X-Sieve: CMU Sieve 2.2
Date: Thu, 23 Dec 2004 10:08:05 -0800
Subject: Comment on Public Draft FIPS 201 - EFF
From: Pam Dixon <pdixon@worldprivacyforum.org>
To: draftfips201@nist.gov
X-Mailer: Apple Mail (2.553)
X-MailScanner:
X-MailScanner-From: pdixon@worldprivacyforum.org

Dear Sir or Ms.:

The Electronic Frontier Foundation, the World Privacy Forum, PrivacyActivism, and the Privacy Rights Clearinghouse respectfully submit our joint comments regarding Public Draft FIPS 201. Our comments are in the attached Microsoft Word file, <fips201comments12cd23.doc>. We have also attached a PDF of the Word file, <pdffips201comments12cd23.pdf>.

If there are any problems or questions, please contact Pam Dixon at (760) 436-2489.

Kind regards,

Pam Dixon

 fips201comments12cd23.doc

 pdffips201comments12cd23.pdf

---

Pam Dixon
Executive Director
World Privacy Forum
Phone: 760-436-2489
2033 San Elijo Avenue #402
Cardiff by the Sea, CA 92007
www.worldprivacyforum.org

Comments on FIPS PUB 201: Personal Identity Verification (PIV) for Federal Employees and Contractors Public Draft

General Comments about FIPS PUB 201

The Electronic Frontier Foundation, World Privacy Forum, Privacy Activism, and Privacy Rights Clearinghouse respectfully submit these comments on the Personal Information Verification System Standard. We generally oppose PIVSS, as explained below.

Our major concern is that the PIVSS will establish the infrastructure for a full-fledged national ID system, linking and integrating the various ID cards and systems now being created by the federal government. As the background document http://csrc.nist.gov/piv-project/Papers/Background-Version3.pdf shows, the Defense Department Common Access Card has been issued to 4.4 million people, the Transportation Security Administration Transportation Workers Identification Credential will be issued to 12-15 million people, and the "Contactless Chip" U.S. Passport will be issued to all American passport holders.

The PIVSS card will not only add to these numbers, but also provide an interoperability platform that can link these disparate systems. Absent any controls on "mission creep," it is almost inevitable that the PIVSS card (or an architecturally compatible card system) will be used for state and local employees and their contractors, and eventually spread to state identification cards such as driver's licenses. Of course, the current plans for the PIV in itself is ambitious. One of the NIST project briefing presentations about the system states that it will include even "long term frequent visitors (e.g. press corps members)," which raises significant First Amendment press freedom issues. (See "Personal Identity Verification For Federal Employees and Contractors, http://csrc.nist.gov/piv-project/PIV-BriefingSept16-2004-1.pdf).

We will not repeat here the many objections to a national ID system, which are well known. See, e.g., the National I.D. Coalition letter of October 19, 2004 http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=17146&c=206 . We do note, however, that most of the privacy and civil liberties issues associated with national ID systems are magnified by the use of biometrics and RFID or "contactless" smart card technology. Biometrics remains an evolving technology; many biometrics have not been tested over a ten-year-plus period; many have no proven track record for use in large-scale databases; all pose major privacy issues.

RFID – more generally, any "contactless" technology – poses the risk of unwanted and unnecessary exposure of information during transmission. As NIST well knows, cards using the ISO 14443 Type B contactless interface can be read by interlopers at a considerable distance.

> "Using a reader equipped with an antenna, NIST testers were able to lift "an exact copy of digitally signed private data" from a contactless e-passport chip 30 feet away," said Neville Pattinson, director of business development technology and government affairs for smart-card provider Axalto Americas.

(See Junko Yoshida, EE Times, "Tests reveal e-passport security flaw -- U.S. unfazed at copying of unencrypted data" Aug. 30, 2004, http://www.eet.com/sys/news/showArticle.jhtml?articleID=45400010.)

Procedural issues:

We are disappointed by the lack of publicity and outreach to the privacy community on PIVSS. The undersigned organizations did not learn of this project until a few days ago. For this reason, our comments today are far less substantive than they might have been. From what we can tell, no representatives from privacy organizations, not even the ACLU, presented at any of the PIV workshops this fall. Given the implications of a national ID system for privacy and civil liberties – a controversial issue since 9/11 – we believe it is important for the government to consider privacy and civil liberties issues at the beginning of this process.

We also believe that any meaningful public comment on PIVSS must include, at a minimum, some estimate of the cost of the system. We have been unable to find any cost estimate for implementation of PIV cards. Before the government spends any more taxpayer dollars on this initiative, the public should be told how much it is likely to cost.

Privacy policy issues:

Because of the grave implications of a national ID system, biometrics, and RFID technology for privacy and civil liberties, it is imperative that there be a robust and thoughtful privacy policy for the PIV card if the government continues with this project. We cannot ascertain, however, whether FIPS 201 contemplates a systemwide privacy policy, even though Homeland Security Presidential Directive 12 (HSPD-12) specifically directs compliance "with the Constitution and applicable laws, including the Privacy Act . . . and other statutes protecting the rights of Americans." For example, Section 3.2 of the FIPS ("PIV Responsibilities"), which outlines PIV system roles and responsibilities, does not mention privacy or assign any particular agency the task of creating a privacy policy. Privacy guidance must be given to the government entities and private contractors that collect, store or process personal information for the system.

The process for developing such a policy must take place alongside any technical development, and should begin with a Privacy Impact Assessment (PIA) that complies with the Federal Information Security Management Act of 2002 (FISMA). Under FISMA, agencies must conduct PIAs before procuring information technology that collects, maintains, or disseminates identifiable information or for any new information

collection that uses information and that includes information in an identifiable form that could permit physical or online contact with a specific individual.

We also urge that the government make the PIA public as soon as possible as part of the record for the generation of a privacy policy. We expect that the government will follow the spirit and the letter of the Privacy Act, as specified in HSPD-12, and issue appropriate Privacy Act notices, including system of records notices, for all PIV implementations. Additional issues include the need for strong audit trails, access controls, and appeal procedures for individuals who are denied a card.

We also recognize that the standard legal framework for the Privacy Act contemplates that individual agencies comply with the Privacy Act. Where the system crosses agency lines in a regular and systematic way, as it does here, we believe that the government should comply with the Privacy Act on an interagency, integrated, systemwide basis.

Specific Comments about FIPS PUB 201

Comments on Section 1.2: Scope

A. Categories of Card Recipients

The scope of the standard as stated in Section 1.1 is overbroad, and needs to be specified in greater detail. According to this section, current categories of card recipients are "Federal employees and contractors (including contractor employees) for gaining access to Federally-controlled facilities and logical access to Federally-controlled information systems" (p. 1).

This categorization as stated does not adequately or precisely define the issue of non-employees/contractors who need long-term physical access to government systems or facilities. Press pool members, for example, have access to the White House. Will this category of individual, which does not fall into that of a government contractor or employee, be required to obtain a level one PIV? There are many other examples of individuals who may be required to obtain a PIV card, such as other types of long-term visitors who may not fall under the contractor or Federal employee umbrella.

All categories of PIV recipients need to be delineated in detail prior to the implementation of the PIV system. Otherwise, varying interpretations of the implementation will arise as a matter of course given the scale of the system.

B. Graduated position sensitivity levels

The FIPS states that position sensitivity levels are to be determined by departments and agencies. The absence of a systemwide policy on position sensitivity levels not only creates security issues, but also gives card issuers enormous discretion to conduct privacy-invasive background checks in an arbitrary and discriminatory fashion.

Comments on Section 2.2.1: Identity Proofing and Registration of New Employees and Contractors

A. I-9 Form Information Collection, Copying, and Storage

According to Table 2-1 of the Public Draft, level one applicants will be required to turn in Form I-9. The I-9 forms contain a Privacy Act notice: "The authority for collecting this information is the Immigration Reform and Control Act of 1986, Pub. L. 99-603 (8 USC 1324a) (Form I-9, p.1). This notice does not currently indicate that the information is being collected for use in any identification card application, or that such use is a routine use under the Privacy Act.

Moreover, the forms do not indicate to prospective employees how long the information will be kept, what system of records the data enters, where or how many copies are to be kept, and does not reference a privacy policy. All of this information should be provided in written form clearly and unambiguously to the applicant prior to the point at which the applicant's personally identifiable information is collected or stored.

B. Standard Form 85 and 85P Routine Uses

According to Table 2-1 of the Public Draft, level two through four PVI applicants will be required to turn in Standard Form 85 or 85P.

The Standard Form 85 and 85P both contain a Privacy Act notice of routine uses that is fairly detailed. However, Section 2.2.1 of the public draft does not discuss any routine uses under the Privacy Act notice on Standard Form 85 or 85P. The public draft needs to be amended to include details about which routine use this new system of records will use, and how this routine use may be implemented.

Additionally, the forms do not indicate to prospective employees how long the information will be kept, what system of records the data enters, where or how many copies are to be kept, and does not reference a privacy policy. All of this information should be provided in written form clearly and unambiguously to the applicant prior to the point at which the applicant's personally identifiable information is collected or stored.

C. Inclusion of Source Document Copies with Application

This section states that an applicant "provides two forms of identification from the list of acceptable documents included in the Form 1-9." The section also states that these documents are photocopied and forwarded by the sponsoring organization with an application and a request for a PIV card to its management. These documents could include copies of birth certificates, SSN cards, drivers' licenses, and other documents containing personally identifiable information. This data is highly sensitive, and prior to acquiring such documents, a system of records, a privacy policy, and detailed access and

privacy policies must be in place.

Additionally, when an individual terminates employment with the Federal Government or contractor and the PIV card is revoked, the copies of the source documents should be destroyed. If these documents are to be retained indefinitely, applicants should be informed of this prior to the information collection in a detailed privacy policy. While it may be reasonable to retain PKI certificates, it is not reasonable to retain copies of the source documents indefinitely.

D. Background Checks

As discussed in Table 2-2, some form of background check will be conducted for all PIV applicants. The Table information indicates that while levels 1 and 2 are subject to fingerprint checks and NACI checks, level three applicants are subject to a credit check, and level four applicants are subject either to a limited background check or a background investigation.

While it is clear that background checks will be conducted, there is a lack of clarity on precisely which candidates will get what type of background check. And while Annex D of the Public Draft indicates how deep the background checks will go, it does not discuss the full procedures for conducting the tests.

For example, how is the Fair Credit Reporting Act implemented in this environment? What are the specific procedures for the *implementation* of the background checks portion of the PIV system? Is there a standard already in place for Federal and contract employees? If so, it should be added in detail to this framework, as background checks are an integral part of the validation process.

Furthermore, as noted above, there is no obvious systemwide policy on either position sensitivity levels or background checks. Absent such a policy, an agency or department may abuse its discretion by conducting unnecessarily intrusive background checks of disfavored individuals, which is especially dangerous to civil liberties if applied to members of the press. Accordingly, there should be a systemwide policy, consistent with constitutional procedural due process requirements, for background checks.

E. Registration Authority Security and Access Control

In the current PIV scheme, the Registration Authority shall be responsible to maintain an extraordinary amount of highly sensitive data, much of which is apparently in paper format, at least originally. For example, Section 2.2.1 lists that the Registration Authority will keep copies of the identity source documents, a completed and signed background form from the Applicant, results of the required background check, and any other materials used to prove the identity of the Applicant.

Unfortunately, missing from this section of the public draft are the specific and detailed procedures the Registration Authority will use to store, handle, report on, correct, and delete these highly sensitive materials.

We strongly recommend that due to the highly sensitive nature of the documents entrusted to the Registration Authority, that a specific, detailed plan to implement fair information practices is included in this section.

The PIV system must be constructed in a way that protects individuals' privacy and data security. Knowing that much of the threat to this information will come from individuals with internal access to the data, much more detail and attention must be given to fleshing out this area of implementation.

Comments on Section 2.3: Identity Credential Issuance

The Issuing Authority will be responsible to maintain four items: the completed and formally authorized PIV Request, the name of the PIV identity credential holder, the expiration date of the identity credential, and the credential identifier such as an "identity credential serial number" (Public Draft, 8).

No discussion of controlling and limiting the use of the "credential identifier" is made in the public draft. This is a substantial omission, and should be corrected. If the history of the Social Security Number is any indication, this "credential identifier" may be appropriated and used in ways the originators of the system did not envision.

A thorough discussion of appropriate and allowable uses of the "credential identifier" need to be set down as part of the official framework. Disallowed uses of the "credential identifier" also need to be discussed and set down prior to implementation, in a public document.

Comments on Section 3.2.1: Agency Responsibilities

There is a significant omission in this section delineating agency responsibilities. In addition to the responsibilities listed in the Public Draft, agency responsibilities should also include the task of implementing the Privacy Act of 1974 in full in regards to the entire PIV process and framework.

Comments on Section 3.3.2

This section states that all information collected from the applicant, including biometric data, is stored in the Registration Repository. A detailed description of the Registration Repository needs to be given, along with information about what system of records the Registration Repository falls under, and the nature of the security controls that will be used to protect applicants' information.

Comments on Section 4.2: Cardholder Unique Identifier

The Federal Agency Smart Credential Number (FASC-N) that uniquely identifies each card is, according to the Public Draft, available through a contactless interface without card activation. For this reason, it is critical that the FASC-N is limited in when it may be collected, how the identifier may be used, and in what circumstances. Cardholders should be told when and where their cards may be read, and by whom.

It is also unclear whether the CHUID and the biometric data stored on the PIV card are secure against unauthorized access. Section 4.1.5.2 ("File Structure") states that "the CHUID and biometric information shall be stored as transparent files . . . to facilitate rapid retrieval for physical access control applications." If these two data elements are not encrypted, as this statement suggests, obvious privacy issues regarding unauthorized capture are presented.

Comments on Section 4.2.2: Asymmetric Signature Field in CHUID

A. Inappropriate Key Size

The key size requirements for the PIV are unacceptably low. An RSA 1024 bit encryption is not appropriate for information as sensitive as is contained on the PIV card, and such a low encryption level is not appropriate for card use in sensitive areas of employment. The ability to break 1024 bit encryption is well-documented and does not need to be rehashed here; however, waiting until the year 2010 to install 2048 encryption is unrealistically late. The standard set for the PIV card is too low to be secure.

B. Primes Testing

This section mentions X.509 certificates will be issued for the cards, however it did not mention primes testing of the certificates. At some point prior to implementation, primes testing needs to be completed for the PIV cards. This testing is essential. While the testing could conceivably take up to 6 months, depending on the number of certificates issued, it would be negligent to leave primes testing incomplete.

Comments on Section 5.1.1: Registration Database

The standard for the registration database discussed in the Public Draft does not specifically delineate the process by which individual access to the Registration Database will be controlled. Because of the highly sensitive nature of the information, and the importance of the Registration Database, this process needs to be spelled out in detail, and should be symmetrical or very nearly symmetrical across government agencies.

Comments on Section 5.1.2: PKI Repository, Certificate Management, and Associated Privacy Issues

It is assumed from this section of the Public Draft that once generated, a card will be revoked but not deleted due to the necessity of keeping a Master Certificate Revocation list.

However, no mention is made of this in the Public Draft. We strongly suggest that any stored revoked certificate is encrypted at a minimum of 2048 bit RSA, and preferably higher. A 1024 bit encryption level for revoked certificates in storage is not nearly robust enough to protect the information the revoked certificates would likely contain.

Additionally, a privacy notice should be provided to applicants prior to their initial hand-over of the PVI application documents that explains how their information will be handled long-term in the PKI certificate management environment.

Comments on Section 5.2.1

See comments for Section 2.2.1.

Conclusion

Media reports indicate that the current FIPS 201 will be significantly revised. We hope that NIST will obtain input from and increase the participation of privacy groups during the revision process.

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation

Pam Dixon
Executive Director
World Privacy Forum

Deborah Pierce
Executive Director
Privacy Activism

Beth Givens
Executive Director
Privacy Rights Clearinghouse