X-Sieve: CMU Sieve 2.2
Subject: Comments on Public Draft FIPS 201
Date: Thu, 23 Dec 2004 13:45:03 -0600
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Comments on Public Draft FIPS 201
Thread-Index: AcTpKlaOD1iallGiS2CqNrkvJotapw==
Priority: Urgent
Importance: high
From: "Mark Becker" <mbecker@jdstrategies.com>
To: <DraftFips201@nist.gov>
Cc: <william.burr@nist.gov>, <william.polk@nist.gov>, <donna.dodson@nist.gov>,
"Gary Clayton" <gclayton@jdstrategies.com>,
"Roanne Shaddox" <rshaddox@jdstrategies.com>
X-MailScanner:
X-MailScanner-SpamScore: s
X-MailScanner-From: mbecker@jdstrategies.com

On behalf of Jefferson Data Strategies,LLC, attached are comments on Public Draft FIPS 201. We look forward to working with NIST as it finalizes its PIV standard. Please do not hesitate to contact us with any questions or concerns. Happy holidays.

Best regards,

Mark

Mark Becker
Director
Jefferson Data Strategies, LLC
1401 K Street
Washington, DC 20005
Phone: 202-626-8550, ext.596
Mobile: 301-332-9728
www.jdstrategies.com
www.jeffersonconsulting.com

 Mark Becker.vcf

 Jefferson Data Strategies - FIPS 201 12.04 Comments.doc

JEFFERSON Data Strategies, LLC

December 23, 2004

COMMENTS ON PUBLIC DRAFT FIPS 201
Re: National Institute of Standards and Technology
Personal Identity Verification (PIV) Draft Standards

Introduction

Jefferson Data Strategies ("JDS") (formerly known as Privacy Council)[1], in response to the draft FIPS PUB 201, the Federal Personal Identity Verification (PIV) Standard ("PIV Standard") issued by National Institute of Standards and Technology ("NIST") and the Department of Commerce, respectfully submits comments concerning the role of privacy in the creation of a PIV Standard.

On August 27, 2004, President Bush issued the Homeland Security Presidential Directive (HSPD-12) stating:

> [I]t is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and *protect personal privacy* by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)." (*Emphasis added*).

To that end, the President directed the Department of Commerce to promulgate a government-wide secure identification standard.

On October 20, 2004, NIST issued a preliminary draft of the Federal Personal Identity Verification standard. In response to that draft, JDS submitted comments that stressed the importance of implementing comprehensive privacy practices and procedures at each stage that personally identifiable data is collected, used

[1] Founded in 1998, JDS is the world's leading privacy solutions firm, working with companies and governmental agencies throughout the United States and around the world. JDS has been actively involved with industry groups, and has worked with the U.S. Department of Commerce on the Safe Harbor negotiations between the United States and Europe, the Article 29 Working Committee in the European Union, and global data management projects and initiatives in the United States and over 55 jurisdictions globally. JDS has also been active in Washington, D.C. on privacy and technology issues, including participating in Federal Trade Commission forums and testifying before Congress.

and stored. JDS recommended the adoption of best privacy practices, such as the Fair Information Practices; JDS' Seven Step Privacy Management Process; and the issuance of privacy impact assessments.

Since the last comment period, Congress passed significant privacy legislation requiring federal agencies to have a Chief Privacy Officer (CPO). And most recently, JDS had the pleasure to meet with NIST staff from its Computer Security Division. We applaud the NIST staff's efforts to minimize the amount of personally identifiable information on the actual card and appreciate their interest in learning how the standards can help bridge the privacy knowledge gap at the agency technical level.

Federal Chief Privacy Officer Law

As part of the recently enacted omnibus spending act for fiscal year 2005, Congress recognized the importance of privacy and data protection by requiring that agencies appoint a CPO responsible for implementing a comprehensive privacy management program.[2]

Specifically, the law requires the:

- CPO to assure technology sustains and does not erode privacy protections, conduct privacy impact assessment of proposed rules promulgated by the Department, and train and educate employees on privacy.
- CPO to establish and implement comprehensive privacy and data protection procedures by end of 2005.
- CPO to prepare an annual report to Congress on activities of the Department that affect privacy.
- CPO to prepare a report of its use of information along with its privacy and data protection policies and procedures to serve as a benchmark for the agency and record it with the agency's Inspector General.
- Inspector General to contract with an independent, third party that is a recognized leader in privacy consulting, privacy technology, data collection and data use management and global privacy to review the privacy and data protection procedures of the agency.
- Inspector General to submit a detailed report to the head of the agency concerning the third party review, including recommendations for improvement.

This new mandate not only acknowledges the government's increased use and collection of personal data as it continues to secure buildings, ports and critical infrastructure, but the ease in which the government is able to access such data in the digital age. The law also complements the E-Government Act of 2002 that,

[2] Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (division H of the Consolidated Appropriations Act, 2005) (HR 4818).

among other things, requires Federal agencies to conduct a Privacy Impact Assessment (PIA) when procuring or deploying a new information technology system that collects, uses and shares personal information. While the information collected under the PIV standard may be primarily viewed as an internal system, in the interest of transparency, it would be a best practice for agencies to perform PIAs on such systems

In charging an agency's Inspector General with retaining an independent third party that is a recognized privacy consulting leader to conduct a biennial review, the Congress created additional accountability within an agency that should heighten the public's confidence in the government's treatment of their personal data.

One of the first tasks a new CPO may face is the implementation of the NIST PIV standards. Given that past is prologue, it is critical for a new CPO to appreciate that privacy management is not merely a regulatory compliance hurdle, but the backbone to any information collection program. A sound privacy management program that is incorporated into a system from its inception is essential to building public support for the program and to the program's ultimate success. A weak privacy management initiative of a high profile program, such as one envisioned by HSPD-12, will handicap the program, regardless of the strong IT security parameters built into the system.

Notably, recent federal government projects had to either be revamped or canceled because of significant privacy concerns raised by the public and privacy community. This negative outcome can be prevented, or at lease mitigated, by a recognition from the highest levels of an agency that the use and collection of personal data requires an effective management strategy that respects and protects an individual's personal information.

In addition, it is critical that those within the agencies directly responsible for implementing the PIV standard understand their responsibility to coordinate with agency privacy officials at each step of the way. This is particularly important given the potential for the standard to impact not just Government employees and contractors, but also military family members. Therefore, JDS recommends that the standard acknowledge the importance of such coordination and the need for each agency to develop a privacy management program in conjunction with the implementation of the new PIV standard.

Biometrics and Privacy

As JDS stated in our last round of comments, the Fair Information Practices (FIPs) are widely recognized privacy principles that serve as the foundation for any comprehensive privacy program. The FIPs include: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; Enforcement/Redress.

It is the Integrity/Security principle that NIST needs to address as it plans to collect biometric data. The latest public draft requires the collection of the following biometric data:

- Ten fingerprints to support law enforcement check during the application process;
- Two electronic fingerprints to be stored on the card for automated verification process; and
- A digitized facial image to be stored on the card for alternate identity verification process.[3]

JDS understands and supports the use of biometric data, provided the appropriate protections of this sensitive data are woven into the standards at the time the database is being created.

A concern the privacy community has raised with biometric identifiers involves compromised data through fraudulent applicants at registration and security breaches. For instance, if an individual provides fake documentation, such as a passport, social security number or birth certificate, then the biometric used at the time of registration will only serve to validate the underlying fraudulent data. It is therefore critical to search the database for an individual using multiple identifies or duplicating an existing one.

A biometric identifier may also be altered at the time of registration. For example, a Japanese study using artificial fingers made out of gelatin, similar to "gummy bears," successfully deceived fingerprint scanners 67% of the time using 11 different fingerprint systems.[4]

Additionally, there is always the potential for hackers to alter stored data or data as it being transmitted. The seriousness of a security breach that compromises biometric data can be irreparable since, unlike a fraudulent or stolen document, a stolen biometric cannot be replaced. The charlatan will be granted access, while the victim of this identity theft will be denied access and be left with the unthinkable task of proving someone else has his/her unique biometric identifier.

Finally, in order to ensure compliance with Section 508 of the Rehabilitation Act of 1973,[5] NIST should explore alternative biometric identifiers such as iris scans, gait technology that recognizes an individual's walk, and vein patterns.[6]

---

[3] Federal Information Processing Standards Publication 201, "Personal Identity Verification (PIV) for Federal Employees and Contractors," *PUBLIC DRAFT*, p. 30 (Version 1.0).

[4] Tsutomu Matsumoto, et al. "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Graduate School of Environment and Information Sciences, Yokohama National University at http://cryptome.org/gummy.htm (January 2002)

[5] The Workforce Investment Act of 1998, Public Law 105–220, amended Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d).

[6] "An Biometric Identification System by Extracting Hand Vein Patterns" at http://www.cs.virginia.edu/~jones/cs851sig/papers/im01_hand_vein_patterns.pdf

Conclusion

The creation of a government-wide PIV Standard is a logical and practical step in the right direction. At the same time, it is critical for NIST to ensure that a comprehensive privacy program be an integral part of the PIV Standard so as to fulfill the President's directive to protect personal privacy.

JDS appreciates the opportunity to provide these comments to the FIPS 201 and is willing to assist NIST, in any way, as it moves forward with this project. JDS looks forward to your comments and questions.

Contact:

Mark Becker
Director
Jefferson Data Strategies, LLC
1401 K Street
Washington, DC 20005
202-626-8596
mbecker@jdstrategies.com

cc: William e. Burr (william.burr@nist.gov)
W.Timothy Polk (william.polk@nist.gov)
Donna F. Dodson (donna.dodson@nist.gov)
National Institute of Standards and Technology
Computer Security Division
Information Technology Laboratory