To: DraftFIPS201@nist.gov
From: Ari Schwartz <ari@cdt.org>
Subject: Policy Comments on FIPS 201

CDT's comments on FIPS 201 are attached. Please feel free to contact me with any questions.

Thank you,

Ari


CDT_PIV_comments.doc

DraftFIPS201@nist.gov

December 22, 2004

Comments on Public Draft FIPS Publication 201, *Federal Personal Identity Verification (PIV) for Federal Employees and Contractors*

Summary

CDT appreciates the need for a single standard for identity cards for federal employees and contractors. The haphazard way in which identification standards and systems were developing would have made it difficult to achieve the goals of efficiency and of securing the cards and the personal information associated with them. In particular, we are pleased that the PIV standard devised by NIST generally seems to have the flexibility to support a diversity of services and uses, but still provide a standard look and information set.

However, **CDT is concerned that the technical standards for the PIV are moving forward without an adequate policy framework** to prevent misuse of the cards and associated data. The failure to adopt policies before technologies are designed and procured puts at risk both the privacy and security of card-holders and the systems involved.

CDT believes that development of basic policies to **limit misuse and overuse of the cards and the information on the cards** should be a top priority for NIST and OMB in setting standards and then implementing it.

In this regard, we are encouraged to hear that OMB is planning a public meeting to discuss policy issues surrounding development and use of ID cards. An additional step in developing a sound policy framework should be the performance of a Privacy Impact Assessment, a very useful mechanism for surfacing and addressing privacy issues.

Background

HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," calls upon the Secretary of Commerce to "promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification."

The Directive notes possible privacy and security concerns with greater use of a standardized card. Therefore, the functional objectives of the card identified by NIST rightly include "protect(ing) the privacy of card holders" and "provid(ing) appropriate security to the entire identity proofing and authentication process." These concerns are broadened by the fact that a standard that will affect the federal government and many of its contractors is likely to have a major impact

on the private sector, including industries dealing with physical security and access control, the ID and smart card industry, and the computer industry as a whole

As NIST correctly pointed out in Special Publication 800-27, "Computer Security: Principles for Information Technology Security (A Baseline for Achieving Security):" "securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology and operational aspects of information technology."

Sound technology design principles dictate that policy – the business plan — be established first. We recognize that NIST cannot develop PIV policies on its own. A better approach is for NIST and OMB to work in tandem, combining their efforts rather than bifurcating them, with OMB taking the lead in developing PIV policies before the technical standards are finalized.

Lack of a Policy Framework

NIST's Public Draft FIPS Publication 201 makes the common mistake of decoupling technology from policy. It clearly addresses the specifically technological protections for privacy and security in [the] PIV, but defers to the agencies and OMB the development of protections at the level of people and operations.

In this regard, the Draft FIPS creates a risk that technological decisions will be made that are incompatible with policy and vice versa. At the very least, the FIPS opens the door to agencies pursuing inconsistent policies for PIV, which could undermine the goals of HSPD-12. The lack of guidance on people and processes could lead agencies to infer that privacy and security policies are adequate as is.

Security Levels

CDT is concerned that there seem to be no limitations or security levels specified for uses of the [PIV] card. This could have a major impact on both privacy and security. As agencies use the card, there may be a tendency to require the strongest level of authentication for all transactions. However, sound policy would dictate that authentication requirements be set depending on the sensitivity of the transaction and that the authentication required for any class of transactions should be no stronger than is necessary for the specific purpose.

Overuse of stronger authentication credentials or identity information creates greater privacy risks by linking more personal information to more transactions than is needed. This will serve to weaken the effectiveness of the PIV system. A major component of the policies for the card should be that specific programs or transactions get the only the information they need at the time that they need it

for the level of sensitivity involved.

Mission Creep

CDT is also concerned that a lack of limitations on use of the card will lead to the card being used in unintended ways that could compromise both the security and privacy of cardholders.

CDT recommends that a process be put in place to approve:

- Limitations for card issuers to share enrollment and other backend information with non-federal entities — Non-Privacy Act entities (ie, entities other than Section M contractors) should not be able to gain access to information about card holders that could compromise the security of the system. While this may seem like common sense, there are currently no protections to stop an agency from doing this under wither HSPD-12 or in the standard.
- Access to specified identification and authentication information, including biometric information — Clear procedures tied to level setting should be created for all agencies to follow to help limit misuse.
- New uses for the card — In order to ensure that levels can be set and clear procedure can be created, agencies need to be given a clear set of approved uses after they have explored potential uses as directed in HSPD-12 and these uses have been reviewed. Of course agencies should be able to develop new uses for the card, but, because of the delicate nature of the security and privacy issues, these uses should be reviewed for their potential impact on the system as a whole and not just within an individual agency.
- Sharing of transactional information between agencies — For the first time, agencies are going to be able to easily share transactional information among themselves. These uses clearly have to be in accordance with the Privacy Act, but even if it meets a strict legal standard a specific type of sharing may accidentally open the card to abuse.

Biometrics

Finally, CDT would like to address the issue of biometrics. CDT has been supportive of the idea of greater use of biometric technology when privacy issues have been addressed in the design of the project.[1] CDT is concerned about a

[1] See Paul Rosensweig, Alan Kochems, and Ari Schwartz "Biometric Technologies: Security, Legal, and Policy Implications," Heritage Foundation, June 21, 2004. Available at http://www.cdt.org/security/20040421biometric.pdf

one issues raised in the PIV draft standard in particular.

Storing the image of the fingerprint on the card itself — as suggested in the PIV draft standard — has a very specific benefit, in that the information never has to be updated to replace a template. However, any major breach of security not only would put the PIV system at risk, but would put any further use of fingerprint technology. While the risk of a breech is slim, the consequences are simply too high to risk the privacy and security of the federal workforce and beyond.

Conclusion

While there have been unusual efforts to consult with industry on the PIV technology, including two public forums, there has been little or no effort to consult publicly on policies and procedures. The planned public meeting is a good first step, but the process should also include issuance of draft policies for comment.

Too often, public policy lags behind technology, and the technology does not garner trust, because the technological standards are put into place before the policy issues are resolved. NIST and OMB can avoid that common mistake.

CDT would be happy to help work on the public forum on this issue and to address any further questions.

Respectfully submitted,

Ari Schwartz
Associate Director

Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
(202) 637-9800
http://www.cdt.org