Electronic Privacy Information Center (EPIC)

Jeanette Thornton introduced Ms. Wellings as the first presenter for the afternoon session. *Ms. Wellings closely followed her prepared PowerPoint slide presentation ("Privacy Protection and the Common Identification Standard for Federal Employees and Contractors").*

Ms. Wellings explained the significance of privacy protections for the federal employee ID noting that one of the functional objectives is to protect the privacy of the cardholder; that the proposal does not include adequate safeguards to protect the cardholder's privacy; and persistent identification raises additional risks that should be addressed. She stated that Fair Information Practices could be a guideline for protection of employee information. She stated these practices require that employees, contractors and other data subjects must know that a record is being kept, must be able to find out what information is being gathered and retained and how it is used and must be able to correct the information held. The information should be used for only the purpose specified and it must be reliable and secure.

Ms. Wellings stated that the federal ID proposal cries out for a Privacy Impact Assessment that should be performed immediately. The PIA must be proactive, incorporating privacy protections into the decision making process rather than awkwardly and inefficiently adjusting later. Ms. Wellings also asserted that source documents should not be retained.

Ms. Wellings also discussed the need for data minimization, the need to secure backend information, the life cycle of information in databases, mission or function creep, employee redress, biometric facial imaging, and identity theft. She opposes contactless cards because they pose a real security problem.

Ms. Wellings stated that there is strong, historic opposition in the United States to the use of a single identifier. Even though the SSN is widely used, the Privacy Act makes clear that its use should be limited and the trend in many institutions is to move away from a single identifier. She summarized her presentation by stating there needs to be a Privacy Impact Assessment, there is a need to question the scope of this new standard ID system, and in order to really protect the privacy of federal employees who are dedicating themselves to public service, this type of proposal will require legislation enforcing their rights.

(*See Attachment 8, a copy of Frannie Wellings' PowerPoint slide presentation)*

Privacy Policy Principles
John Sabo, Manager, Security Privacy and Trust Initiatives, Computer Associates International

Mr. Sabo was introduced by Jeanette Thornton following the conclusion of Frannie Wellings' comments. *Mr. Sabo closely followed his PowerPoint slide presentation ("Privacy Policy Implementation and HSPD-12").*

Mr. Sabo opened by providing the requirements of the Privacy Act (identify each system of records and publish notice; review content to ensure collection and maintenance are necessary and relevant to law or executive order; inform individuals of the purpose for collection, rights, benefits, obligations; maintain accounting of all disclosures of information; assure records are accurate, relevant, timely, complete; permit individuals access and amendment of records; provide reasonable safeguards regarding disclosures and protections against security and integrity threats).

Mr. Sabo also discussed the Canadian Standards Association's Model Code for the Protection of Personal Information, Privacy Impact Assessments and the Information Security and Privacy Advisory Board (ISPAB) Report, dated September 2002 which he said is still valid today. He also discussed four privacy references in FIPS-201 (protecting the privacy of e cardholder, contactless use of PINs and biometrics is not supported; standards for validated components and validation maintenance).

Mr. Sabo thinks a primary issue is developing companion policy guidance on privacy requirements. He concluded by making six recommendations: address privacy management responsibilities with the same diligence as security; establish a clear set of deliverables coincident with HSPD-12 timeframes; use the standard development process defined by NIST; issue a publication on agency HSPD-12 privacy management; use existing bodies and expertise, including industry and government efforts; and use industry expertise in compliance management).

(*See Attachment 9, a copy of John Sabo's PowerPoint slide presentation)*

Privacy Policy Principles
Steve Holden, Assistant Professor, University of Maryland, Baltimore County

Following Mr. Sabo's comments, Jeanette Thornton introduced Steve Holden. *Mr. Holden closely followed his PowerPoint slide presentation ("Privacy Implications of E-Authentication"), noting only an error in pagination between page 5 and 6.*

Mr. Holden noted that authentication technologies have privacy implications but stated that affecting privacy is not always a violation of privacy. He discussed the Code of Fair Information Practices highlighting the fact that there must be no personal data record-keeping systems whose very existence is secret; there must be a way for a person to find out what information is in a record and how it is used; there must be a way for a person to prevent information obtained for one purpose from being used for other purposes without consent; there must be a way for a person to correct or amend a record of identifiable information; and any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data and take precautions to prevent misuse.

He discussed the National Research Council (NRC) Report that provides a toolkit with a checklist of questions regarding four major design decisions (attribute choice, identifier choice, identity selection, authentication phase). He stated that each design decision must be examined against four types of privacy implications (information privacy, bodily integrity, decisional privacy and communications privacy). He compared the NRC toolkit to the Privacy Impact Assessment and concluded with his recommendations.

Mr. Holden responded to questions from the audience immediately following his presentation.

Question 1: How are the privacy rules different for contractors?

Answer: I don't know if the standard makes a distinction.
Steve Holden

Question 2: There are countless examples of data mining and exploitation. For instance, at OMB an employee got into the system. Who will be responsible for oversight?

Answer: Data held by registration authority raises the prospect that such data will be a target. An addendum is needed so that people can correct incorrect data. There must be ways to minimize impact of people being able to look at data when data is centralized. If data

> is used for purposes other than that for which it was originally collected, that presents a problem.
> *Steve Holden*

(*See Attachment 10, a copy of Steve Holden's PowerPoint slide presentation which notes a change in page numbering.)*

The audience took a fifteen minute break after Mr. Holden's presentation.

Technology and Privacy
Gary E. Clayton, President and CEO, Jefferson Data Strategies

After the break, Jeanette Thornton introduced Gary E. Clayton as the next presenter. *Mr. Clayton followed almost verbatim his prepared comments on a common identification standard.*

Mr. Clayton discussed the Federal Personal Identity Verification (PIV) Standard issued by NIST and the Department of Commerce. He indicated his company had been actively involved in the development of effective management processes and tools to ensure the protection of privacy. He thinks the proposed standard appears to have the flexibility to support a wide variety of services and uses, while still providing a standard look and information set. He stated that significant input and/or specifications for an adequate policy framework to prevent misuse of the cards and the associated data are missing from the standard.

He feels the technology has been designed without adequate involvement and input on privacy and policy and this puts both the privacy and security of cardholders and the systems involved at risk. He noted that the Fair Information Practices provides fundamental principles that should be addressed in the standard especially with regard to mission creep; data retention and standard uses; source documents; identity credential issuance; registration database; limitations in the amount of data obtained; contact versus contactless cards; biometrics; and permanent or persistent employee ID concerns.

He concluded by stating that prior to the issuance of the final standard, it is imperative to issue draft policies for public comment. He feels a common mistake by technologists is to design the technology and then involve policy and privacy as an afterthought then technologies fail to garner public support and/or trust.

(See Attachment 11, a copy of Gary Clayton's prepared comments. No variances were noted between the prepared comments and the oral presentation.)

Technology and Privacy
Dan Bailey, RFID Solutions Architect, RSA Laboratories

Jeanette Thornton introduced Dan Bailey as the next presenter. *There were no variances noted between his comments and his PowerPoint slide presentation ("Contactless Threats to FIPS 201 Systems").*

Mr. Bailey focused on two basic threats to card-based identification systems: cloning and tracking/targeting. He indicated FIPS 201 provides different protections against these threats when applied to the contact or contactless interface. The contact interface gets a public-private keypair and certificate. The contactless interface is prohibited from using these probably because of power and range issues.

He described CHUID, ISO 14443 devices and a local authentication key on the card for a challenge-response protocol. He recommended that the latter become mandatory. Other recommendations was enabling the contactless interface only while the cardholder is pressing a button on the card similar to cards piloted by MasterCard; allowing an authenticated contact reader to switch off the contactless interface with software commands; instructing cardholders to store cards in a foil-lined bag when not in use; replacing the CHUID with a random identifier.

Mr. Bailey fielded questions from the audience immediately following his comments.

Question: You talked about authenticating the card and reader. What additional security is provided by requiring a PIN?

Answer: The way the system works is that the card presents itself to the reader and tells it which key to use to start the challenge-response process. If you have a card-specific key, there must be someway to reveal that key to the reader, thus you reveal information about the card that may be used to track it.
Dan Bailey, RFID Solutions Architect, RSA Laboratories

Follow-up: Then the only way to prevent tracking by an attacker is to carry the card in a lead-lined pouch.

Answer: Yes, but that's impractical.
Dan Bailey

(See Attachment 12, a copy of Dan Bailey's PowerPoint slide presentation. No variances were noted between the prepared comments and the oral presentation.)

Technology and Privacy

Howard Schmidt, Chief Security Strategist, eBay and Former White House Cyber Security Advisor

Jeanette Thornton introduced Howard Schmidt as the final presenter. *There were no variances noted between his comments and his PowerPoint slide presentation ("HSPD-12 Technology and Privacy Panel").*

Mr. Schmidt began his presentation with a provocative statement indicating that "without security there is no privacy; privacy is a goal, security is the means to achieve this." He indicated that the current password behavior leaves end-users vulnerable and that consumes are concerned about security as reflected by their use of anti-virus services. He described common attacks (e-mail spoofing, password trap and phishing) and stated that we need encryption, authentication, and proof of identification.

Mr. Schmidt indicated there are four keys to securing privacy: authentication, data privacy, non-repudiation and authorization. He discussed two-factor authentication and authentication selection criteria based on cost, usability, and strategic fit. He believes there is an opportunity for the government to lead and that a federated consumer authentication is the future. He believes there are several benefits from having a federated identity model including better protection of user privacy, greater choice for users and centralized identity benefits.

(See Attachment 13, a copy of Howard Schmidt's PowerPoint slide presentation. There were no variances noted between the prepared comments and the oral presentation.)

Questions and Answers

No one came forward during the "open microphone" period to ask any questions following the last presentation.

(*See Attachment 14, for a copy of the HSPD12 meeting agenda)*