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,[1] 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.

---

[2] *See, e.g.*, Comments of EPIC to DHS, Insider Threat Program System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2015-0049 and 0050 (Mar. 28, 2016), https://epic.org/apa/comments/EPIC-DHS-Inisder-Threat-Comments.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2016-0002 and 0001 (Feb. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORNExemptions-2016.pdf; Comments of EPIC to the Department of Education, Impact Evaluation of Data-Driven Instruction Professional Development for Teachers System of Records Notice, FR Doc. 2015-30526 (Jan 4., 2016), https://epic.org/privacy/student/EPIC-Comments-ED-Impact-Eval-SORN.pdf.

[3] OPM SF 85P ICR at 16,225.

[4] OPM SF 85P ICR at 16,225.

[5] Standard Form 85P, *Questionnaire for Public Trust Positions* (1995).

### 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.[6] The OPM breach exposed sensitive background investigation data spanning three decades.[7] "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.[8] The fingerprints of 5.6 million people were also stolen in the data breach.[9]

As a consequence of the OPM data breach, federal employees were asked to enroll in credit and identity theft monitoring.[10] 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.[11] Also, several lawsuits have been filed against the agency, charging that OPM violated the Privacy Act by disclosing individuals' personally identifiable

[6] Dan Goodin, *Call it a "Data Rupture": Hack Hitting OPM Affects 21.5 Million*, ARSTECHNICA (July 9, 2015), http://arstechnica.com/security/2015/07/call-it-a-data-rupture-hack-hitting-opm-affects-21-5-million/.
[7] Andrea Shalal & Matt Spetalnick, *Data Hacked from U.S. Government Dates Back to 1985: U.S. Official*, REUTERS (June 5, 2015), http://www.reuters.com/article/us-cybersecurity-usa-idUSKBN0OL1V320150606.
[8] Office of Personnel Management, *Cybersecurity Incidents, Cybersecurity Resource Center*, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.
[9] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sep. 23 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.
[10] Office of Personnel Management, *Cybersecurity Resource Center*, https://www.opm.gov/cybersecurity/.
[11] Michelle Singletary, *What to do if you are affected by the OPM data breach*, WASH. POST (Dec. 11, 2015), https://www.washingtonpost.com/business/get-there/what-to-do-if-you-are-affected-by-the-opm-data-breach/2015/12/09/534455e0-9dd0-11e5-a3c5-c77f2cc5a43c_story.html.

information and that OPM "intentionally, willfully, and with flagrant disregard" violated the Federal Information Management Security Act.[12] Congress held several hearings to uncover the extent of OPM's breach.[13] OPM Director Katherine Archuleta eventually resigned.[14] And earlier this year, OPM CIO Donna Seymour resigned as well.[15]

In November of 2014, the Inspector General warned OPM about serious security and privacy concerns after a smaller-scale data breach earlier that year.[16] In fact, the Inspector General reported significant cybersecurity weaknesses at the agency as far back as 2007.[17] 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-

---

[12] Class Action Compl. at 47, *American Federation of Gov't Employees v. OPM* , (No. 15-01015) (D.D.C. filed June 29, 2015), *available at* http://www.girardgibbs.com/blog/wp-content/uploads/2015/06/Complaint-American-Fed-of-Govt-Employees-v-US-OPM.pdf. *See also* Meredith Somers, *Lead Attorney Named for Class-Action Case Against OPM*, FEDERAL NEWS RADIO (Feb. 1, 2016, 5:12 am), http://federalnewsradio.com/opm-cyber-breach/2016/02/lead-attorney-named-class-action-case-opm/.

[13] *See, e.g.*, *OPM: Data Breach Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (2015), https://oversight.house.gov/hearing/opm-data-breach/; *OPM: Data Breach: Part II Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (2015), https://oversight.house.gov/hearing/opm-data-breach-part-i/.

[14] Julie Hirschfeld Davis, *Katherine Archuleta, Director of Personnel Agency, Resigns*, N.Y. TIMES (July 10, 2015), http://www.nytimes.com/2015/07/11/us/katherine-archuleta-director-of-office-of-personnel-management-resigns.html?nlid=66044131.

[15] Angus Loten, *OPM CIO Resigns, but Blame for Data Breach Lingers*, WALL ST. J: CIO JOURNAL (Feb. 23, 2016, 5:33 PM), http://blogs.wsj.com/cio/2016/02/23/opm-cio-resigns-but-blame-for-data-breach-lingers/.

[16] U.S. Office of Personnel Management, Office of the Inspector General, *Federal Information Security Management Act Audit: FY 2014* (Nov. 12, 2014), https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[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."[18] The 2015 data breach at OPM compromised the background investigation records of 21.5 million individuals.[19] 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.[20] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[21]

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."[22] According to the GAO report, a majority of federal agencies "have weaknesses with the design and implementation of information security controls …"[23] 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."[24] 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."[25]

---

[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) http://www.gao.gov/assets/680/674829.pdf [hereinafter "GAO Cybersecurity Report"].
[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,[26] financial,[27] and education[28] records; Social Security numbers;[29] and individuals' photographs or images.[30] 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.[31]

In *NASA v. Nelson*,[32] 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").[33] 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.[34] 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

[26] *See* Heath Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C.).
[27] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered section of 12 and 15 U.S.C.).
[28] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[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").
[31] Brief for Union of Concerned Scientists as Amici Curiae Supporting Respondents, *Nat'l Aeronautics & Space Admin. v. Nelson* , 562 U.S. 134 (2011) (No. 09-530); Brief for American Astronomical Society as Amici Curiae Supporting Respondents, *Nat'l Aeronautics & Space Admin. v. Nelson* , 562 U.S. 134 (2011) (No. 09-530); Brief for EPIC and legal scholars and technical experts as Amicus Curiae Supporting Respondents, *Nat'l Aeronautics & Space Admin. v. Nelson*, https://epic.org/amicus/nasavnelson/EPIC_amicus_NASA_final.pdf.
[32] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[33] Brief for EPIC and legal scholars and technical experts as Amicus Curiae Supporting Respondents, *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011), https://epic.org/amicus/nasavnelson/EPIC_amicus_NASA_final.pdf.
[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.
[36] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).
[37] Natasha Singer, *Losing in Court, and to Laptop Thieves, in a Battle With NASA Over Private Data*, N.Y. TIMES (Nov. 28, 2012), http://www.nytimes.com/2012/11/29/technology/ex-nasa-scientists-data-fears-come-true.html.
[38] *See* Jeff Jonas and Jim Harper, *Open Government: The Privacy Imperative*, in OPEN GOVERNMENT: TRANSPARENCY, COLLABORATION, AND PARTICIPATION IN PRACTICE 316-317 (Daniel Lathrop and Laurel R.T. Ruma eds., 2010), *available at* http://jeffjonas.typepad.com/Open_Government_ch29_Sampler.pdf . *See also* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in*

### 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."[39] 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."[40] 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.[41] Social media monitoring by the government raises significant privacy and civil liberty risks.[42] Congress previously scrutinized government social media monitoring.[43] The Equal Employment Opportunity Commission has also raised concerns about the potential discriminatory ways in which employers may use prospective employees' social media information.[44] 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)."[45] As of 2016, Alaska, Colorado, Oregon, Washington, and Washington, D.C. have legalized recreational marijuana use. Twenty more states have legalized medical marijuana.[46] 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.
[42] *See, e.g.*, EPIC, *EPIC v. Department of Homeland Security: Media Monitoring (Seeking Disclosure of Records Detailing the Department of Homeland Security's Media Monitoring Activities)*, https://epic.org/foia/epic-v-dhs-media-monitoring/.
[43] *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy Before the Counterterrorism and Intelligence Subcommittee*, 112th Cong (2012), https://homeland.house.gov/hearing/subcommittee-hearing-dhs-monitoring-social-networking-and-media-enhancing-intelligence/.
[44] Press Release, U.S. Equal Employment Opportunity Commission, Social Media is Part of Today's Workplace but its Use May Raise Employment Discrimination Concerns (Mar. 12, 2014), https://www.eeoc.gov/eeoc/newsroom/release/3-12-14.cfm.
[45] OPM SF 85P ICR at 16,225.
[46] Liz Rowley, *Where is Marijuana Legal in the United States? List of Recreational and Medicinal States*, MIC (Oct. 5, 2015) https://mic.com/articles/126303/where-is-marijuana-legal-in-the-united-states-list-of-recreational-and-medicinal-states#.rDqnsSDN5. Medical marijuana use is legal in Alaska, Arizona, California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, Oregon, Pennsylvania, Rhode Island, Vermont, and Washington. *Id*.

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/.