Subject: Comments on Public Draft FIPS 201
From: "Jennifer A. Kerber" <jkerber@itaa.org>
To: <DraftFips201@nist.gov>
Cc: "Jennifer A. Kerber" <jkerber@itaa.org>

December 22, 2004<?xml:namespace prefix = o ns = "urn:schemas-microsoft-com:office:office" />

Chief

Computer Security Division, Information Technology Laboratory

Attention: Comments on Draft **FIPS 201**

100 Bureau Drive--Stop 8930

National Institute of Standards and Technology

Gaithersburg, MD 20899-8930

Re: Comments on Public Draft FIPS 201

To Whom It May Concern:

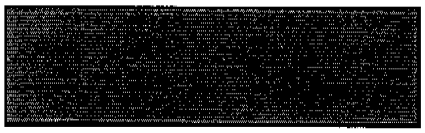
The Information Technology Association of America (ITAA) submits these comments in response to the November 8, 2004 Federal Information Processing Standards Publication 201, *Personal Identity Verification Standards for Federal Employees and Contractors*. As discussed in more detail in the attached document, the ITAA has significant concerns regarding the FIPS 201 draft standard. In particular, ITAA is concerned the FIPS 201 draft does not take into full consideration the significant expertise and work done by both the Government Smart Card Interagency Advisory Board (IAB) and the Federal Identity Credentialing Committee (FICC).

The ITAA's members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. We provide global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. The ITAA consists of over 500 corporate members throughout the U.S., and a global network of 47 countries' IT associations. The ITAA plays a leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. Please visit www.ITAA.org for more

information on the ITAA's activities.

The ITAA appreciates this opportunity to comment on the proposed NIST standards. We look forward to continuing our dialogue with NIST on this and other issues important to Federal identity management.

Respectfully submitted,



Harris N. Miller

President

Information Technology Association of America

Jennifer Kerber
Director
Enterprise Solutions Division
Information Technology Association of America
1401 Wilson Boulevard, Suite 1100
Arlington, VA 22209

(703) 284-5337
(703) 598-4977 (c)
www.itaa.org

 Jennifer Kerber (E-mail)1.vcf

 ITAA Draft NIST PIV Comments FN.doc


ITAA Comments Temp.xls

ITAA Comments on NIST FIPS 201 Draft
Personal Identity Verification (PIV) for Federal Employees and Contractors
December 22, 2004

Executive Summary

ITAA is concerned the NIST FIPS 201 draft does not take into full consideration the significant expertise and work done by both the Government Smart Card Interagency Advisory Board (IAB) and the Federal Identity Credentialing Committee (FICC). The draft creates a new technical standard and architecture for government smart card solutions and replaces the existing Government Smart Card Interoperability Specification (GSC-IS), which was jointly developed over the past five years among industry and government. The draft also fails to recognize the latest technologies in the area of identity proofing currently being used by the public and private sector. ITAA believes that together these actions put at significant risk the effective implementation of HSPD-12.

ITAA strongly requests that NIST reexamine its PIV specifications. Specifically ITAA encourages NIST to:

- Move forward with a standard that relies on the GSC-IS v2.1 as its basis;
- Delay the October 2005 implementation deadline to allow industry and government to expeditiously implement these requirements through the existing framework of the GSC-IS;
- Work with the Office of Management and Budget to coordinate an immediate review of the anticipated plans and costs for implementation of HSPD-12; and
- Incorporate a layered identity authentication and verification process that recognizes new technologies and methods available to ensure the verification and authentication of individuals before the issuance of a secure credential.

Personal Identity Verification (PIV) Standards

The issuance of Homeland Security Presidential Directive 12 (HSPD-12) by President Bush this past August was a watershed event in the Federal government's efforts to improve the security and functionality of government credentialing systems. A strong, standards-based Personal Identity Verification (PIV) system for all of the Federal government and government contractors will result in significant increases in security and convenience for all agencies, and is a step that ITAA believes is long overdue.

To date, good efforts and success toward the goal of a standards-based, interoperable approach to verifying identity across the government have taken place under the guidance of the Office of Management and Budget (OMB), working with the General Services Administration (GSA), the National Institute of Standards and Technology (NIST), and numerous other Federal agencies. Together, these agencies have facilitated both the Government Smart Card Interagency Advisory Board (IAB), which has led the development of a Government Smart Card Interoperability Specification (GSC-IS). They have also supported the Federal Identity Credentialing Committee (FICC), which has generated appropriate policies for identity management and credentialing across the federal government.

ITAA believes that an appropriate approach to implementing HSPD-12 would be one that builds on the work done to date through the IAB and FICC by embracing existing industry standards and practices that have been utilized by numerous Federal agencies to date in support of their smart card deployments and identity management services.

ITAA is concerned with some aspects of the NIST FIPS 201 draft. From reviewing the November 8, 2004 draft standards documents, it appears that NIST's draft has not taken into full consideration the significant expertise and work done by both the IAB and FICC. Part I overlooks the latest technologies in the area of identity proofing currently being used by the government. Part II pursues an implementation strategy that seeks largely to replace the existing GSC-IS, which was jointly developed over the past five years among industry and government, including significant guidance and support from NIST. The GSC-IS is a standard that enjoys significant support across government and industry, and numerous COTS products are available to support it. In its place, NIST has proposed to create a new technical standard and architecture for government smart card solutions that differs from the solution set envisioned in the GSC-IS.

ITAA believes that together these actions put at significant risk the effective implementation of HSPD-12. ITAA strongly requests that NIST reexamine its PIV specifications as outlined below.

Part 1: PIV - I Common Identification and Verification Requirements

The standards proposed in Part I of the PIV do not address all the work government and industry have done validating and authenticating claimed identity before issuing a secure credential. The standards proposed should be part of a layered authentication and

validation system. As written, the standards fail to ensure someone is who they say they are before issuing a secure credential and rely on old methods with inherent weaknesses. Identity fraud and the use of fraudulent identification documents (i.e. driver licenses, passports, etc.) is often used as individuals attempt to assume other identities. Special care needs to be taken to ensure that the individual presenting himself for the credential has not assumed the identity of another individual and or is in possession of a falsified breeder or identification document.

As public and private sector organizations recognize the limitations of traditional identity documentation and the possible consequences of the use of fraudulent identity, new methods of identity authentication have been developed. The FIPS 201 should acknowledge new technologies such as knowledge-based authentication and document verification technology and incorporate them where appropriate into the different levels of security.

NIST's solution to identity proofing require agencies to:

- Check and verify validity with each document's issuer (for "low level" sensitivity positions);
- Require a law enforcement check using fingerprints; and
- Conduct some type of verification of the applicant supplied employment and schooling information – i.e., a level of "background checking" (for all higher levels of sensitivity).

These solutions have several inherent weaknesses when used exclusively. The most obvious weakness is the shear volume of validations required. With over a million new Federal employees being processed each year, the wait time to complete these checks or manpower need to respond to them, will overwhelm an already dysfunctional system. In the absence of these checks being completed, NIST suggests that the employees would be given visitor-type ID passes – an inadequate solution institutionalizing system vulnerabilities.

In addition, background checking (including law enforcement fingerprint checks) alone has a number of inherent limitations in addressing the three key areas in the identity proofing process:

1. Does the identity exist?
   Thorough, on-the-ground background checks can be a reasonably reliable way of confirming the existence of an identity. Investigators can inspect public records on site and conduct in-person interviews of key references.

   One potential weakness with many background check protocols currently in use is an over-reliance on information originally provided by the individual. References are often nominated by the individual, as is other information such as educational background and employment history. Background investigations that rely on applicant-generated data for follow-up interviews are exposed to potential conspiracies.

2. Is the individual actually that identity?
   Background checks must be interactive to prove an identity relationship. Investigators can query references that can vouch for the authenticity of an individual, but that query and response must link the individual to the reference through either in-person recognition or a reliable, recognizable biometric that is resistant to error and fraud. A further complication is the validity of the references themselves – as with breeder documents, there is the risk of an "authentication pyramid." Finally, background checks fail to identify if an identity is being used by more than one individual (for example, was stolen or is part of a fraudulent scheme). Consequently, using background checks to confirm an identity relationship can be costly, time-consuming, and complex, and sometimes incomplete.

3. Does the individual merit the trust of that situation?
   Although criminal checks based on fingerprints, as well as credit history, can be useful to identify past behaviors that would limit the "trust" to be placed in an individual, a person recruited to perpetrate fraud or a terrorist act may have no past history of negative behaviors in these areas. Further, not all criminal histories are recorded at the national level due to limitations in state processes. Additionally, traditional background checks often have an over-reliance on information provided by the individual, as noted above.

ITAA members have been working closely with key government entities to find ways to overcome these limitations. Knowledge based authentication is a form of identity proofing used in the public and private sector. As databases containing personal information continue to grow and network capabilities extend to virtually every government and business office, the disciplined review of an individual's historical data has become a highly effective approach for validating an individual's identity. Document verification technology is another form of verification used in the private sector to validate security features on ID's are in the proper format and that the document has not been tampered with. These types of technologies, when used in conjunction with effective background checking, result in a far higher degree of confidence in the identity proofing and registration process. A multi-layered identity proofing solution utilizing new proven technologies will provide a greater chance of preventing unwanted persons from obtaining legal credentials.

Clearly, ensuring verification and authentication before issuing or relying upon an identification card is critical for the integrity of the overall identity architecture. ITAA encourages NIST to revisit this key area and to incorporate a layered identity authentication and verification process that recognizes new technologies and methods available to ensure someone is who they say they are.

Part II: PIV - II Card Issuance, Management, Authentication and Validation Requirements

While the proposed NIST approach for FIPS 201 and SP 800-73 present an interesting architecture, ITAA has had serious concerns about the adverse effects it could have both on agencies implementing PIV systems, and on the developing identity management industry that will need to build the hardware and software solutions to support this new system. Specifically, ITAA believes that the current NIST PIV draft standard would jeopardize existing government identity management systems by ignoring the infrastructure already developed to implement the GSC-IS. The Association is also concerned about the effects the draft standard will have on industry, which will need to make costly reinvestments in its offerings, and more significantly, that the new approach will cause substantial delays in the implementation timeline envisioned by President Bush for secure PIV systems across government. These delays will ultimately degrade the level of security afforded by existing smart card solutions.

ITAA is encouraged, however, by NIST's recent decisions to move back towards the GSC-IS and seek the active participation of the Government Smart Card Interagency Advisory Board (IAB) in formulating the next drafts of FIPS 201 and SP 800-73. By choosing to leveraging the years of hard work already done under the IAB and embracing GSC-IS as the core of the SP-800-73, NIST has chosen a path that ensures government and industry will not have to reinvent the wheel or engage in major overhauls of existing smart card systems. However, ITAA also recognizes the importance of NIST's work to map the new PIV standards to existing and evolving international standards.

However, ITAA is concerned that the latest NIST draft would relax the October, 2005 requirement to implement all HSPD-12 requirements, with the exception of some very basic claimed identity validation practices. ITAA believes that if the current approach is not abandoned, this staggered implementation of a NIST standard may set in motion a series of events that will actually degrade the security of the identity management systems deployed across government over the next two to three years. Specifically, the current approach could have the following effects:

- Agencies that have already implemented or plan to implement secure identity management systems will delay these efforts in the wake of no firm timeline for PIV-II compliance.
- Agencies that would have been prompted to upgrade their identity management systems by the original October, 2005 deadline anticipated by HSPD-12 will continue to make use of non-secure legacy systems because of the relaxed requirements in the public FIPS 201 draft.

The goal of HSPD-12 is to ensure that all government employees and contractors hold secure identification credentials that positively establish an individual's identity to minimize risks of terrorist attacks from within government and the government contracting community. ITAA believes that the current GSC-IS standard provides a solid foundation on which to implement the requirements of HSPD-12. The GSC-IS has been specifically designed in a collaborative environment among industry and government for

this very purpose; it is an accepted standard today, there are numerous COTS products that support it and are ready for purchase, and there are numerous agencies that have already successfully deployed PIV solutions around the standard. The GSC-IS provides a solid foundation on which to build enhanced identity management programs and presents the only suitable means by which to implement the requirements of HSPD-12 in the timeframe established by the President.

ITAA recommends that NIST moves forward with a standard that relies on the GSC-IS v2.1 as its basis, and which augments it both with work done by the Government Smart Card Interagency Advisory Board (IAB) on issues such as physical access interoperability, data models and topology, as well as with additional items dealing with new requirements such as claimed identity validation.

ITAA believes that President Bush was not ambiguous when he signed HSPD-12. The Directive was clear in stating that there is a vital and immediate need to eliminate the "wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks." The establishment of an October 2005 deadline is a challenge to both industry and government to expeditiously implement these requirements through the existing framework of the GSC-IS.

ITAA recommends that NIST work with the Office of Management and Budget to coordinate an immediate review of the anticipated plans and costs for implementation of HSPD-12. ITAA also strongly encourages OMB to consider developing common solutions for Identity and Access Management through the creation of an Identity and Access Management Line of Business under the Federal Enterprise Architecture; this would involve the development of a cross-agency Identity and Access Management Business Case as part of the Budget process in all budget requests from federal agencies. HSPD-12 is an immense undertaking and resource requirements for federal agencies that do not currently have infrastructure in place should be carefully assessed.

ITAA looks forward to working with the government to leverage the advancements made through the GSC-IS and move forward to enhance existing programs to better protect the homeland. ITAA has formed an identity management committee with senior leaders from the major private sector identity management providers and would be happy to meet with government leaders to articulate industry concerns with the current approach.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex ,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	ITAA	Jennifer Kerber (703) 284-5337	E	FIPS 201	The standards proposed in Part I of the PIV do not address all the work government and industry have done validating and authenticating claimed identity before issuing a secure credential. As written, the standards fail to ensure someone is who they say they are before issuing a secure credential and rely on old methods with inherent weaknesses.	As public and private sector organizations recognize the limitations of traditional identity documentation and the possible consequences of the use of fraudulent identity, new methods of identity authentication have been developed. The FIPS 201 should acknowledge new technologies such as knowledge-based authentication and document verification technology and incorporate them where appropriate into the different levels of security.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex ,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
2	ITAA	Jennifer Kerber (703) 284-5337	T	FIPS 201	NIST's solution to identity proofing require agencies to: verify documents; conduct background check based on fingerprints; verify the applicants school or employment information provided. These solutions have several inherent weaknesses when used exclusively. The most obvious weakness is the shear volume of validations required. With over a million new Federal employees being processed each year, the wait time to complete these checks or manpower need to respond to them, will overwhelm an already dysfunctional system.	ITAA encourages NIST to revisit this key area and to incorporate a layered identity authentication and verification process that recognizes new technologies and methods available to ensure someone is who they say they are. Knowledge based authentication is a form of identity proofing used in the public and private sector. As databases containing personal information continue to grow and network capabilities extend to virtually every government and business office, the disciplined review of an individual's historical data has become a highly effective approach for validating an individual's identity. Document verification technology is another form of verification used in the private sector to validate security features on ID's are in the proper format and that the document has not been tampered with. These types of technologies, when used in conjunction with effective background checking, result in a far higher degree of confidence in the identity proofing and registration process.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex ,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
3	ITAA	Jennifer Kerber (703) 284-5337	T	FIPS 201	ITAA has had serious concerns about the adverse effects it could have both on agencies implementing PIV systems, and on the developing identity management industry that will need to build the hardware and software solutions to support this new system. Specifically, ITAA believes that the current NIST PIV draft standard would jeopardize existing government identity management systems by ignoring the infrastructure already developed to implement the GSC-IS.	ITAA recommends that NIST moves forward with a standard that relies on the GSC-IS v2.1 as its basis, and which augments it both with work done by the Government Smart Card Interagency Advisory Board (IAB) on issues such as physical access interoperability, data models and topology, as well as with additional items dealing with new requirements such as claimed identity validation. By choosing to leveraging the years of hard work already done under the IAB and embracing GSC-IS as the core of the SP-800-73, NIST will choose a path that ensures government and industry will not have to reinvent the wheel or engage in major overhauls of existing smart card systems.
4	ITAA	Jennifer Kerber (703) 284-5337	E	FIPS 201	The Association is also concerned about the effects the draft standard will have on industry, which will need to make costly reinvestments in its offerings, and more significantly, that the new approach will cause substantial delays in the implementation timeline envisioned by President Bush for secure PIV systems across government. These delays will ultimately degrade the level of security afforded by existing smart card solutions.	Delay the October 2005 deadline. The establishment of an October 2005 deadline is a challenge to both industry and government to expeditiously implement these requirements through the existing framework of the GSC-IS.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex ,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
5	ITAA	Jennifer Kerber (703) 284-5337	T	FIPS 201	ITAA is concerned that the latest NIST draft would relax the October, 2005 requirement to implement all HSPD-12 requirements, with the exception of some very basic claimed identity validation practices. ITAA believes that if the current approach is not abandoned, this staggered implementation of a NIST standard may set in motion a series of events that will actually degrade the security of the identity management systems deployed across government over the next two to three years. Specifically, the current approach could have the following effects: Agencies that have already implemented or plan to implement secure identity management systems will delay these efforts in the wake of no firm timeline for PIV-II compliance. Agencies that would have been prompted to upgrade their identity management systems by the original October, 2005 deadline anticipated by HSPD-12 will continue to make use of non-secure legacy systems because of the relaxed requirements in the public FIPS 201 draft.	Delay the October 2005 deadline. The establishment of an October 2005 deadline is a challenge to both industry and government to expeditiously implement these requirements through the existing framework of the GSC-IS.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex ,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
6	ITAA	Jennifer Kerber (703) 284-5337	E	FIPS 201	HSPD-12 is an immense undertaking and the additional costs on federal agencies that do not currently have infrastructure in place should be carefully assessed.	ITAA recommends that the Office of Management and Budget coordinate an immediate review of the anticipated costs for implementation of HSPD-12. ITAA also strongly encourages OMB to consider developing common solutions for Identity and Access Management through the creation of an Identity and Access Management Line of Business under the Federal Enterprise Architecture; this would involve the development of a cross-agency Identity and Access Management Business Case as part of the Budget process in all budget requests from federal agencies, including for current FY2006 planning and budgeting.