epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, 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, U.S. DEPARTMENT OF COMMERCE

"Request for Comments: Updating Risk Management Framework to Incorporate Privacy Considerations"

June 22, 2018

By notice published on May 9, 2018, the National Institute of Standards and Technology ("NIST") requested comments regarding the updated Risk Management Framework ("RMF") (*Draft NIST Special Publication (SP) 800-37 Revision 2*).[1] The RMF is "a guidance document designed to help organizations assess and manage risks to their information and systems."[2] The Electronic Privacy Information Center ("EPIC") submits these comments to urge NIST to revise the RMF document to make clear that federal agencies are required to conduct privacy impact assessments ("PIA"), under the E-Government Act, prior to the creation of a new system of records containing personally identifiable information.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus on emerging civil liberties issues and protecting privacy, the First Amendment, and constitutional values. EPIC has a long history of promoting transparency and accountability for cybersecurity and government data collection programs, specifically through the enforcement of the Privacy Act and the Freedom of Information Act.[3] EPIC has long worked to promote transparency and accountability for information technology. EPIC has brought numerous successful cases seeking the release of Privacy Impact Assessments. In *EPIC v. DHS*, No. 11-2261 (D.D.C. Dec. 20, 2011), EPIC obtained a PIA and related records concerning a prior effort by the DHS to track social media

[1] SP 800-37 Rev. 2 (DRAFT) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (2018) https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft.

[2] NIST Updates Risk Management Framework to Incorporate Privacy Considerations (2018) https://www.nist.gov/news-events/news/2018/05/nist-updates-risk-management-framework-incorporate-privacy-considerations

[3] See EPIC v. NSA, 678 F.3d 926 (D.C. Cir. 2012); EPIC, Cybersecurity Privacy Practical Implications, http://epic.org/privacy/cybersecurity/; EPIC, EPIC v. NSA – Cybersecurity Authority, http://epic.org/privacy/nsa/epic_v_nsa.html; EPIC, Comments of the Elec. Privacy Info. Ctr. to the Cyber Security and Information Assurance Research and Development Senior Steering Group of the Federal Networking and Information Technology Research and Development Program: Request for Comments, Dec. 19, 2012, available at http://epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-SecurityComments.pdf

users and journalists.[4] EPIC made the previously undisclosed documents available to the public on its website. In *EPIC v. FBI*, No. 14-1311 (D.D.C. Aug. 1, 2014), EPIC obtained unpublished PIAs from the Federal Bureau of Investigation concerning facial recognition technology, which EPIC also made available to the public on its website.[5] And in *EPIC v. DEA*, No. 15-667 (D.D.C. May 1, 2015), EPIC learned that the Drug Enforcement Administration had failed to produce PIAs for the agency's license plate reader program, a telecommunications records database, and other systems of public surveillance.[6] EPIC reported the agency's failure to produce a PIA on its website. More recently, in *EPIC v. Presidential Advisory Commission on Election Integrity*, 266 F. Supp. 3d 297 (D.D.C.), *aff'd on other grounds*, 878 F.3d 371 (D.C. Cir. 2017), EPIC challenged the failure of the Presidential Advisory Commission on Election Integrity to undertake and publish a PIA prior to the collection of state voter data.[7] EPIC's suit led the Commission to temporarily suspend its data collection, discontinue the use of an unsafe computer server, and delete voter information that had been illegally obtained.[8] EPIC's new "Privacy Impact Assessment" initiative is a key component of the organization's long-running open government project and consumer protection work. EPIC broadly promotes "Algorithmic Transparency."[9]

While previous versions of the RMF were primarily concerned with cybersecurity protections from external threats, the updated version focuses on individuals' privacy to ensure that organizations are able to identify and respond to privacy risks, particularly those associated with personally identifiable information."[10] EPIC supports NIST's focus on privacy risks. However, there is a glaring omission: the Section 208 of E-Government Act, which requires federal agencies to conduct and publish Privacy Impact Assessments, prior to collection of personally identifiable information, is not mentioned. Since the RMF is a guidance document to be used by the federal government, it is essential to include a discussion of when agencies are required to produce PIAs under the E-Government Act.

NIST should revise the RMF to explain the legal obligation federal agencies have to conduct PIAs prior to creating new systems that collect personal information. The RMF's mention of PIAs does not adequately convey their importance. In the RMF's section on authorization packages, the document states: "[t]he security and privacy plans may also include as supporting appendices or as references, additional security- and privacy-related documents such as a privacy impact assessment…"[11] This gives a misleading impression that a PIA is supplementary to an agency's responsibilities to safeguard privacy, when in fact it is essential. Moreover, the definition of PIA does not properly explain this.[12]

---

[4] *See* EPIC, *EPIC v. Department of Homeland Security: Media Monitoring* (2015), https://www.epic.org/foia/epic-v-dhs-media-monitoring/.
[5] *See* EPIC, *EPIC v. FBI – Privacy Assessments* (2016), https://epic.org/foia/fbi/pia/.
[6] *See* EPIC, *EPIC v. DEA – Privacy Impact Assessments* (2016), https://epic.org/foia/dea/pia/.
[7] *See* EPIC, *EPIC v. Presidential Election Commission* (2018), https://epic.org/privacy/litigation/voter/epic-v-commission/.
[8] *Id.*
[9] EPIC, *Algorithmic Transparency*, https://epic.org/algorithmic-transparency/.
[10] *Id.*
[11] *Supra* note 1 at 133.
[12] *Id.* at 101.

Under Section 208 of the E-Government Act, agencies must undertake and publish a Privacy Impact Assessment *before* the agency (1) "develop[s] or procur[es] information technology that collects, maintains, or disseminates information that is in an identifiable form," or (2) "initiat[es] a new collection of information" that "includes any information in an identifiable form."[13] Information is "in an identifiable form" if it allows the identity of an individual to be directly or indirectly inferred.[14]

A PIA evaluates potential privacy risks "at the beginning of and throughout the development life cycle of a program or system."[15] Through the creation and publication of a PIA, the public can learn what personally identifiable information ("PII") is being collected, "why it is being collected, and how it will be used, shared, accessed, secured, and stored."[16]According to the Office of Management and Budget, which oversees enforcement of the E-Government Act, "Agencies should commence a PIA when they begin to develop a new or significantly modified [information technology] system or information collection."[17]

A PIA at the "IT development stage" should "address the impact the system will have on an individual's privacy specifically identifying and evaluating potential threats[.]"[18] The PIA "may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis."[19]

The updated RMF process is based on seven key steps—prepare, categorize, select, implement, assess, authorize, and monitor—and the first three steps mirror PIA requirements. Agencies are to first *prepare* to execute the RMF from the perspective of both the overall organization as well individual systems. Specifically, agencies are tasked with completing essential tasks to determine help prepare to manage security and privacy risks via the RMF. As agencies prepare, agencies will establish how to secure privacy information. Under the E-Government Act, agencies are required to include disclose in their privacy impact assessment "how the information will be secured."[20] Thus, the first step of the RMF aligns with the sixth PIA requirement.

---

[13] E-Government Act of 2002, Pub. L. No. 107-347, § 208(b)(1)(A), 116 Stat. 2899 (2002).
[14] U.S. Dep't Homeland Sec., *Privacy Impact Assessments: The Privacy Office Official Guidance* 1 (2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf [hereinafter *DHS PIA Official Guidance*].
https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html
[15] U.S. Dep't of Homeland Sec., *Privacy Compliance: Privacy Impact Assessment (PIA)* (Mar. 30, 2017), https://www.dhs.gov/compliance.
[16] U.S. Dep't of Homeland Sec., *Privacy Compliance: Privacy Impact Assessment (PIA)* (Mar. 30, 2017), https://www.dhs.gov/compliance.
[17] Office of Mgmt. and Budget, Exec. Office of the President, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* at 5 (Sept. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf [hereinafter *OMB E-Government Act Guidance*].
[18] *Id.*
[19] *Id.* at 5–6.
[20] § 208(b)(2)(B)(ii)

Once the preparation phase is complete, agencies are to *categorize* their systems as well as the information flowing in and out of the systems based on their analysis of security impact. Categorization results impact the selection of security controls for the system and thus should take into consideration the level of sensitivity of the information involved, especially if personally identifiable information. The E-Government Act also charges agencies to disclose "what information is to be collected," "why the information is being collected," "the intended use of the agency of the information," "with whom the information will be shared," "what notice or opportunities for consent should would be provided to individuals regarding what information is collected and how that information is shared," and "whether a system of records is being created." Thus, the second step of the RMF aligns with the first-fifth and seventh PIA requirement.

Post preparation and categorization, agencies are to *select* system controls and modify those controls when needed based on a risk assessment and local conditions. In this step, agencies allocate security and privacy requirements to their systems and the environment they operate in. Thus, the third step also aligns with the sixth PIA requirement under the E-Government Act.

The RMF should explain the correlation between its first three steps—prepare, categorize, and select—and the PIAs mandated by the E-Government Act. This will clarify how federal agencies' legal obligations fit into NIST's privacy framework.

NIST's update to the RMF comes at a critical time. In fiscal year 2016, government agencies reported 30,899 information security incidents, including attacks on vital election and tax systems.[21] Many of these incidents could have been avoided if agencies had conducted Privacy Impact Assessments and followed NIST's framework.

NIST's objective to protect the nation from cybersecurity threats and protect individuals' privacy will be better served if NIST revises the RMF document to include a discussion of the obligation of federal agencies to undertake Privacy Impact Assessments.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow

/s/ *Jasmine Bowers*
Jasmine Bowers
EPIC PhDX Fellow

[21] Riley Walters, Federal Cyber Breaches in 2017, The Heritage Foundation (Jan. 3, 2018), https://www.heritage.org/cybersecurity/report/federal-cyber-breaches-2017. A Russian hacker was seeking to sell access credentials of the Election Assistance Commission database and the IRS Data Retrieval Tool was hacked, compromising the personal information of approximately 100,000 people.