epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

National Institute of Standards and Technology

Request for Comments on Federal Information Processing Standard (FIPS) 201-3

[Docket No. 201023-0280]

February 1, 2021

EPIC submits these comments in response to the National Institute of Standards and Technology's (NIST) draft updates to the Federal Information Processing Standards (FIPS), Personal Identity Verification of Federal Employees and Contractors standard, FIPS 201-3.[1] NIST's proposed updates will permit increased collection of biometric data including iris and facial recognition images, strengthen cryptography requirements for identity verification systems, and require broader federation for identity card systems among other changes.[2]

EPIC is concerned that the current draft standards are not sufficiently privacy-protective for federal employees and contractors. EPIC is also concerned that the standards will lead to unnecessarily stringent identity verification in the private sector, escalating surveillance of private sector employees and the public. EPIC urges NIST to adopt standards that 1) require anonymous credentialing for identity verification, 2) limit all collection and use of biometric data to 1:1 matching with a biometric profile encoded on the identity card, not stored in a virtual database, 3)

---

[1] Request for Comments on Federal Information Processing Standard (FIPS) 201-3, 85 Fed. Reg. 69599, Nov. 3, 2020.
[2] Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS PUB 201-3 (draft), Nov. 2020, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3-draft.pdf.

require regular privacy audits of PIV systems, and 4) provide employees with convenient personal access to identity verification logs.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has long advocated for limits on the use of biometric identifiers to protect privacy and civil liberties.[3] EPIC has also focused on the need to preserve privacy protections for federal employees.[4]

I. Features of a Privacy Protective Personal Identity Verification System

The updates to FIPS 201-3 provide an opportunity for NIST and the federal government to take a leading role in promoting privacy protective standards for authentication in both physical systems and online. This leadership is sorely needed to make sure that there are good, interoperable authentication mechanisms that are both secure and privacy friendly. Whatever standards NIST adopts will drive private sector practices because of the scale of the systems deployed by the federal government. NIST should be careful to adopt the most privacy-protective technologies and designs available to protect government workers and, by downstream effects, private sector employees.

---

[3] EPIC, *Biometric Identifiers*, https://epic.org/privacy/biometrics/; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf; Comments of EPIC to the Department of Homeland Security, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services—018 Immigration Biometric and Background Check (IBBC) System of Records, Docket Nos. DHS-2018-0002 and DHS-2018-0003 (Aug. 30, 2018), https://epic.org/apa/comments/EPIC-DHS-Immigration-Biometric-Database.pdf; Comments of EPIC to the Department of Homeland Security/U.S. Customs and Border Protection, Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, Docket No. USCBP-2020-0062 (Dec. 21, 2020), https://epic.org/apa/comments/EPIC-Comments-CBP-Biometric-Entry-Exit-December-2020.pdf.

[4] Comments of EPIC to the Department of Transportation, Notice of Privacy Act System of Records; Notice of Proposed Rulemaking Insider Threat Database, (Nov. 2, 2018), https://epic.org/apa/comments/EPIC-Comments-DOT-Insider-Threat-Database.pdf.

EPIC believes that the best standards for identity verification would use cryptographic digital certificates to associate a device (such as a laptop, a smartphone or a special-purpose authentication dongle or badge) with a particular employee or organization. That way, the verification of the employee device need not involve third-party intermediaries; instead, the verifier can simply check the certificate, and can operate off-line. Moreover, no one except the verifier with whom the employee is interacting will learn of the employee's activities, protecting the employee's privacy. Such features are important for many of the 2.1 million federal employees and millions of federal contractors who use systems that require identity verification.[5]

As biometrics are adopted for identity verification it is crucially important for NIST to ensure that the systems are reliable and preserve privacy. The draft standards meet this need by permitting 1:1 authentication with fingerprint, iris, or facial images stored directly on the PIV card.[6] However, NIST's proposed standards would permit both off-card authentication (§ 6.2.1) and on-card authentication (§ 6.2.2) by biometric identifiers. NIST should endorse only on-card authentication to minimize the exposure of biometric information and consequential risk of data breach. NIST should also mandate contemporaneous notice for the employee any time a biometric is collected and require employee consent before the collection of biometric information.

The best design would be compatible with anonymous credentials to implement privacy-preserving authentication.[7] Anonymous credentials would allow a federal employee to prove to a

[5] Cong. Rsch. Serv., R43590, Federal Workforce Statistics Sources: OPM and OMB 4 (*last updated* Oct. 23, 2020), https://fas.org/sgp/crs/misc/R43590.pdf.
[6] FIPS PUB 201-3 (draft) at 70-72.
[7] *See e.g.* Anna Lysyanskya, *Signature schemes and applications to cryptographic protocol design* (2002), https://dspace.mit.edu/handle/1721.1/29271, Melissa Chase, *Efficient Non-Interactive Zero-Knowledge Proofs for Privacy Applications* (May 2008), http://static.cs.brown.edu/research/pubs/theses/phd/2008/chase.pdf, Fonteini Baldimtsi, *Efficient Cryptography for Information Privacy* (May 2014), https://cs.brown.edu/research/pubs/theses/phd/2014/baldimtsi.pdf, Endre Bangerter, Jan Camenisch, Anna Lysyanskaya, A Cryptographic Framework for the Controlled Release of Certified Data, 3957 LNCS 20-42 (2006), https://link.springer.com/chapter/10.1007%2F11861386_4.

verifier that the employee has a security clearance, without revealing any other information. Unlike other verification standards, anonymous credentials do not leave behind a persistent identifier that can link an employee to other authentication instances. This both safeguards the personal privacy of the employee (so that even verifiers cannot trace an employee across many transactions) and still ensures that government data will not be accessed without the proper credentials.

To protect individuals from the threat of data breach, NIST should also require regular privacy audits. The audits should ensure that records of employee movements are securely stored and promptly deleted after the appropriate retention period. Data breaches are common across the federal government and often harm public sector workers. For example, many agencies across the federal government were recently exposed in the SolarWinds hack.[8] Hackers gained access to systems across the federal government despite DHS's complex cybersecurity defense systems and a 2018 warning from the GAO that agencies were vulnerable to the exact type of "supply chain" attack used by the SolarWinds hackers.[9] A 2015 data breach at the Office of Personnel Management (OPM) exposed social security numbers and other personal data from 21.5 million individuals.[10] Both strong data security standards and limited retention of sensitive information are necessary to combat the threat of data breach.

In addition to the regular privacy audits, NIST should also mandate that employees have convenient access to their authentication logs, equivalent to the employer's access. Providing easy

[8] Megan Roos, *Suspected Russian SolarWinds Hack Compromised Homeland Security Department*, Newsweek (Dec. 14, 2020) https://www.newsweek.com/suspected-russian-solarwinds-hack-compromised-homeland-security-department-1554656.
[9] Brian Barrett, *Security News This Week: Russia's SolarWinds Hack Is a Historic Mess*, Wired (Dec. 19, 2020) https://www.wired.com/story/russia-solarwinds-hack-roundup/.
[10] GAO-19-105 Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions (Dec. 18, 2018), https://www.gao.gov/assets/700/696105.pdf.

access to these logs would allow employees to identify and correct errors, and to understand how their data is being collected and used.

Conclusion

EPIC urges NIST to revise the draft PIV FIPS to adopt privacy-enhancing standards and technologies. NIST should 1) require anonymous credentialing for identity verification, 2) limit all collection and use of biometric data to 1:1 matching with a biometric profile encoded on the identity card, not stored in a virtual database, 3) require regular privacy audits of PIV systems, and 4) provide employees with convenient personal access to identity verification logs.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Law Fellow

Alan Butler
Alan Butler
EPIC Interim Executive Director