COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to the
OFFICE OF PERSONNEL MANAGEMENT
Notice of Submission for Approval: Information Collection 3206-0258; Questionnaire for Public Trust Positions (SF 85P) and Supplemental Questionnaire for Selected Positions (SF 85P-S)
[OMB Control No. 3206-0258]
May 24, 2016

By notice published on March 25, 2016, the Office of Personnel Management (“OPM”) seeks Office of Management and Budget (“OMB”) approval for a revised information collection, control number 3206-0258, Questionnaire for Public Trust Positions, Standard Form 85P (SF 85P) and Supplemental Questionnaire for Selected Positions, Standard Form SF 85P-S (SF 85P-S). Pursuant to OPM’s notice, the Electronic Privacy Information Center (“EPIC”) submits these comments to address the substantial privacy and security issues raised by this information collection and to recommend that OPM narrow the categories of information collected in SF 85P and SF 85P-S.

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

1 Notice of Submission for Approval: Information Collection 3206-0258; Questionnaire for Public Trust Positions (SF 85P) and Supplemental Questionnaire for Selected Positions (SF 85P-S), 81 Fed. Reg. 16,224 (proposed Mar. 25, 2016) [hereinafter “OPM SF 85P ICR”].
protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards, established by Congress, for information collected by the federal government.²

1. **Purpose and Scope of the SF 85P and SF 85P-S Questionnaires**

OPM use Questionnaire for Public Trust Positions (“SF 85P”) and Supplemental Questionnaire for Selected Positions (“SF 85P-S”) to collect personal information for employment background investigations within the Federal government.³ The SF 85P-S supplements the SF 85P form for certain positions, including those that require carrying firearms. Federal government civilian employees, applicants, and Federal contractors are expected to complete the SF 85P Form and SF 85P-S Form.⁴

With the SF 85P Forms, OPM collects a wealth of sensitive, personal information about current and prospective employees of the Federal government, as well as their family members and friends. OPM collects the applicant’s full name, contact information, citizenship, biometric data, Social Security number, previous places of residence, educational history, past employment activities, medical information, foreign travel, drug use, and financial records.⁵ In addition, the agency collects extensive personal information about the applicant’s spouse, including Social Security number.

---


³ OPM SF 85P ICR at 16,225.

⁴ OPM SF 85P ICR at 16,225.

2. The Massive 2015 OPM Data Breach Compromised SF 85P and SF 85P-S Questionnaires Data of Millions of Americans

The detailed sensitive information included in the SF-85P Forms was a focal point of the 2015 OPM data breaches, which compromised the personal data of 21.5 million people, including 1.8 million people who did not apply for background checks. The OPM breach exposed sensitive background investigation data spanning three decades. “If you underwent a Federal background investigation in 2000 or afterwards (which occurs through the submission of forms SF-86, SF-85, or SF-85P for either a new investigation or a reinvestigation), it is highly likely that you are impacted by the incident involving background investigations. If you underwent a background investigation prior to 2000, you still may be impacted, but it is less likely,” OPM warns on its website. The fingerprints of 5.6 million people were also stolen in the data breach.

As a consequence of the OPM data breach, federal employees were asked to enroll in credit and identity theft monitoring. Many employees were wary that the monitoring service itself could be subject to a data breach and were reluctant to provide more personal information as was required for these services. Also, several lawsuits have been filed against the agency, charging that OPM violated the Privacy Act by disclosing individuals’ personally identifiable information.

---

information and that OPM “intentionally, willfully, and with flagrant disregard” violated the Federal Information Management Security Act. Congress held several hearings to uncover the extent of OPM’s breach. OPM Director Katherine Archuleta eventually resigned. And earlier this year, OPM CIO Donna Seymour resigned as well.

In November of 2014, the Inspector General warned OPM about serious security and privacy concerns after a smaller-scale data breach earlier that year. In fact, the Inspector General reported significant cybersecurity weaknesses at the agency as far back as 2007. OPM failed to act on these repeated warnings, resulting in the unprecedented breach of government-held data.

3. OPM Should Limit Information Collection in Light of its Inability to Effectively Protect the Data it Maintains

Data held by OPM and other Federal agencies is highly vulnerable to unauthorized access and theft, as cybersecurity weaknesses are widespread across government information systems. According to a recent report by the U.S. Government Accountability Office (“GAO”), “[c]yber-

---

17 Id. at 5.
based intrusions and attacks on federal systems have become not only more numerous and
diverse but also more damaging and disruptive.” The 2015 data breach at OPM compromised
the background investigation records of 21.5 million individuals. Also in 2015, the Internal
Revenue Service (“IRS”) reported that approximately 390,000 tax accounts were compromised,
exposing Social Security numbers, dates of birth, street addresses, and other sensitive
information. In 2014, a data breach at the U.S. Postal Service exposed personally identifiable
information for more than 80,000 employees.

The latest series of high-profile government data breaches indicates that Federal agencies
are incapable of adequately protecting sensitive information from improper disclosure. Indeed,
GAO recently released a report on widespread cybersecurity weaknesses throughout the
executive branch, aptly titled “Federal Agencies Need to Better Protect Sensitive Data.”
According to the GAO report, a majority of federal agencies “have weaknesses with the design
and implementation of information security controls …” In addition, most agencies “have
weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate
access to computer resources and managing the configurations of software and hardware.”
The GAO report concluded that, due to widespread cybersecurity weaknesses at most federal
agencies, “federal systems and information, as well as sensitive personal information about the
public, will be at an increased risk of compromise from cyber-based attacks and other threats.”

---

18 U.S. Gov’t Accountability Office, DHS Needs to Enhance Capabilities, Improve Planning, and Support
Greater Adoption of Its National Cybersecurity Protection System (Jan. 2016)
19 GAO Cybersecurity Report at 8.
20 Id. at 7-8.
21 Id. at 8.
22 GAO Sensitive Data Protection Report.
23 Id. at unpaginated “Highlights” section.
24 Id.
25 Id. at 12.
The information collected in the SF-85P forms includes health, financial, and education records; Social Security numbers; and individuals’ photographs or images. Federal contractors, security experts, and EPIC have previously argued to the U.S. Supreme Court that the federal governments simply should not collect much of this information.

In *NASA v. Nelson*, the Supreme Court considered whether federal contract employees have a Constitutional right to withhold personal information sought by the government in a background check. EPIC filed an *amicus* brief, signed by 27 technical experts and legal scholars, siding with the contractors employed by the Jet Propulsion Laboratory (“JPL”). EPIC’s brief highlighted problems with the Privacy Act, including the “routine use” exception, security breaches, and the agency’s authority to carve out its own exceptions to the Act. EPIC also argued that compelled collection of sensitive data would place at risk personal health information that is insufficiently protected by the agency, stating,

If NASA is permitted to collect the Scientists’ personal health information, there is a substantial risk that the data will be disclosed as a result of a data breach. Even the most rigorous statutory protections are no guarantee against exposure of

---

29 *See* Driver’s Privacy Protection Act, 18 U.S.C. § 2725(4) (defining “highly restricted personal information” to include “social security number”).
30 *Id.* § 2725(4) (defining “highly restricted personal information” to include “individual’s photograph or image”).
34 *Id.* at 20-28.
personal information in data breaches. . . [T]he well-documented, ubiquitous, imminent threat of data breaches demonstrates that NASA’s data collection does “implicate[] the principal concern for the privacy of [the Scientists’] personal information.” The only way that NASA can in good faith assure the Scientists that their information will not be disclosed is not to collect it in the first place.35]

The Supreme Court acknowledged that the background checks implicate “a privacy interest of Constitutional significance” but stopped short of limiting data collection by the agency, reasoning that the personal information would be protected under the Privacy Act.36

That turned out not to be true. Shortly after the Court’s decision, NASA experienced a significant data breach that compromised the personal information of about 10,000 employees, including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.37 The JPL-NASA breach is a clear warning that OPM should narrow the amount of sensitive data collected. Simply put, the government should not collect so much personal data; to do so unquestionably places people at risk.

In light of the unprecedented data breaches OPM experienced in 2015 and critical cybersecurity weaknesses across the federal government, OPM should limit the amount of sensitive data it collects via the SF 85P Forms and focus on improving data protection. OPM should also limit its retention of this sensitive data. Limiting the collection and retention of personal information minimizes the harm that results from potential data breaches.38

35 Id. at 28, 33.
4. **The Proposed Revisions to SF 85P Would Vastly Expand the Amount of Personal, Sensitive Information Collected by OPM, Creating Further Risk to Federal Employees**

Incredibly, following the unprecedented breach of sensitive data, the Congressional hearings, and the resignation of the OPM Director and the CIO, OPM seeks to collect even more personal information about more individuals. The agency should abandon this ill-advised plan and focus its efforts on improving its data protection practices.

OPM currently collects the full name, date of birth, country of birth, country(ies) of citizenship, and current address for the respondent’s Mother, Father, Stepmother, Stepfather, Foster Parent, Child, and Stepchild. OPM proposes to expand the category of relatives about whom information is collected to also include “Half-brother, Half-sister, Father-in-law, Mother-in-Law, and Guardian.” These individuals will involuntarily be placed at significant risk of having their personal data compromised due to OPM’s inadequate data protection.

OPM proposes to revise its request for information on “Involvement in Non-Criminal Court Actions” to collect information about any non-criminal court action in which the individual was a “participant.” Previously, this request was limited to actions in which the individual was the defendant. Such an expanded request could encompass child custody disputes and divorce proceedings. It could also require domestic abuse survivors to provide details about restraining orders they have obtained. These court actions can reveal highly personal and sensitive information that is unrelated to employment eligibility.

---

*the Global Economy* 21 (Feb. 23, 2012) (stating that companies “should collect only as much personal data as they need to accomplish purposes” and “should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise”).

39 OPM SF 85P ICR at 16,225.
40 OPM SF 85P ICR at 16,225.
OPM proposes to collect information from social media activity as part of the employment background investigation. Social media monitoring by the government raises significant privacy and civil liberty risks. Congress previously scrutinized government social media monitoring. The Equal Employment Opportunity Commission has also raised concerns about the potential discriminatory ways in which employers may use prospective employees’ social media information. Accordingly, OPM should not collect social media information as part of the employment background investigation.

OPM further proposes to revise questions about “Illegal Use of Drugs and Drug Activity” to require that “drug use of activity illegal under Federal laws must be reported, even if that use or activity is legal under state or local law(s).” As of 2016, Alaska, Colorado, Oregon, Washington, and Washington, D.C. have legalized recreational marijuana use. Twenty more states have legalized medical marijuana. This expanded information collection will impact a significant number of individuals, including many D.C. residents employed by the many Federal agencies located in that region. Additionally, requiring individuals to disclose their use of

---

41 OPM SF 85P ICR at 16,225.
45 OPM SF 85P ICR at 16,225.
medical marijuana implicates significant privacy interests in medical information and treatment confidentiality.\(^{47}\)

**Conclusion**

For the foregoing reasons, OPM should repeal its proposed expansion of information collected via Forms SF 85P and prioritize limiting data collection and improving cybersecurity.

Respectfully submitted,

Marc Rotenberg  
EPIC President and Executive Director

Khaliah Barnes  
EPIC Associate Director and Administrative Law Counsel

Claire Gartland  
EPIC Consumer Protection Counsel

---

\(^{47}\) See, e.g., EPIC, *IMS Health v. Sorrell* (Concerning the Use of Prescriber-Identifiable Data for Targeted Marketing), https://epic.org/privacy/ims_sorrell/.