Public Comments "NIST Special Publication 800-73"
Interfaces for Personal Identity Verification

Submitted by the

Electronic Privacy Information Center (EPIC)
Washington, DC

February 14, 2005

These comments are submitted on the revised Special Publication 800-73, on behalf of the Electronic Privacy Information Center. The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging civil liberties issues as they related to information technology and to protect privacy, the First Amendment, and constitutional values. EPIC is a recognized expert in matters related to privacy and has testified before numerous federal agencies on matters ranging from identification systems to consumer financial privacy. EPIC has a long-standing interest in the impact of technical standards developed by the federal government on the privacy rights of Americans.

We note at the outset that Homeland Security Presidential Directive/HSPD-12 ("Policy for a Common Identification Standard for Federal Employees and Contractors") which established the legal authority for the NIST to undertake this work on Personal Identity Verification said explicitly:

> This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5. U.S.C. 552a) and other statutes protecting the rights of Americans.

However, there is nothing in the revised NIST Publication to suggest that the agency even considered the privacy implications of the standard proposed. In fact, a text search of the entire 48-page document for the string "privacy" produces only one hit and that is for the generic description of the Information Technology Lab that appears before any of the substantive proposals.

In light of this fundamental failure to address a critical requirement set out in the Presidential Directive, we strongly urge the NIST to withdraw the proposal and to develop a new standard that at least considers privacy issues as required by the Directive. We offer these further comments as baseline considerations or a revised standard for a Common Identification Standard.

The proposal to use a cardholder unique identity data object should not mean in anyway the use of the employee's Social Security Number (SSN). In 4.2 Cardholder Unique Identifier references [8] as providing the format for the Federal Agency Smart

Credential Number. This number should not contain in part or in whole the employee's or contractor's SSN. The use of the SSN by federal agencies is clearly regulated under Section 7 of the Privacy Act. Moreover, the widespread use of the SSN by both the government and the private sector has contributed to the growing problem of identity theft. The inclusion of the SSN as the unique identifier for federal employees also creates the very real risk that it will become easier for those who seek to do harm to impersonate a federal employee or contractor.

EPIC urges caution regarding this proposal

A universal federal ID platform would not prevent false positives and false negatives. An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals may target low-level employees who would present easier targets for gaining access to federal identification documents that could provide the underlying protocols that are the basis for the overall system of federal employee identification.

A universal federal employee ID would require a massive bureaucracy that may compromise the privacy of federal employees. If these systems use biometric systems that are augmented by RFID technology the location of federal employees on and away from the workplace may be open for monitoring.[1] RFID reader technology will only improve with time, and encryption that may be applied may communicate to others the importance of the person in possession of the identification. Further, recently questions regarding the security of RFID technology have been disclosed by a Johns Hopkins research paper.[2]

Any universally deployed federal employee ID system should not depend on both the issuance of an ID card and the integration of huge amounts of personal information included in state and federal government databases. One employee mistake, an underlying database error rate, or common fraud could take away an individual employee's ability to move freely from place to place or even make them unemployable until the government fixed their "file." Anyone who has attempted to fix errors in their credit report can imagine the difficulty of causing an over-extended government agency to correct a mistake that precludes a person from getting employment or gaining access to their job if they are employed.

A one ID fits all federal employment would accrue more expense to some federal agencies than others which would also be required to direct resources away from other more effective counterterrorism measures. The costs of a universal federal employment ID system should be accessed and compared with other methods of ensuring security.

A universal federal employment ID would both contribute to identity fraud and make it more difficult to remedy. A universal national ID would be "one stop shopping"

---

[1] "Letter to Don Hagland, Brittan Board of Trustees," available at http://www.epic.org/privacy/rfid/brittan-letter.pdf

[2] "Analysis of the Texas Instruments DST RFID" available at http://rfidanalysis.org/

for perpetrators of identity theft who usually use SSN and birth certificates for false IDs (not identification documents). Even with a biometric identifier, such as a fingerprint, on each and every ID, there is no guarantee that individuals won't be identified - or misidentified - in error. The accuracy of biometric technology varies depending on the type and implementation. And, it would be even more difficult to remedy identity fraud when a thief has a federal employment ID card with your name on it, but his biometric identifier.

If the standard for the platform that will be used to read and write to the federal identification system has known vulnerabilities it would be advisable to avoid that platform to decrease the likelihood of failures and interruptions to the system.

Additional card applications for interoperability with other systems outside of the process of identifying employees should be avoided, i.e. monitoring employees use of restrooms or trips to break areas should not be done. The ability to convey interoperability to any proposed federal employment identification card as described in section 3.2.2 if related to uses other than employee identification should be avoided. Such a scheme would open the door to vulnerabilities to the overall scheme of checks that are required for the effort to improve security and the privacy of federal employees.

Security Architecture as described by section 3.3 should also include the consideration of federal employee privacy.

Beware of Mission Creep

A universal federal employment ID card could become a de facto internal passport, further compromising the federal employment ID and the privacy of federal workers. Once local and state government databases are integrated with federal employment ID card, the uses of sensitive personal information would inevitably expand. Law enforcement, tax collectors, and other government agencies would want access to the data. Employers, landlords, insurers, credit agencies, mortgage brokers, direct mailers, private investigators, civil litigants, and a long list of other private parties would also begin using the ID and even the database, further eroding the privacy that Americans rightly expect in their personal lives. It would take us even further toward a surveillance society that would significantly diminish the freedom and privacy of law-abiding people in the United States. A federal employment ID would foster new forms of discrimination and harassment.

Avoid building an identification system based on false assumptions

- The identification will only be used to gain entrance to employment and sensitive areas.

- The identification will not be used for non-government employment related purposes.

- The possession of the identification will not convey any level of assumed trust.

- The identification will only be one component of authentication of federal government employees.

Conclusion

Security needs clearly vary across the federal government. Gaining entrance to a highly sensitive Department of Energy facility does not pose the same risk as gaining entrance to the Smithsonian Museum. However, if the two sites use the same security scheme, there will be serious problems. As security experts have said, "if we have the same security standards for toothbrushes as we do for diamonds, we will lose many fewer toothbrushes, but many more diamonds."

Although the process outlined in draft Special Publication 800-73 clearly states that the Personal Identity Verification integrated circuit card will have two components: the high-level PIV client application program interface (API) and the low-level PIV card command interface (card edge), the report states that the "information processing concepts and data constructs on both interfaces are identical." Consider that the level of caution applied to the handling of the identification is diminished by the skills and sensitivity associated with the job and the identification holder. A grounds keeper at a Federal Park may not have the same level of diligence regarding their identification documents as a NASA aerospace engineer. Questions should be asked prior to deployment regarding the risk to highly sensitive government activities if the same identification system is universally deployed throughout the federal government. Further, what will deter state and local governments from adoption of this new federal identification system for their employees?

These are just a few of the questions that the NIST needs to consider before it goes forward with the proposal for a Personal Identity Verification Card. Among the others questions that almost must be considered are these.

- How will the privacy of holders be ensured?

- How will commercial and other governments (state and local) use this new identification for their own purposes?

- Will the identification be subjected to the best efforts of government resources that specialize in finding weaknesses in identification systems?

- How will lost or stolen identification documents be reported?

- Will the system be secure against "Trojan horse" attacks that use the identification card itself as a means of gaining access to the system?

- Will the information be secured against third party access to the data contained on the card?

- If each command on the card command interface is implemented by the card application that is resident in the integrated circuit card does this compromise privacy and security of the card and cardholder?

- What are vulnerabilities in the ability to reset identification cards or their authentication systems to their default state?

- Is it possible to spoof the access mode and security conditions as described by section 3.3.1 Access Control Rule?

Extensive materials on these topics may be found at the EPIC web site. http://www.epic.org.

Sincerely yours,

Marc Rotenberg
EPIC Executive Director

Lillie Coney
EPIC Associate Director

Melissa Ngo
EPIC Staff Counsel