UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, ROBERT CRAWFORD, and ADAM DALE on behalf of themselves and all others similarly situated, Plaintiffs, vs. UNITED STATES OFFICE OF PERSONNEL MANAGEMENT, 1900 E. Street, NW Washington, DC 20415, KATHERINE ARCHULETA, Director of United States Office of Personnel Management, in her official capacity, 1900 E. Street, NW Washington, DC 20415, DONNA SEYMOUR, Chief Information Officer, in her official capacity, 1900 E. Street, NW Washington, DC 20415, and KEYPOINT GOVERNMENT SOLUTIONS, 1750 Foxtrail Drive Loveland, CO 80538. Defendants.	Case No. 1:15-cv-1015 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs the American Federation of Government Employees, AFL-CIO ("AFGE"), Robert Crawford, and Adam Dale individually and on behalf of the proposed class described below, bring this action for injunctive relief, and actual and statutory damages against Defendants United States Office of Personnel Management ("the OPM"), Director Katherine

Archuleta ("Archuleta"), Chief Information Officer Donna Seymour ("Seymour") (collectively "the OPM Defendants"), and KeyPoint Government Solutions ("KeyPoint") and allege as follows:

I. SUMMARY OF THE CASE

1. This case arises out of the cyber-breach of OPM's systems that compromised the security of up to 18 million federal applicants' personnel and security files, which top lawmakers described as "the most devastating cyber attack in our nation's history" (the "OPM Breach"). Plaintiffs and Class members include current, former, and prospective employees and contractors ("federal applicants") of the U.S. government.

2. The OPM is a government agency responsible for maintaining large amounts of data about federal applicants:

> [The] OPM provides investigative products and services for over 100 Federal agencies to use as a basis for suitability and security clearance determinations as required by Executive Orders and other rules and regulations. [The] OPM provides over 90% of the Government's background investigations, conducting over two million investigations a year.

3. As part of the OPM's security clearance protocol, applicants applying for security clearance ("security applicants") must submit Standard Form 86 ("SF-86"), a detailed, 127-page form that includes questions regarding "[security] applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and coworkers."

4. Since at least 2007, the OPM has been on notice of significant deficiencies in its cyber security protocol. Despite the fact that the OPM handles massive amounts of federal applicants' private, sensitive, and confidential information, the OPM failed to take steps to

remedy those deficiencies. The OPM's Office of Inspector General ("OIG") was required under federal law to, and did, conduct annual audits of the OPM's cyber security program and practices, identifying "material weakness[es]"[1] as far back as 2007. The OPM not only failed to cure the weaknesses, but the OIG found that in many areas the OPM's performance actually got worse. According to a 2014 OIG report, the "drastic increase in the number of [software] systems operating without valid authorization is alarming and represents a systemic issue of inadequate planning by the OPM offices to authorize the [software] systems they own."

5. From 2007 to the present, the OPM, Seymour, and Archuleta—who has served as the OPM's director since November 2013—repeatedly failed to comply with federal law and make the changes required by the OIG's annual audit reports. Thus the OPM failed to comply with the Privacy Act which requires federal agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

6. In its November 2014 audit report, the OIG identified multiple cyber security deficiencies that "could potentially have national security implications." These included: (1) the OPM's decentralized governance structure; (2) a lack of acceptable risk management policies and procedures; (3) failure to maintain a mature vulnerability scanning program to find and track the status of security weaknesses in software systems; (4) a high rate of false

[1] The Government Accountability Office describes a "material weakness" as a deficiency or combination of deficiencies in internal controls such that there is a reasonable possibility that a weakness in an agency's systems security program or management control structure will not "be prevented, or detected and corrected on a timely basis."

security alerts that could delay the identification of and response to actual security breaches; (5) failure to use tools to monitor the progress of corrective efforts for cyber security weaknesses; (6) remote access sessions which did not terminate or lock out after the period of inactivity required by federal law; (7) failure to continuously monitor the security controls of all software systems; (8) failure to maintain and test contingency plans for every information system as required under the OPM's policies; and (10) failure to use Personal Identification Verification ("PIV") Cards[2] for multi-factor authentication in all major software systems. As a result, the OIG concluded that the OPM's software systems were so vulnerable that Archuleta and the OPM should consider largely "shutting [them] down."

7. In December 2014, KeyPoint, the private OPM contractor that handled the majority of federal background checks at the time, announced that it had suffered a computer network breach. At the time, OPM spokeswoman Nathaly Arriola said that there was "no conclusive evidence to confirm sensitive information was removed from the system" but that the OPM would notify 48,439 federal workers that their information may have been exposed. After the OPM Breach became public, however, Archuleta and the OPM identified the misuse of a KeyPoint user credential as the source of the breach. For example, Archuleta told Senator Bonnie Watson Coleman—member of both the House Committees on Homeland Security and Oversight and Government Reform—that "there was a credential that was used and that's the way [the hackers] got in."

[2] PIV cards are government identification cards used to access software systems. Data is stored on the card through an embedded smart card chip. When accessing a software system, the user must insert the card into a card reader and provide a Personal Identification Number (PIN). The PIV card and pin verifies the user's identity and allows access to the software system.

8. KeyPoint President and Chief Executive Officer ("CEO") Eric Hess responded to Archuleta's contention on June 24, 2015 in a prepared testimony before the House Committee on Oversight and Government Reform, stating, "I would like to make clear that we have seen no evidence suggesting KeyPoint was in any way responsible for the OPM Breach." Regarding who is to blame for the OPM Breach, Hess said, "To be clear, the employee was working on OPM's systems, not KeyPoint's." It is unsurprising that both KeyPoint and OPM cite a 'lack of evidence' of culpability because, according to a report by a forensic expert who analyzed the OPM Breach, "KeyPoint had never set up logs. 'In other words, they don't know what happened . . . . It's like if you go into a 7-Eleven and the security camera is not on.'"

9. Despite (1) knowledge of the recent KeyPoint Breach and, (2) being explicitly warned about deficiencies in cyber security protocol and the dangers associated with those deficiencies, the OPM Defendants elected not to shut down the OPM's software systems. On June 4, 2015, the OPM announced that it had been the subject of a massive cyber attack that compromised millions of federal applicants' personally identifiable information ("PII"),[3] records, and sensitive information.

10. The combination of KeyPoint's cyber security weaknesses and the OPM's cyber security failures caused the massive scope of the OPM Breach. According to CNN, "after [the KeyPoint intrusion] last year, OPM officials should have blocked all access from KeyPoint, and that doing so could have prevented more serious damage."

[3] PII is defined by the OPM as information that can be used to discern or trace a person's identity; and alone, or combined with other information, can be used to compromise the integrity of records relating to a person by permitting unauthorized access to or unauthorized disclosure of these records.

11. According to one report, the OPM Breach resulted in "30 years' worth of sensitive, security clearance, background-check, and personal data from at least 10 million current, past, and prospective federal employees and veterans" being compromised.

12. After the OPM announced that it had been hacked, top OPM officials, including Archuleta and Seymour, were criticized by members of the House Oversight and Government Reform Committee as "grossly negligent." U.S. Representative Jason Chaffetz—chairman of the House Oversight and Government Reform Committee—likened the OPM's lax cyber security protocol to "leaving all the doors and windows open in your house and expecting that no one would walk in and nobody would take any information." Congressman Steve Russell similarly criticized the OPM's testimony that, but for fixing problems with its cyber security protocol, "we would never have known about the breach" as tantamount to saying "if we had not watered our flowerbeds, we would have never seen the muddy foot prints on the open windowsill." Congressman Russell concluded that "this is absolute negligence that puts the lives of Americans at risk . . . ."

13. Information about the scope of the OPM Breach continues to emerge. Though initial reports were that only 4 million federal applicants were impacted, on June 11, 2015, U.S. officials announced that up to 14 million federal applicants' PII was compromised. On June 22, 2015, CNN reported that these numbers continue to increase, and that the OPM Breach potentially affects 18 million federal applicants.

14. As a result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer actual damages and pecuniary losses, including costs associated with mitigating the risk of identity theft, such as costs for credit monitoring services and identity theft insurance, and costs associated with freezing and unfreezing their accounts.

15. Defendants' conduct violated the Privacy Act of 1974, the Administrative Procedure Act, and constitutes negligence. Plaintiffs request damages to compensate them for their current and future losses and injunctive relief to fix the OPM's security protocol, implement the OIG's latest audit instructions, to provide adequate credit monitoring services for a sufficient time period, and to provide after-the-fact identity repair services and identity theft insurance to protect Class members from fraud or identity theft.

II. PARTIES

A. Plaintiffs

16. Plaintiff AFGE is a labor organization and is headquartered at 80 F. Street, N.W., Washington, DC 20001. The AFGE represents, on its own and through its affiliated councils and locals, approximately 650,000 federal government civilian employees in departments and agencies across the federal government for a variety of purposes, including for the purpose of collective bargaining. Workers in virtually all functions of the government at numerous federal agencies depend upon AFGE for legal representation, legislative advocacy, technical expertise, and informational services. AFGE exists "For the purpose of promoting unity of action in all matters affecting the mutual interests of government civilian employees in general, all other persons providing their personal service indirectly to the U.S. Government and for the improvement of government service." For over 80 years, AFGE has taken seriously its responsibility to help provide good government services while ensuring that government workers are treated fairly and with dignity. As is described in more detail below, since the OPM disseminated news of the breach, AFGE has actively advocated on behalf of its members, including demanding that employees be granted administrative leave to register for credit monitoring and fraud protection and deal with any

other fallout resulting from the OPM Breach, and seeking lifetime credit monitoring services for all federal employees.

17. AFGE members have been impacted by the OPM Breach. Multiple members have received notifications from the OPM that their PII may have been compromised in the OPM Breach.

18. Plaintiff Robert Crawford is a resident of the State of Indiana. He is currently employed with the Federal Railroad Administration as an Operating Practices Inspector and is an active member of AFGE. Mr. Crawford received notification from the OPM that his PII may have been compromised in the OPM Breach.

19. Plaintiff Adam Dale is a resident of the State of Michigan. He is a former United States Social Security Administration attorney advisor and supervisory attorney advisor. He received notification from the OPM that his PII may have been compromised in the OPM breach. In response to the OPM Breach, he purchased Lifelock comprehensive identity theft protection.

B. Defendants

20. Defendant OPM is a U.S. agency with headquarters at 1900 E. Street, NW, Washington, DC 20415. The OPM handles many aspects of the federal employee recruitment process, including managing federal job announcements, conducting background investigations and security clearances, overseeing federal merit systems, managing personal retirement and health benefits, providing training and development programs, and developing government personnel policies. As part of the recruitment process, the OPM collects and maintains federal applicants' records including PII, background investigations, and security clearance forms. The OPM conducts more than two million background

investigations annually, provides critical human resources services to other agencies, and audits agency personnel practices.

21. Defendant Archuleta is the Director of the OPM and works at the agency headquarters in Washington, D.C. She was sworn in as Director of the OPM in November 2013. She "lead[s] the government's efforts to recruit, retain and honor a world-class workforce through an agency of more than 5,000 employees." She oversees a broad range of policy and administrative issues in the OPM, including oversight of its cyber security policies and practices. Plaintiffs bring this action against Archuleta in her official capacity as Director of the OPM only.

22. Defendant Seymour is the Chief Information Officer ("CIO") for the OPM and works at the agency headquarters in Washington D.C. Archuleta hired Seymour as the CIO in December 2013. She oversees the OPM's software systems and cyber security policies and practices. Plaintiffs bring this action against Seymour in her official capacity as CIO for the OPM only.

23. Defendant KeyPoint describes itself as a "leading provider of investigative and risk mitigation services to government organizations, including the U.S. Office of Personnel Management, Customs and Border Protection and Department of Homeland Security." KeyPoint maintains its corporate headquarters in Loveland, Colorado. In recent prepared testimony before the House Committee on Oversight and Governance Reform, KeyPoint's President and CEO described KeyPoint's work for the OPM as "provid[ing] fieldwork services for background investigations." Hess said KeyPoint "employs investigators in every state [and] is proud to be part of OPM's team, helping to ensure that the security clearance investigations it conducts are thorough, detailed, and consistent." As of December 2014, it

was reported that KeyPoint was the "largest private clearance firm working for federal agencies." KeyPoint's parent company is Veritas Capital, a private equity firm that according to news reports has a long history of "controversial government contracting" including its prior ownership of DynCorp, which "frequently billed the government for work that was never requested." According to one report, KeyPoint became the federal government's largest private provider of background investigations after "Veritas again leveraged its relationship with a former official. Shortly after KeyPoint became a Veritas portfolio company in 2009, Veritas brought on former Secretary of Homeland Security Michael Chertoff to serve on its board of directors."

III. JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiffs bring class claims on behalf of citizens of states different than Defendants' states of citizenship, the amount in controversy exceeds $5 million, and the proposed class includes in excess of 100 members.

25. This Court also has subject matter jurisdiction over the federal claim in this action pursuant to 28 U.S.C. § 1331.

26. This Court also has subject matter jurisdiction over the Privacy Act of 1974 claim pursuant to 5 U.S.C. § 552a(g)(1).

27. This Court has personal jurisdiction over the OPM because it maintains headquarters in the District of Columbia and the relevant conduct occurred in the District of Columbia.

28. This Court has personal jurisdiction over Archuleta because she works as Director in the District of Columbia office and the relevant conduct occurred in the District of Columbia.

29. This Court has personal jurisdiction over Seymour because she works as CIO in the District of Columbia office and the relevant conduct occurred in the District of Columbia.

30. This Court has personal jurisdiction over KeyPoint because it conducts significant business in the District of Columbia and much of the relevant conduct occurred in the District of Columbia.

31. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant OPM is located in the District of Columbia and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in the District of Columbia.

32. Venue is also proper in this district under 5 U.S.C. § 552a(g)(5) and 5 U.S.C. § 703.

IV. FACTUAL ALLEGATIONS

A. The Office of Personnel Management is Responsible for the Collection and Storage of a Substantial Amount of Confidential and Sensitive Personnel Records

33. The OPM is an independent government agency that manages the civil service of the U.S. government. The OPM handles a broad range of federal employee related issues including: (1) managing job announcement postings and setting policies on government-wide hiring procedures; (2) conducting background investigations for prospective employees and security clearances across the government; (3) upholding and defending the merit system in the federal civil service; (4) managing pension benefits for retired federal employees and

their families and administering health and other insurance programs for federal employees and retirees; (5) providing training and development programs and other management tools for federal employees and agencies; and, (6) taking the lead in developing, testing and implementing government-wide policies relating to personnel issues.

34. Since November 2013, Archuleta has served as the Director of the OPM, in which capacity she "lead[s] the government's efforts to recruit, retain and honor a world-class workforce through an agency of more than 5,000 employees." She oversees a broad range of policy and administrative issues in the OPM, including oversight of cyber security policies.

35. The OPM collects and stores large amounts of government-wide human resources data. The OPM manages the electronic Official Personnel Folder ("eOPF"), a software system that provides on-demand Web-based access to personnel folders and 24/7 concurrent access to personnel information by human resources staff and employees. The eOPF file contains employee performance records, employment history, employment benefits, federal job applications (which include social security numbers and address information, among other things), resumes, school transcripts, documentation of military service, and birth certificates.

36. The OPM provides investigative products and services for over 100 federal agencies. Through its Federal Investigative Services division, the OPM manages and oversees a substantial portion of the federal government's employee security clearances, which involves conducting "over two million background investigations yearly with over 650,000 conducted to support initial security clearance determinations . . . more than 90% of the Government total." The background investigation toolset is called EPIC which is an

acronym based on its major components, each of which requires aggregation and storage of a wealth of confidential federal applicant information:

- **E**, for the Electronic Questionnaires for Investigations Processing ("e-QIP") system a "Web-based" automated software system designed to process standard investigative forms used when conducting background investigations. The e-QIP system purports to provide a "secure internet connection to electronically enter, update, and transmit [applicants'] personal investigative data over a secure Internet connection to a requesting agency."
- **P**, for the Personal Investigations Processing Systems ("PIPS"), a background investigation case management software system that handles individual investigation requests from agencies. PIPS contains the Security/Suitability Investigations Index (SII), a master record of background investigations conducted on government employees.
- **I**, for Imaging—which allows users to view digitalized paper case files such as surveys, questionnaires, written reports, and other images stored in the software system.
- **C**, for the Central Verification System ("CVS"), the "mother lode" of background investigation data. CVS contains "information on security clearances, investigations, suitability, fitness determinations Homeland Security Presidential Directive 12 (HSPD-12) decisions,[4] Personal Identification Verification ("PIV") Cards,[5] and

[4] HSPD-12 decisions are the background checks required for employees and government contractors to gain access to federal facilities.

[5] PIV cards are government ID smart cards used for access to government facilities and software systems.

polygraph data."

37. Some aspects of EPIC contain information that is so sensitive it is housed at Fort Meade—the home of Defense Information Systems Agency and National Security Agency ("NSA"). Contractors who conduct security investigations for EPIC require top secret clearances.

38. CVS additionally contains SF-86, a 127-page form that each federal applicant who is being considered for security clearance must submit. According to Krebs on Security, an online source for security news, SF-86 contains "huge treasure troves of personal data," including "[security] applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and coworkers. Employees log in using their Social Security numbers."

39. Leading up to the April 2015 OPM Breach, the OPM received 10 million confirmed intrusion attempts targeting its network in an average month. As a result, the OPM was on notice of the fact that it was heavily targeted by hackers prior to the OPM Breach, a fact that is confirmed by its website, which states, "[s]ecurity is of major concern whenever you're dealing with personal information. The Federal government implemented Federal guidelines to safeguard [PII]."

B. The OPM's Weak Cyber Security Measures

40. The Federal Information Security Management Act ("FISMA")[6] governs software system requirements for software systems owned or operated by federal agencies

[6] At the time the OPM audits were conducted, the Federal Information Security Management Act of 2002 governed the auditing process. 44 U.S.C. § 3541 *et seq.* The OIG submitted the most recent audit report in November 2014. The President signed the Federal Information Security

and contractors. As director of the OPM, under FISMA, Archuleta was under a mandate to "develop and oversee[] the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40."

41. Under FISMA, an agency must develop, implement, and maintain a security program that assesses the risks and provides adequate security for the operations and assets of programs and software systems under its control. Specifically, FISMA requires (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the Office of Management and Budget ("OMB") the results of Inspector General evaluations for unclassified software systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. The OMB uses the reports to help it ensure that the various federal agencies are in compliance with its cyber security requirements.

42. In accordance with FISMA, the OIG conducts annual, independent audits of the OPM's cyber security program and practices. The Department of Homeland Security ("DHS") Office of Cybersecurity and Communications issues Inspector General FISMA Reporting Instructions. Using these guidelines, the OIG reviews the OPM's FISMA compliance strategy and documents the status of its compliance efforts.

43. Pursuant to FISMA, the OIG is required to review the status of the following measures the OPM was supposed to have implemented in its cyber security program: (1) Security Assessment and Authorization (the process of certifying a software system's

---

Modernization Act of 2014 into law on December 18, 2014. The Federal Information Security Modernization Act updates and supersedes the Federal Information Security Management Act. For purposes of this Complaint, "FISMA" means the Federal Information Security Management Act of 2002 and "Modernization Act" means the Federal Information Security Modernization Act of 2014.

security controls and authorizing the system for use); (2) Risk Management (risk management policies and procedures); (3) Configuration Management (controls in place to manage the technical configurations of the OPM's servers, databases, and workstations); (4) Incident Response and Reporting Programs (the procedures and requirements for reporting security incidents); (5) Security Training Program (whether employees are trained in cyber security awareness pursuant to FISMA); (6) Plans of Action and Milestones ("POA&M") Program (the use of POA&M, a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for cyber security weaknesses); (7) Remote Access Program (the policies and procedures related to authorization, monitoring, and controlling all methods of accessing the agency's network from a remote location); (8) Identity and Access Management (the policies and procedures for creating and removing user accounts, and managing user account security); (9) Continuous Monitoring Program (the efforts to continuously monitor the security state of its software systems); (10) Contingency Planning Program (the contingency plan for potential cyber security complications); (11) Contractor Systems (the method used to maintain oversight of contractor systems); and (12) Security Capital Planning (the planning process to determine resources required to protect software systems).

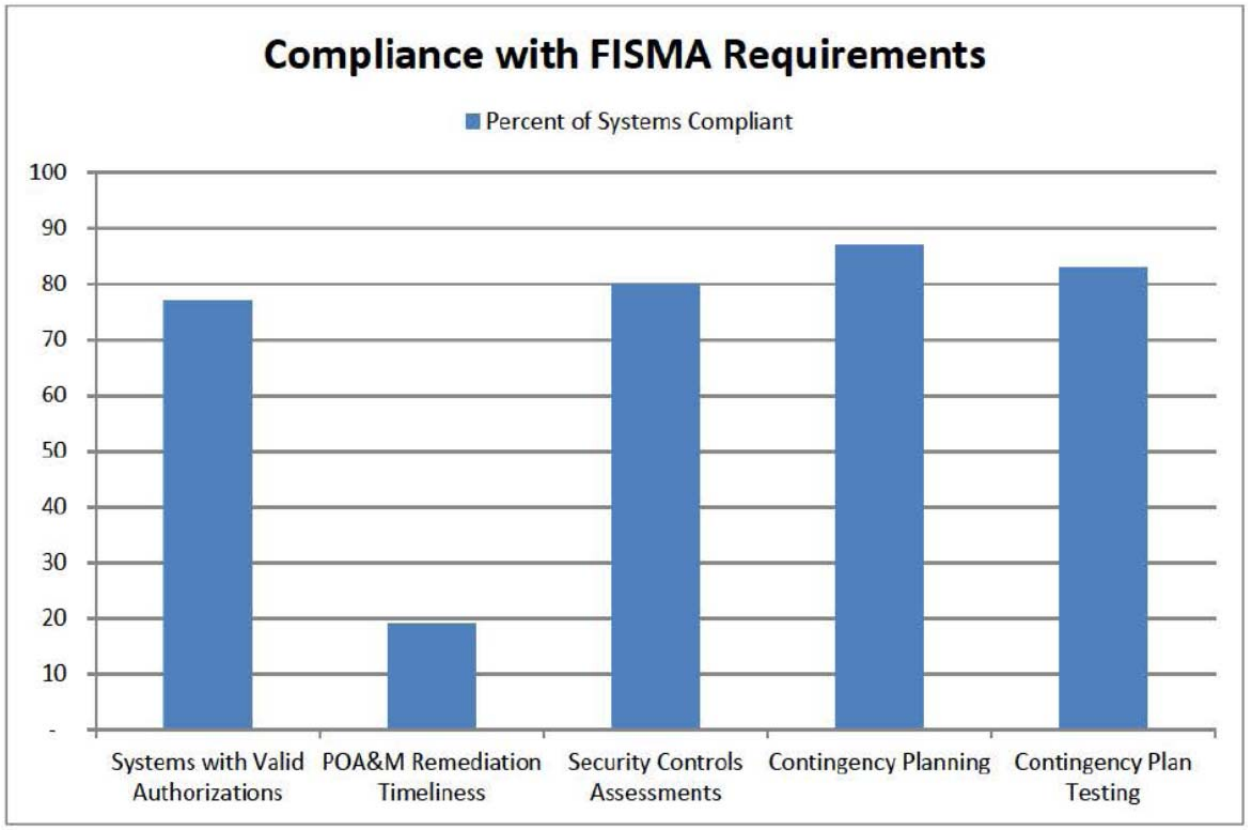
44. In addition to FISMA requirements, the OIG reviews the status of the OPM's Security Governance Structure—the overall framework and management structure that is the foundation of a successful cyber security program. The OIG added this category after repeatedly recognizing problems in the OPM's governance structure over the cyber security process. The Security Governance Structure was designed to protect against decentralized cyber security governance, where various departments are responsible for testing their own

security. Without one team to oversee and coordinate security efforts, there is no uniformity and the OPM cannot ensure that appropriate cyber security measures are in place.

45. In the OIG's most recent 2014 audit, it concluded that the OPM lacked a centralized cyber security team responsible for overseeing all of the OPM's cyber security efforts, creating many instances of non-compliance with FISMA requirements. Designated Security Officers (DSO)—officers who review software systems for cyber security weaknesses and make sure cyber security measures are in place—managed the OPM's cyber security, and reported to various program offices that used software systems. The DSOs are not certified cyber security professionals, however, and perform security duties in addition to their normal, full time job responsibilities.

46. The OPM has had a decentralized cyber security governance structure since at least 2009. In 2012, the OPM attempted to centralize the DSO program by notifying its departments that cyber security responsibilities would be overseen by the Office of the Chief Information Officer ("OCIO"). However, by 2014, the OPM only partially implemented the centralization. Although the OPM designated four centralized officers to oversee DSO's work, the OIG recognized many software systems that were not centralized.

47. As of 2014, because of the OPM's lack of a centralized cyber security governance structure, as demonstrated by the following graph, a large portion of the OPM's software systems were not in compliance with FISMA requirements.



48. Specifically, in its 2014 audit report, which covered the cyber security protocol the OPM had in place as of November 2014, the OIG noted compliance problems in a number of areas.

- The OPM lacked acceptable risk management policies and procedures, and specifically failed to assess risk, maintain a risk registry, or communicate agency-wide risks to its departments.
- The OPM failed to have appropriate configuration controls in place, specifically lacking a "mature vulnerability scanning program" to find and track the status of security weaknesses in its software systems.
- The OPM's automated security alert system reported a high rate of false security alerts that could delay the identification and response to actual security breaches.

- The OPM failed to effectively use POA&M. Accordingly, the OPM could not effectively identify and monitor the progress of the corrective efforts and ensure that those weaknesses were fixed.
- The OIG found that where employees accessed the OPM's system from a remote location, the remote access sessions did not terminate or lock out after the period of inactivity required by FISMA.
- The OPM failed to continuously monitor the security controls of all of its software systems, finding that only 37 of 47 software systems were adequately tested for security issues in 2014, and that it had been "over eight years since all [software] systems were subject to an adequate security controls test." The OIG noted that a "failure to continuously monitor and assess security controls increases the risk that agency officials are unable to make informed judgments to mitigate risks to an acceptable level."
- The OPM failed to maintain and test contingency plans for every software system as required under the OPM's policies. The OPM only maintained contingency plans for 41 of 47 software systems, and only tested 39 of 47 software systems.

49. In addition, the OIG found that the OPM was not in compliance with the OMB's requirements,[7] which mandate the use of PIV Cards for multi-factor authentication in all major software systems.

[7] The February 3, 2011 OMB Memorandum M-11-11 incorporates the DHS PIV card standards requiring: "all new systems [] be enabled to use PIV cards . . . prior to being made operational;" "[e]ffective the beginning of FY2012, existing physical and logical access control systems [] be upgraded to use PIV credentials;" and "Agency processes [] accept and electronically verify PIV credentials issued by other federal agencies."

50. Multi-factor authentication requires more than one form of independent credentials to verify the user's identity to access software systems, thus increasing the barriers to cyber attack. An example of multi-factor authentication would be the combination of a password (something known to the user) and the PIV card (something possessed by the user). The OIG found that none of the OPM's major applications required PIV authentication in the identification process.

51. PIV cards contain computerized chips which build in an extra layer of security to ensure that only authorized users have access to secure software systems.

52. Also in its November 2014 audit report, the OIG found that a critical flaw was the OPM's Security Assessment and Authorization—its process of certifying a software system's security controls. Under FISMA, major software systems are required to be reassessed and reauthorized every three years, or in the alternative, continuously monitored. The OMB requires all federal software systems to have a valid authorization—a DSO must do a comprehensive check on the cyber security of a software system to make sure that it meets all security requirements, and approve the software system for operation—and prohibits the operation of software systems without authorization. Despite these OMB

requirements, the OIG found that only 10 of 21 software systems due for authorization were completed on time. The rest were currently operating without valid authorization, meaning that those software systems had not been checked to determine whether they were vulnerable to a data breach. The OIG noted that the "drastic increase in the number of [software] systems operating without valid authorization is alarming and represents a systemic issue of inadequate planning by [the] OPM [] to authorize the [software] systems they own." The 11 software systems that were not in compliance were located in various departments including the Offices of the Chief Information Officer; Federal Investigative Services; Human Resources Solutions; Office of the Inspector General; and, Office of the Chief Financial Officer.

53. The OIG noted that several of the unauthorized software systems were "amongst the most critical and sensitive applications owned by the agency." It warned that over 65 percent of all software systems operated by the OPM reside in two of the major support systems lacking authorization, and therefore are subject to any security risks that exist on the support systems. According to the OIG audit, two additional software systems without authorization were "owned by Federal Investigative Services, which is responsible for facilitating background investigations for suitability and security clearance determinations." The OIG stated that "[a]ny weaknesses in the [software] systems supporting this program office could potentially have national security implications."

54. The OIG also found that the OPM was not in compliance with several standards promulgated under 40 U.S.C. § 11331, as is required by FISMA, including in the areas of risk management, configuration management, incident response and reporting,

continuous monitoring management, contractor systems, security capital planning, and contingency planning.

55. Because of the significant flaws in the OPM's cyber security systems, the OIG instructed that the "OPM Director consider shutting down [software] systems that do not have a current and valid authorization." In the audit report, however, the OIG noted that the OPM refused, instead stating that it would "work with [information system security officers] to ensure that OPM systems maintain current [authorizations] and that there are no interruptions to the OPM's missions and operations."

C. Key Vulnerabilities in the OPM's Cyber Security Protocol

56. Michael Esser, the assistant inspector general at the OIG, is responsible for auditing the security systems at the OPM. In recent prepared testimony before the House Committee on Oversight & Government Reform, Esser summarized the annual OIG audit reports, stating that the "OPM has a history of struggling to comply with FISMA requirements," and "[a]lthough some areas have improved, such as the centralization of [cyber] security responsibility within the Office of the CIO, other problems persist." Esser highlighted three significant issues identified in the 2014 Audit.

57. **Decentralized Cyber Security Governance.** Esser stated that for several years the OPM had been unclear which cyber security responsibilities fall on the central office, and which are left to individual departments within the OPM. In addition, he noted that some cyber security responsibilities that were left to individual departments ended up being implemented by unqualified officials: "[t]he program office personnel responsible for cyber security frequently had no cyber security background and were performing this function in addition to another full-time role." He stated that, "as a result of this

decentralized governance structure, many security controls went unimplemented and/or remained untested, and the OPM routinely failed a variety of FISMA metrics year after year."

58. **Systems Authorization.** Esser stated that the OPM has a long history of issues related to software system authorization. In 2010, the OIG recognized that the OPM suffered from poor management over the authorization process, OPM divisions often failed to complete authorization on software systems, and OPM failed to establish standardized authorization requirements to ensure that its divisions were not authorizing software systems with significant cyber security risks. The authorization problem initially improved but resurfaced in 2014. Esser stated that only 10 of 21 software systems due for authorization were completed on time. More than half of the software systems were operating without a valid authorization. He stated that it was a "drastic increase from prior years, and represents a systemic issue of inadequate planning by the OPM program offices to assess and authorize the [software] systems that they own. He went on to confirm that "[i]t already appears that there will be a greater number of [software] systems this year operating without a valid authorization," due to the OPM "temporarily put[ting] Authorization efforts on hold while it modernizes the OPM's IT infrastructure in response to security breaches." And he noted that "[a]uthorization should continue, as the modernization is likely to be a long-term effort." Esser also confirmed that in his 2014 report to the OPM, he instructed it to shut down some of its networks because they were vulnerable, but Archuleta declined, saying it would interfere with the agency's mission.

59. **Policies, Procedures & Technical Controls.** Esser said that two of the most critical areas in which the OPM needs to improve its technical security controls "relate to

policies, procedures, and technical controls used to ensure that PIV credentials are securely deployed." He noted that the OPM has "implemented a variety of new controls and tools designed to strengthen the agency's technical infrastructure," but failed to utilize the tools to their fullest potential. He also stated that the OPM does not maintain an accurate centralized inventory of all servers and databases in its network, and that "without a comprehensive list of assets that need to be protected and monitored" the OPM cannot fully defend its network. He confirmed that the OPM failed to use PIV authentication for all 47 of the agency's major applications, adding that "[f]ull implementation of PIV authentication would go a long way in protecting an agency from security breaches, as a [hacker] would need to compromise more than a username and password to gain unauthorized access to a [software] system."

D. The OPM has Repeatedly Failed to Comply with FISMA's Cyber Security Requirements

60. The OIG's 2014 audit report followed years of recognized deficiencies in the OPM's cyber security. Since 2007, the OIG has "reported material weaknesses in controls over the development and maintenance of the OPM's cyber security policies and procedures." For every year from 2009 to 2014, the OIG identified material weaknesses.

61. In 2009, the OIG first recognized a material weakness in the OPM's "overall [cyber] security governance program," noting that the OPM failed to fill key cyber security leadership positions. The absence of leadership meant that the OPM did not have the necessary oversight to correct system-wide cyber security issues. In addition, the OIG found that the OPM lacked evidence that all laptops issued to OPM employees had encryption capability, so laptops with sensitive PII may have been particularly vulnerable to hackers.

62. In 2010, the OIG again found a "material weakness" in the OPM's cyber security governance, meaning that the OPM's employees did not have guidance on how to

prevent software systems from being hacked. In addition, the OIG added Security Assessment and Authorization[8] as a material weakness finding that the quality of the authorization process had worsened from the previous two years. The OIG noted that the OPM lacked the staff to ensure that all software systems had cyber security measures necessary to fend off cyber-hacks.

63. In 2011, the OIG again labeled the OPM's cyber security governance a "material weakness," noting that the OPM continued to lack staff in key cyber security leadership positions, and that the DSO's did not have the technical skill to effectively determine whether a software system was vulnerable to an attack. In addition, the OIG recognized that the authorization process remained inconsistent between different departments, meaning that while some departments were determining which software systems met security standards, other departments were unable to recognize if a software system was vulnerable to attack.

64. In 2012, the OIG continued to recognize a "material weakness" in the OPM's cyber security governance, finding that though the OPM had hired a Chief Information Security Officer ("CISO")—a key leadership position in its cyber security team—the OPM did not give the CISO any authority to oversee the DSOs. This meant the new position failed to centralize the OPM's security personnel and provide an oversight structure to ensure that software systems were secure. The OIG also found that there were "numerous [cyber] security incidents [] that led to the loss or unauthorized release of mission-critical or sensitive data." For example, the Heritage Foundation reported that in May 2012, an unknown hacker broke into the OPM and posted thirty-seven user IDs and passwords online.

[8] In 2010, the OIG labeled this process Certification and Accreditation.

The OIG also found that when employees accessed software systems using a remote access session—where the employee can use a computer to log into the software system from a remote location such as a laptop in a public place—the remote access would not terminate if the user failed to log off. If an employee failed to sign off, other parties could access the system from the same computer without having to enter log-in credentials.

65. In 2013, despite years of documented problems regarding cyber security governance at the OPM, the OIG concluded that "[l]ittle progress was made" to address the lack of "a centralized security management structure," and therefore expressed its doubt as to the OPM's ability to manage major software systems." The OIG also found that the OPM failed to require PIV authentication for any of the 47 major applications, meaning that if a hacker obtained an employee's password, the hacker could access the system without requiring the extra protection afforded by the PIV card.

66. According to technology news source Ars Technica—quoting Vinny Troia, the director of risk and security consulting at McGladrey, LLP—the OPM's recidivism was intentional and a direct result of the fact that "[t]here was no consequence for systems breaking the law."

> The OPM Inspector General report specifically cited the lack of any consequences for not complying with FISMA as a contributing cause to delays in getting the systems up to specifications. And the reason there were no consequences was because the persons responsible for deciding what consequences would be for breaking the law were Archuleta and Seymour.

67. In its 2014 audit report, the OIG similarly found that the OPM's non-compliance with FISMA was intentional and that one of the "core causes" was the "fact that there are currently no consequences for OPM systems that do not have a valid Authorization to operate." As a result, in 2014, the OIG recommended introducing administrative

sanctions to combat instances of willful non-compliance with FISMA requirements. The OIG further recommended "that the performance standards of all OPM major system owners be modified to include a requirement related to FISMA compliance for the systems they own."

E. The OPM's History of Software System Hacks

68. The OPM Breach is not the first attempted data breach involving the OPM in recent years. In July 2014, the New York Times publicized an attempted OPM intrusion that the agency had been investigating since March 2014. Hackers reportedly operating from mainland China broke into the OPM's computer networks, and targeted files of thousands of employees applying for security clearances. The hackers gained access to some of the databases before the federal authorities detected the threat and blocked them from the network. Shortly after the article was published, the OPM sent an email to its employees assuring that it had not identified any loss of PII.

69. In August 2014, media sources revealed that US Investigations Services LLC ("USIS"), a contractor that provided the bulk of background checks for federal security clearances—including for the OPM—had been hacked, potentially exposing thousands of government employee records. In a public statement, the company said the "attack has all the markings of a state-sponsored attack." After the breach, the OPM terminated contracts with USIS. Former Undersecretary for Management of Homeland Security Chris Cummiskey stated that the OPM's response to the hack lacked coordination and, "[w]e've seen this a couple of times now and unfortunately we act like each iteration is the first time it's ever occurred." In testimony before the House of Oversight and Government Reform Committee regarding the 2014 USIS breach, Seymour acknowledged both USIS and the

OPM were attacked by hackers in March 2014, but were able to "put mitigations in place to better protect the situation."

F. The KeyPoint Hack

70. In December 2014, the OPM alerted more than 48,000 federal employees that their personal information may have been exposed following a data breach at KeyPoint (the "KeyPoint Hack"). Nathaly Arriola, the OPM's spokesperson, stated that there was "no conclusive evidence to confirm sensitive information was removed from the [software] system."

71. KeyPoint became the largest government contractor performing private employee clearances after its predecessor, USIS, was terminated after the cyber-attack it experienced in 2014. According to reports, "KeyPoint moved quickly to fill the void, looking to double the size of its investigative workforce." However, because USIS's caseload was significant and involved 21,000 background checks a month, there was skepticism that any entity could cover the workload on "short notice." According to a former USIS senior investigator, "[t]hat amount of work requires significant managerial oversight, which is usually developed over time." After KeyPoint announced that it had assumed USIS's former workload, the same former USIS investigator said a question that concerned her was "Can [KeyPoint] even handle the influx of these new employees and all the work that gets dumped on them by OPM?"

72. In the wake of the KeyPoint Hack, and in view of the OPM Breach, it has become apparent that KeyPoint and the OPM could not handle the workload and protect Plaintiffs and Class members' PII and other confidential information in an adequate and secure manner. Even today, KeyPoint has been unable to identify how the breach it

announced in December 2014 happened. The reason it can't—according to Ann Barron-DiCamillo (director of the DHS U.S. Computer Emergency Readiness team)—is due to "lack of logging." In other words, according to one report, KeyPoint never set up logs to track the malware deployed to infiltrate its systems and therefore "doesn't know what happened . . . . It's like if you go into a 7-Eleven and the security camera is not on."

73. Following the KeyPoint hack, the DHS and other agencies began helping the OPM with its network monitoring. According to DHS spokesman S.Y. Lee, DHS and "interagency partners" were helping the OPM improve its network monitoring "through which [the] OPM detected new malicious activity affecting its [software] systems and data in April 2015." The DHS and "interagency partners" used a security monitoring program to discover a potential breach. According to Lee, "DHS concluded at the beginning of May 2015 that [the] OPM data had been compromised." DHS determined that the event wasn't just historical, but an ongoing breach of the OPM's software systems and data center.

74. After announcement of the KeyPoint Hack, Seymour—in an e-mail to colleagues at the OPM—praised the OPM's commitment to cyber-security measures, stating: "security of our networks and the data entrusted to us remains our top priority. This incident serves as yet another reminder that we all must be ever-vigilant in our efforts to understand, anticipate and guard against the threat of cyber-attacks." During this same time period, however, the OPM was not in compliance with the FISMA or the OIG's recommendations and had not been for years. And despite the KeyPoint hack, the OPM continues to this day to use KeyPoint as its security clearance contractor.

G. The OPM Breach

75. On June 4, 2015, the OPM announced it would notify approximately 4 million

current and former federal applicants and employees in the executive branch that its software system had been hacked and employees' PII had been stolen. Though it only made the OPM Breach public on June 4, 2015 the OPM admits that it detected the intrusion as early as April. The OPM offered credit report access, 18 months of credit monitoring and identity theft insurance and recovery services to affected current and former federal employees. In addition, the OPM issued guidance to individuals to monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.

76. In order to access the OPM's database, hackers installed a malware package that industry analysts opine was likely delivered via an e-mail "phishing"[9] attack within the OPM's software systems through which the hackers gained access to valid OPM user credentials. U.S. investigators believe that the hackers registered the website—OPM-Learning.org—to try and capture employee names and passwords. Because of the lack of multifactor authentication on these software systems, the hackers were able to use the stolen credentials at will to access software systems from within and potentially even from outside the network. By using credentials to get into the software system, hackers could sneak data out of the network over the Internet, hiding its activity internally among normal traffic. It was only when the OPM was assessing its software systems to actually implement continuous monitoring tools, as required by FISMA, that it discovered that something was wrong.

77. The two systems breached were the eOPF system, and the central database behind "EPIC"—the software used by Federal Investigative Services in order to collect data

[9] "Phishing" is an attempt to obtain confidential information from internet users, typically by sending an email that looks as if it is from a legitimate organization but contains a link to a fake website that replicates the real one.

for government employee and contractor background investigations.

H. Public Consensus—OPM is to Blame

78. Over the past few weeks, the OPM has borne the brunt of public criticism for its failure to implement sufficient security practices which enabled the OPM Breach. In a statement to Politico, Seymour stated that the databases penetrated by hackers didn't use industry best practices such as encryption or other technology to protect federal employee's social security numbers. She said that encryption and data obfuscating techniques "are new capabilities that we're building into our databases."

79. Matt Little, VP of Product Development at PKWare, an encryption software company said, "[i]t [is] ridiculous . . . [t]his is not something we typically see in a serious security customer."

80. At the Committee Hearing, Chairman Jason Chaffetz, U.S. Representative for Utah's 3rd congressional district told Archuleta, "you failed. You failed utterly and totally." Chaffetz stated that the breach should "Come as no surprise given [the OPM's] troubled track record." Chaffetz compared the breach to "leaving all the doors and windows open in your house and expecting that nobody" would come in take anything.

81. House Representative Ted Lieu called for Archuleta to resign, stating that "[i]n national security it's got to be zero tolerance, that's got to be the attitude. We can't have these breaches." He added, "[i]n the past when we've had this, leadership resigns or they're fired . . . Send a signal that the status quo is not acceptable. We cannot continue to have this attitude where we make excuse after excuse."

82. House Representative Steve Russell stated that the OPM's failure to encrypt data was "absolute negligence that puts the lives of Americans and also foreign nationals at risk."

I. Information About the Scope of the OPM Breach Continues to Emerge

83. Following the OPM's June 4 disclosure, the magnitude of the breach has become increasingly apparent. The breach, which CNN dubbed "the biggest government hack ever," resulted in leaked background and security clearance investigations on employees, their families, neighbors, and close associates stored in e-QIP and other software systems. In the initial disclosure, the OPM stated that the breach only exposed 4 million former and current employees' PII. But on June 12, 2015, the OPM announced that the scope of the breach was much larger. More sensitive data including SF-86 forms had likely been compromised, potentially involving 14 million current, former, and prospective employees, more than triple the 4 million originally cited by the OPM. In a statement prepared by Archuleta before the House of Oversight and Government Reform Committee, she stated that they were aware that the SF-86 forms had been compromised in May. Despite knowing the scope of the breach, the OPM failed to disclose this information in the June 4, 2015 statement to the public.

84. The scope of the OPM Breach continues to expand. For example, on June 22, 2015, CNN reported that the number of those affected by the OPM Breach continues to grow, and said that 18 million federal applicants potentially had their PII stolen. Federal Bureau of Investigation ("FBI") Director James Comey gave the 18 million person estimate in a closed-door briefing to Senators, and included among those impacted by the OPM

Breach people who applied for government jobs, but never ended up working for the government.

85. On June 24, 2015, online news source The Daily Beast reported that "adjudication information" was compromised. Adjudication information contains detailed and highly confidential personal data that U.S. investigators gather on government employees and contractors who apply for positions requiring heightened security clearance, including positions as intelligence agents. Adjudication information is highly sensitive, and includes data like the results of polygraph examinations and intimate personal details. According to technology security expert Michael Adams, who served for over twenty years in the U.S. Special Operations Command: "Whoever compromised the adjudicated information is going to have clear knowledge, beyond what's in the SF86, about who the best targets for espionage are in the United States."

86. A report by the OIG filed in November 2014 confirms that relatively little is known about the amount of data stolen in the breach. In the report, the OIG stated that the "OPM does not maintain a comprehensive inventory of servers, databases, and network devices." Without a comprehensive list of the software systems it owns, OPM simply cannot verify whether it has accounted for all software systems that may have been breached. As was the case with the KeyPoint Hack, a key reason why the scope of the OPM Breach is difficult to ascertain and continues to develop is a lack of adequate logging by the OPM. According to recent reports "OPM apparently lacked logs too. The most recent event began in June 2014 and was not identified until April. The federal government still does not know the extent of the intrusion as of June 24, 2015." Seymour recently admitted as much, stating, "[w]e had put the tools on our network just over the last six months or so to be able to see

this type of activity on our network" enabling officials to go back in time and track "this latent activity that went back to even prior to my arrival at OPM."

87. In the OPM Breach, the hackers stole eOPF files that contain employee performance records, employment history, employment benefits information, federal job applications, resumes, school transcripts, documentation of military service, and birth certificates. The compromised federal job applications include social security numbers, mailing addresses, birthplaces, and other names used. According to one recent report, "foreign hackers compromised the intimate personal details of an untold number of government workers. Likely included in the hackers' haul: information about workers' sexual partners, drug and alcohol abuse, debts, gambling compulsions, marital troubles, and any criminal activity." In questioning Archuleta, Senator Benjamin Sasse similarly observed "[a]s those of us who've been through top secret background checks know, they ask lots of questions about sexual history, relationships, associations, anything that could lead an individual to be coerced or blackmailed." He asked "[c]an you help us understand why this information would have been stored on OPM's networks to begin with?" Archuleta responded that OPM is still trying to "understand how that data was saved" and admitted "I actually don't know what is stored in which files."

88. Colleen M. Kelley, President of National Treasury Employees Union, the nation's second biggest federal employee collective bargaining Union, stated that she was "very concerned" about the breach because "[d]ata security, particularly in an area of identity theft, is a critically important matter." According to CBS, millions of federal employees could be the "subject of identity theft—from intelligence and law enforcement agents to federal parks workers."

89. In an article by the Washington Post, Ed Mierzwinski, Federal Consumer Program Director, stated that the information in federal job applications can be used for identity theft to set up fraudulent lines of credit. Mierzwinski recommended that federal applicants tell credit monitoring agencies to stop any new lines of credit from being opened in their name. To do that, a federal applicant would be required to contact all three of the major credit monitoring agencies and pay a fee—between $10 and $15 per agency to freeze and unfreeze each time they want to open a line of credit. Mierzwinski stated that monitoring services, like the one OPM is providing, create a false sense of security, and an 18 month window of protection would not be enough to protect federal applicants from harm down the line, and if data is sold off, it could take a long time before it's used.

90. In testimony before the Subcommittee on Information Policy, Census and National Archives Committee on Oversight and Government Reform: Identity Theft, Daniel Bertoni, Director of the United States Government Accountability Office ("GAO") stated that, "[m]any victims of identity theft face substantial costs and inconvenience repairing damage to their credit records . . . and some have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft." Bertoni stated that, "in [one] year, as many as 10 million people – or 4.6 percent of the U.S. adult population—discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion."

91. Already, hackers are taking advantage of the OPM's breach. Following the breach, the OPM emailed employees whose information was compromised and offered credit monitoring services through a link in the email. These emails were quickly duplicated by hackers, and used to send "phishing" emails attempting to trick employees into handing over

account logins and other personal information, much in the same way that the hackers obtained information in the original OPM Breach. Both the authentic and duplicated emails told employees to click on a link to register for credit monitoring services. According to the Washington Post, computer experts have noted that the OPM could be "putting federal [software] systems in jeopardy again by asking employees to click on links in the emails," because "[t]here's a risk that you desensitize people by telling them that occasionally there's going to be a very important email you have to click on."

92. Some officials opine that the perpetrators of the OPM Breach carried out the secondary phishing attack. According to one report, "the original OPM hackers obtained a copy of the real CSID announcement e-mail and modified it for their own criminal purposes. It was because of this actual attack, and the e-mail notification's poor design, that on June 15, the [Department of Defense] announced" suspension of further notification to Department of Defense personnel "until an improved, more secure notification and response process is in place." The same report of the secondary phishing attack notes "[i]t's little short of appalling that for a week the OPM sent out emails telling recipients to click on an embedded link to register for their credit monitoring services. This opened the door wide for phishing attacks."

93. The records stolen in the OPM Breach also have national security implications. The hackers accessed EPIC, a background investigation toolset, and stole SF-86 forms all service members and civilians seeking security clearance are required to fill out. The SF-86 forms require federal applicants to disclose personal information about details on alcohol and drug use, mental illness, credit ratings, bankruptcies, arrest records, and court actions. The SF-86 "gives you any kind of information that might be a threat to [the employees'] security

clearance," said Jeff Neal, a former DHS official and a senior vice president at ICF International. "It's really a personal document."

94. Log-in credentials stolen in the OPM Breach are reportedly already being offered for sale on the internet. Chris Roberts, a security expert and founder of Oneworldlabs, a search engine that checks the internet for data that could compromise clients' security, uncovered 9,500 government log-in credentials that were stolen this week from a number of government offices across the U.S. According to Roberts, "[t]he recent OPM breach was identified, noted and the credentials and identities have been discovered online and are being traded actively."

J. The OPM's Evolving Public Reaction to the Breach

95. The OPM and Archuleta have not disclosed in a timely or adequate manner the facts surrounding how the breach happened, why it happened, who was affected, and what was stolen.

96. The OPM reported that it discovered the breach on its own in April 2015, but did not disclose the breach for months, despite the sensitive nature of the information the hackers obtained. The Wall Street Journal reported that the breach was actually discovered during a sales demonstration by a security company named CyTech Services, during a CyTech demonstration of its forensic product. Ben Cotton, CEO of CyTech Services, stated that using CyTech's product, his company "quickly identified a set of unknown processes," which "was ultimately revealed to be malware." Cotton stated that CyTech "remained on site to assist with the breach response, provided immediate assistance and performed incident response services supporting [the] OPM until May 1, 2015."

97. OPM press secretary Samuel Schumach disputed CyTech's involvement in the detection, stating that "[t]he assertion that CyTech was somehow responsible for the discovery of the intrusion into [the] OPM's network during a product demonstration is inaccurate," and the "OPM's cybersecurity team made this discovery in April 2015 as previously disclosed and immediately notified [the U.S. Computer Emergency Readiness Team] and the FBI to investigate the intrusion." Schumach stated "[i]f not for the fact that [the] OPM was already in the process of updating and strengthening our IT infrastructure, we would have not known about the intrusion, and would have not been able to mitigate any damage."

98. During testimony before the House of Oversight and Government Reform Committee, Archuleta deferred answering nearly every substantive question about the breach, including which software systems were affected, how many individuals' data was exposed, and what type of data was accessed. When asked directly how many people had been affected by the breach and whether it included both federal employee and contractor information, Archuleta replied "I would be glad to discuss that in a classified setting."

99. Representative Stephen Lynch stated, "[t]his is one of those hearings where I think I am going to know less coming out of this hearing than I did when I walked in, because of the obfuscation and dancing around that we're all doing here." He told Archuleta, "I wish that you were as strenuous and hard-working at keeping information out of the hands of hackers as you are keeping information out of the hands of Congress and federal employees."

100. Despite the OPM's "history of struggling to comply with FISMA requirements" and failure to take recent steps to secure its software systems, the OPM

continues to insist it did nothing wrong. Archuleta stated that "if anyone is to blame, it is the perpetrators." Archuleta claimed that she had huge problems with the agency's computer security when she assumed her post 18 months ago. She claimed that the OPM's cybersecurity posture was a work in progress, and stated that "[b]ut for the fact that [the] OPM implemented new, more stringent security tools in its environment, we would have never known that malicious activity had previously existed on the network and would not have been able to share that information for the protection of the rest of the federal government."

101. When pressed on why software systems had not been protected with encryption, Archuleta said, "It is not feasible to implement on networks that are too old." However, according to Ars Technica, there are numerous software libraries that can be used to integrate encryption schemes into older applications. The OPM's problems were more fundamental than mere failure to implement encryption however. DHS Assistant Secretary for Cybersecurity Andy Ozment stated that the problem was that the "OPM didn't have the authentication infrastructure in place for its major applications to take advantage of encryption in the first place," and therefore, encryption would "not have helped in this case."

102. When asked why Archuleta did not shut down software systems despite the OIG Audit's instruction, Archuleta said "[i]t was my decision that we would not [close down the software systems] but continue to develop the [software systems] and ensure we have security on those [software] systems." According to Ars Technica, the truth is that "Archuleta did not shut down EPIC and other systems that were out of compliance with the law [because] EPIC is essential to OPM's whole background investigation system, and shutting it down would have caused epic delays in processing new requests for security

clearances and determinations of whether contractors and potential federal employers met 'suitability' standards for access to federal facilities."

103. Most recently, the OPM has sought to shift blame for the OPM Breach to KeyPoint. Archuleta told lawmakers "[t]here was a credential that was used and that's the way they got in." She later attempted to back off her statements but still laid blame for the OPM Breach on KeyPoint: "[w]hile the adversary leveraged a compromised KeyPoint user credential to gain access to [the] OPM network, we don't have any evidence that would suggest that KeyPoint as a company was responsible or directly involved in the intrusion . . . . We have not identified a pattern or material deficiency that resulted in the compromise of the credentials." Reacting to these and other comments by Archuleta, U.S. Representative Mark DeSaulnier told Archuleta, "You appear to come across as petulant, defensive, and evasive" and "[s]ometimes you can feel passionate about things but not be capable of doing what you desire to do."

104. KeyPoint President and CEO Eric Hess responded to Archuleta's claims by denying all culpability: "I would like to make clear that we have seen no evidence suggesting KeyPoint was in any way responsible for the OPM breach." He then shifted blame back to the OPM: "[t]o be clear, the employee was working on OPM's systems, not KeyPoint's."

105. According to the Air Force Times, KeyPoint and Archuleta's comments amount to a statement that "no one person was responsible." But the OPM's long history of failed cyber security measures and the KeyPoint Hack—attributable at least in part to its haste to take on a substantial workload for which it was unprepared—suggest the OPM Breach could have been avoided. And it was Archuleta's decision not to shut down many of

the OPM's software systems in late 2014—in contravention of the OIG's instructions—that led directly to the OPM Breach.

106. The OPM continues to actively attempt to disclaim liability. In a letter sent to people affected by the breach, the OPM offers 18 months of credit monitoring services, but states that the "services are offered as a convenience to you," but "nothing in this letter should be construed as [the] OPM or the U.S. Government accepting liability for any of the matters covered by this letter or for any other purpose."

107. Numerous sources have criticized as insufficient the 18 months of credit monitoring that the OPM is offering federal applicants. U.S. Senator Mark Warner pointed out that "federal workers deserve more than 18 months of credit monitoring following a breach of such enormous size and scale." Warner criticized the quality of the credit monitoring services the OPM provided, stating that he had "heard complaints from many [former or retired federal employees] about the poor quality of service provided by the [credit monitoring service provider]." He stated that the "website crashes frequently, [] the dedicated hotline regarding the OPM Breach has incredibly long wait times, [often over an hour]," and that many employees have "reported receiving inaccurate or out-of-date information regarding their credit history, which calls into question [the provider's] ability to appropriately protect them from fraud and ID theft." He further noted that employees have "reported extreme difficulties with obtaining information [] regarding the $1 million in identity theft insurance."

V. PLAINTIFFS' DAMAGES

108. Due to Defendants' willful, intentional, and flagrant disregard of Plaintiffs' and Class members' privacy rights, and the OPM Defendants' failure to implement the

OIG's detailed recommendations and instructions—including shutting down the OPM's software systems to prevent the breach—Plaintiffs and Class members have suffered and will continue to suffer damages, including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress. They have suffered or are at increased risk of suffering from:

- the loss of the opportunity to control how their PII is used;
- the diminution in the value and/or use of their PII entrusted to the OPM for the purpose of deriving employment from the OPM and with the understanding that the OPM and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others;
- the compromise, publication, and/or theft of their PII and the PII of their family members, neighbors, and acquaintances;
- out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
- lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the OPM Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse;
- costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;
- unauthorized use of compromised PII to open new financial and/or health care or medical accounts;

- the continued risk to their PII, and the PII of their family members and acquaintances, which remains in the OPM's possession and is subject to further breaches so long as KeyPoint and the OPM fail to undertake appropriate and adequate measures to protect the PII in its possession;
- current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the OPM Breach for the remainder of the lives of the Class members and their families.

VI. CLASS ACTION ALLEGATIONS

109. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of a class of similarly situated persons, which they initially propose be defined as follows:

> All current, former, and prospective employees and contractors of the United States whose PII was compromised as a result of the data breach that the OPM first announced on June 4, 2015.

110. Excluded from the proposed class are the OPM, Archuleta, Seymour, and KeyPoint, as well as agents, officers and directors (and their immediate family) of the OPM and KeyPoint, their parents subsidiaries, affiliates and controlled persons. Also excluded is any judicial officer assigned to this case.

111. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4).

112. Numerosity—Fed. R. Civ. P. 23(a)(1). The members of the class are so numerous that joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiffs at the present time and can only be ascertained through appropriate discovery, Plaintiffs believe that there are eighteen million or more members of

the class located throughout the United States. It would be impracticable to join the class members individually.

113. Existence and predominance of common questions of law—Fed. R. Civ. P. 23(a)(2), 23(b)(3). Common questions of law and fact exist as to all members of the class and predominate over any questions solely affecting individual members of the class. Among the many questions of law and fact common to the class are:

(i) whether the OPM's conduct violated the Privacy Act of 1974;

(ii) whether the OPM failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to the security and integrity of these records;

(iii) whether the OPN disclosed Plaintiffs and Class members' PII without their prior written consent;

(iv) whether the OPM's conduct was willful or with flagrant disregard for the security of Plaintiff and Class Members' PII;

(v) whether the OPM's conduct violated the Administrative Procedure Act;

(vi) whether KeyPoint had a legal duty to use reasonable cyber security measures to protect Plaintiffs and Class members' PII;

(vii) whether KeyPoint breached its legal duty by failing to protect Plaintiffs and Class members' PII;

(viii) whether KeyPoint acted reasonably in securing Plaintiffs and Class members' PII;

(ix) whether Plaintiffs and Class members are entitled to damages, declaratory or injunctive relief.

114. Typicality—Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of the claims of the members of the class. Among other things, Plaintiffs and Class members are all former, current, and prospective employees and contractors of the federal government who filed SF-86 and other sensitive documentation with the OPM.

115. Adequacy—Fed. R. Civ. P. 23(a)(4). Plaintiffs will adequately represent the proposed Class members. They have retained counsel competent and experienced in class action and internet privacy litigation and intend to pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of class members.

116. Superiority—Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

117. In the alternative, the class may be certified under Rule 23(b)(1), 23(b)(2) or 23(c)(4) because:

(i) The prosecution of separate actions by the individual members of the class would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants;

(ii) The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;

(iii) Defendants acted or refused to act on grounds generally applicable to the class, thereby making appropriate final injunctive relief with respect to the members of the class as a whole; and

(iv) The claims of class members are comprised of common issues that are appropriate for certification under Rule 23(c)(4).

VII. STANDING

118. The AFGE has standing to pursue declaratory and injunctive relief in this action because its members—including Plaintiff and active AFGE member Robert Crawford—have standing to sue on their own behalf, by this action it seeks to protect the privacy interests of its members (employees of the federal government), and this action (and the declaratory and injunctive relief the AFGE seeks through it) does not require the participation of individual AFGE members.

VIII. CLAIMS

COUNT ONE
(On behalf of Plaintiffs Crawford, Dale, and Class members against the OPM)
VIOLATION OF UNITED STATES 5 U.S.C. § 552a PRIVACY ACT OF 1974 ("PRIVACY ACT")

119. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

120. The OPM is an "agency" within the meaning of the Privacy Act.

121. Pursuant to 5 U.S.C. § 552a(b), agencies are prohibited from disclosing "any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . ."

122. Pursuant to 5 U.S.C. § 552a(e)(10), "[e]ach agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

123. The OPM obtained and preserved Plaintiffs and Class members' PII, including SF-86 and other records, in a system of records during the recruiting and security check processes.

124. The OPM is therefore prohibited from disclosing federal applicants' PII under 5 U.S.C. § 552a(b) and is responsible for establishing appropriate "safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity" under 5 U.S.C. § 552a(e)(10)."

125. The OPM is, and at all relevant times was required by law to comply with both FISMA and the Modernization Act. The OPM is also responsible for ensuring that its cyber security systems comply with 5 U.S.C. § 552a and other rules and regulations governing cyber security practices.

126. However, dating back to at least 2009, through a continuous course of conduct, the OPM intentionally, willfully, and with flagrant disregard failed to comply with FISMA and demonstrated multiple "material weaknesses." The OPM thus knew that its computer security practices were not in compliance with 5 U.S.C. § 552a, FISMA, the Modernization Act, and other rules and regulations governing cyber security practices because the OIG's annual audit reports have consistently recognized the OPM's noncompliance with FISMA.

The OIG explicitly recognized that the OPM failed to comply with FISMA each year from 2009-2014:

- **2009.** "The continuing weaknesses in OPM's information security program result directly from inadequate governance. Most, if not all, of the exceptions we noted this year resulted from a lack of necessary leadership, policy, and guidance."
- **2010.** "We continue to consider the IT security management structure, insufficient staff, and the lack of policies and procedures to be a material weakness related to the management of OPM's Certification and Accreditation (C&A) process. The C&A concerns were reported as a significant deficiency in the FY 2008 and FY 2009 [FISMA] audit reports."
- **2011.** "We continue to believe that information security governance represents a material weakness in OPM's IT security program. . . . [T]here were, in our opinion, three root causes of OPM's C&A issues: insufficient staffing in the IT Security and Privacy Group, a lack of policy and procedures, and the decentralized DSO model in place at OPM."
- **2012.** "Throughout FY 20-12, the OCIO continued to operate with a decentralized IT security structure that did not have the authority or resources available to adequately implement the new policies . . . . Th[is] material weakness remains open in this report, as the agency's IT security function remained decentralized throughout the FY 2012 FISMA reporting period and because of the continuing instances of non-compliance with FISMA requirements."

- **2013.** "The findings in this audit report highlight the fact that OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."
- **2014.** "The findings in this audit report . . . indicate that OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."

127. Specifically, the OPM was required—but failed—to take several steps to comply with applicable security rules and regulations including but not limited to:

- Implementing PIV multi-factor authentication for all 47 of the agency's major applications, as required by the OIG's prior audit reports and required by OMB Memorandum M-11-11;
- Centralizing its cyber security structure to ensure that it can effectively manage its cyber security program and protect its software systems against a breach; and
- Shutting down unauthorized software systems and ensuring that all software systems are authorized before being put back into operation.

128. The OIG found that one of the "core causes" of the OPM's non-compliance with FISMA was the "fact that there are currently no consequences for OPM systems that do not have a valid Authorization to operate." As a result, in 2014, the OIG recommended introducing administrative sanctions to combat instances of willful non-compliance with FISMA requirements.

129. From 2009 to 2014, the OIG also found that the OPM was not in compliance with several standards promulgated under 40 U.S.C. § 11331, as is required by FISMA, including in the areas of risk management, configuration management, incident response and

reporting, continuous monitoring management, contractor systems, security capital planning, and contingency planning.

130. Through a continuous course of conduct, the OPM thus willfully, intentionally and with flagrant disregard refused to take steps to implement "appropriate safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity."

131. The OPM Defendant's history of non-compliance with FISMA's legal requirements that culminated in Archuleta's decision not to follow the OIG's 2014 instruction to shut down information systems that did not have current and valid authorizations resulted (1) the disclosure of Plaintiffs and Class members' records without prior written consent in violation of 5 U.S.C. § 552a(b) and ultimately (2) the "substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members," that 5 U.S.C. § 552a(e)(10) is designed to protect against.

132. As a result of the OPM Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the privacy act. Such damages have included or may include without limitation (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to the OPM for the purpose of deriving employment from the OPM and with the understanding that the OPM and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members, neighbors, and acquaintances; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5)

lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the OPM Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) the continued risk to their PII, and the PII of their family members, neighbors, and acquaintances, which remains in the OPM's possession and is subject to further breaches so long as the OPM fails to undertake appropriate and adequate measures to protect the PII in its possession; and (9) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the OPM Breach for the remainder of the lives of the Class members and their families. Plaintiffs and Class members are thus entitled to relief pursuant to 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

COUNT TWO
(On behalf of Plaintiffs and Class members against the OPM Defendants)
VIOLATIONS OF THE ADMINISTRATIVE PROCEDURE ACT, 5 U.S.C. § 701, *ET SEQ.*

133. Plaintiffs incorporate each and every allegation as if fully set forth herein.

134. The OPM was required to comply with FISMA and has a continuing obligation to comply with the Modernization Act. Moreover, under FISMA, Archuleta was required to exercise oversight over the OPM's information security policies and practices, including implementation of rules and standards complying with 40 U.S.C. § 11331. However, as is alleged at paragraphs 60-67, 126, and 129 from 2009 to 2014, through a continuous course of

conduct, the OPM intentionally failed to comply with FISMA and 40 U.S.C. § 11331 resulting in violations of the Privacy Act, 5 U.S.C. § 552a.

135. The OPM Defendants' non-compliance with FISMA's requirements was consistent from 2009 to 2014 and was not a valid exercise of discretion. FISMA and the Modernization Act are the law and pursuant to FISMA's terms, Archuleta is required oversee the OPM's compliance with both. The OIG found that she failed to do so and that her failure was caused in large part by the absence of any consequence for such noncompliance. Ultimately the OPM's noncompliance with FISMA and the Modernization Act resulted in the Privacy Act violations at the center of this lawsuit

136. The OPM's noncompliance with FISMA is well documented in each of the OIG's annual audit reports issued from 2009 to 2014. As is alleged at paragraphs 60-67, 126, and 129 in each of the OIG's audit reports, the OIG tells the OPM to bring its cyber security systems in compliance with FISMA, but each year, the OPM Defendants made the decision not to do so. For example, from 2011 to 2014, the OIG told the OPM it was not in compliance with FISMA because of its decentralized cyber security governance system. Yet the OPM Defendants repeatedly made the decision not to comply with FISMA's requirements. And in 2014, the OIG specified: "OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."

137. The OPM's continuous string of decisions not to comply with FISMA culminated in Archuleta's choice not to follow the OIG's November 2014 instruction to shut down several of its compromised software systems. In the 2014 audit report, the OIG found 11 of 21 software systems were unauthorized, meaning that those software systems had not been checked to determine whether they were vulnerable to a data breach. The OIG

instructed Defendants to shut down "[software] systems that do not have a current and valid authorization." However, the OPM refused to shut down its software systems to make sure "that there [were] no interruptions to [the] OPM's missions and operations." At the Committee Hearing, Archuleta stated that, "[i]t was my decision that we would not [close down the software systems] but continue to develop the systems and ensure we have security on those systems."

138. The OPM Defendants' many decisions not to comply with FISMA including but not limited to (1) deciding not to implement a centralized cyber security governance system, and (2) deciding not to follow the OIG's recommendation and shut down its software systems, constitute final agency actions because the decisions were the consummation of the OIG's decision making process, were not of a merely tentative or interlocutory nature, and denied Plaintiffs and Class members the right to protection of their PII, including SF-86 and other records. Because the OPM Defendants' willful and intentional continuous course of conduct resulted in the OPM Breach in which Plaintiffs and Class members' PII was compromised, the OPM Defendants continuous string of decisions not to comply with FISMA caused violations the Privacy Act and damages to Plaintiffs and Class members.

139. The OPM Defendants violated their obligation to comply with FISMA, 40 U.S.C. § 11331, and the Privacy Act because, for years, they ignored the OIG's detailed instructions and ultimately, decided to reject its instruction that the OPM shut down certain of its major software systems that were not in compliance with FISMA.

140. Defendants' continuous string of decisions not to comply with FISMA—including its decisions not to implement a centralized cyber security governance system and its refusal to shut down the OPM's software systems in contravention of the OIG's

instructions—was arbitrary, capricious and otherwise not in accordance with law; was in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; and was without observance of procedure required by law.

141. Because of the OPM Defendants' decisions not to comply with FISMA, the OPM Defendants violated the Privacy Act, Plaintiffs and Class members suffered a legal wrong, and were adversely affected insofar as cyber attackers gained access to their sensitive, confidential, and personal information, including but not limited to PII and information contained on the SF-86.

142. Plaintiffs and Class members are thus entitled to declaratory and injunctive relief.

COUNT THREE
(On behalf of Plaintiffs Crawford, Dale, and Class members against KeyPoint)
NEGLIGENCE

143. Plaintiffs incorporate each and every allegation as if fully set forth herein.

144. From 2014 to present, KeyPoint has worked as a contractor for OPM responsible for conducting background checks on federal applicants. KeyPoint's employees were granted access to OPM's systems containing Plaintiffs and Class members' PII.

145. KeyPoint owed Plaintiffs and Class members a duty to take reasonable steps to maintain and protect against any dangers to Plaintiffs and Class members' PII presented by cyber attackers. This duty included, among other things, maintaining and testing KeyPoint's cyber security systems, taking other reasonable security measures to protect and adequately secure the PII of Plaintiffs and Class members from unauthorized access, and taking reasonable steps to ensure that hackers did not compromise KeyPoint employees' credentials.

146. KeyPoint owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate cyber security practices. It was foreseeable that if KeyPoint did not take reasonable security measures—including protecting its OPM credentials—the PII of Plaintiffs and Class members would be stolen. KeyPoint knew or should have known that OPM employee data was an attractive target for cyber attackers, particularly in light of the prior data breaches experienced by the OPM and its contractors, and yet KeyPoint failed to take reasonable precautions to safeguard the PII of federal applicants.

147. A finding that KeyPoint owed such a duty to Plaintiffs and Class members would not impose a significant burden on KeyPoint. KeyPoint has the ability to sufficiently guard against cyber attackers accessing OPM's systems by implementing adequate measures to protect KeyPoint employees' credentials from compromise. The cost borne by KeyPoint for these efforts is insignificant in view of the dangers posed to Plaintiffs and Class members by KeyPoint's failure to take such steps.

148. In December 2014, the OPM announced that KeyPoint's cyber security systems sustained a breach. In that breach, cyber attackers were able to access KeyPoint's OPM credentials, which, according to Archuleta, facilitated the massive OPM Breach which compromised the PII of approximately 18 million federal employees.

149. By failing to implement necessary measures to protect KeyPoint's security credentials, KeyPoint departed from the reasonable standard of care and breached its duties to Plaintiffs and Class members.

150. But for KeyPoint's failure to implement and maintain adequate security measures to protect Plaintiffs' and Class members' PII, and failure to adequately log security

intrusions into its software systems, the PII of Plaintiffs and Class members would not have been stolen, Plaintiffs and Class members would not have been injured, and Plaintiffs and Class members would not be at a heightened risk of identity theft in the future.

151. KeyPoint's negligence was a substantial factor in causing harm to Plaintiffs and Class members. As a direct and proximate result of KeyPoint's failure to exercise reasonable care and deploy reasonable cyber security measures, the PII of Plaintiffs and Class members was accessed by cyber attackers who can use the compromised PII to commit identity theft and health care and/or medical fraud.

152. As a result of KeyPoint's negligence, Plaintiffs and Class members have suffered damages that have included or may include without limitation: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to the OPM and KeyPoint for the purpose of deriving employment from the OPM and with the understanding that the OPM and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members, neighbors, and acquaintances; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the OPM Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7)

unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) the continued risk to their PII, and the PII of their family members, neighbors, and acquaintances, which remains in KeyPoint and the OPM's possession and is subject to further breaches so long as KeyPoint and the OPM fail to undertake appropriate and adequate measures to protect the PII in its possession; and (9) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the OPM Breach for the remainder of the lives of the Class members and their families.

COUNT FOUR
(On behalf of Plaintiffs and Class members against KeyPoint)
DECLARATORY JUDGMENT

153. Plaintiffs incorporate each and every allegation as if fully set forth herein.

154. As previously alleged, Plaintiffs and Class members have stated claims against KeyPoint based on negligence.

155. KeyPoint has failed to satisfy its obligation take reasonable steps to maintain and protect against any dangers to Plaintiffs and Class members' PII presented by cyber attackers, as is evidenced by the KeyPoint Hack which was announced in December 2014.

156. KeyPoint continues to work as the OPM's security clearance contractor, in which capacity it maintains Plaintiffs and Class members' PII. KeyPoint is thus under a continuing obligation to take reasonable cyber-security measures to maintain and protect against dangers to Plaintiffs and Class members' PII presented by potential cyber attacks.

157. An actual controversy has arisen in the wake of the OPM Breach regarding KeyPoint's *current* obligations to provide reasonable data security measures to protect the PII of Plaintiffs and Class members. KeyPoint maintains that its cyber security measures

were, and remain, reasonably adequate, that weak cyber security measures were not a factor in the KeyPoint Hack, and that the KeyPoint Hack was not related to the OPM Breach.

158. Plaintiffs thus seek a declaration that to comply with its existing obligations, KeyPoint must implement specific additional, prudent industry practices, as outlined below, to provide reasonable protection and security to the PII of Plaintiffs and Class members.

159. Specifically, Plaintiffs and Class members seek a declaration that (a) KeyPoint's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, KeyPoint must implement and maintain reasonable security measures on behalf of Plaintiffs and Class members, including, but not limited to: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on KeyPoint's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its cyber security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, data not necessary for KeyPoint or the OPM's business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; and, (6) receive periodic compliance audits by a third party regarding the security of the computer systems KeyPoint uses to store the PII of the OPM's current and former employees.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

(a) Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' counsel to represent the class;

(b) Award Plaintiffs and Class members appropriate relief, including actual and statutory damages;

(c) Award equitable, injunctive, and declaratory relief as may be appropriate:

(d) Find that KeyPoint breached its duty to implement reasonable security measures to safeguard and protect the PII of Plaintiffs and Class members that was compromised in the OPM Breach.

(e) Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

(f) Award pre-judgment and post-judgment interest as prescribed by law; and,

(g) Grant further and additional relief as this court may deem just and proper.

X. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: June 29, 2015

Respectfully submitted,

WHITFIELD BRYSON & MASON LLP

By:*/s/ Gary E. Mason*
Gary E. Mason

1625 Massachusetts Ave., NW, Ste. 605
Washington, DC 20036
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

GIRARD GIBBS LLP
Daniel C. Girard (*pro hac pending)*
Adam E. Polk (*pro hac pending)*
Christopher K. Hikida (*pro hac pending)*

601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiffs

JS 44 (Rev. 12/12)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

American Federation of Government Employees, AFL-CIO; Robert Crawford; and Adam Dale; on behalf of themselves and all others similarly situated

(b) County of Residence of First Listed Plaintiff 11001
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Gary E. Mason, Whitfield Bryson & Mason LLP
1625 Massachusetts Ave. NW, Ste. 605
Washington, DC 20036 Tel: (202) 429-2290

DEFENDANTS

United States Office of Personnel Management; Katherine Archuleta; Donna Seymour; and KeyPoint Government Solutions

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☒ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
5 U.S.C. § 552a (Privacy Act), 5 U.S.C. § 701, et seq. (APA), negligence, Declaratory Judgment

Brief description of cause:
Violations of Privacy Act and Administrative Procedure Act

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 6/29/15

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Columbia

American Federation of Government Employees, AFL-CIO; Robert Crawford; and Adam Dale; on behalf of themselves and all others similarly situated

Plaintiff(s)

v.

United States Office of Personnel Management, Katherine Archuleta, Donna Seymour, and Keypoint Government Solutions

Defendant(s)

Civil Action No. 1:15-cv-1015

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Katherine Archuleta
United States Office of Personnel Management
1900 E. Street, NW
Washington, DC 20415

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Gary E. Mason
Whitfield Bryson & Mason LLP
1625 Massachusetts Ave. NW, Ste. 605
Washington, DC 20036
Telephone: (202) 429-2290

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: 06/29/2015

Signature of Clerk or Deputy Clerk

Civil Action No. 1:15-cv-1015

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Columbia

American Federation of Government Employees, AFL-CIO; Robert Crawford; and Adam Dale; on behalf of themselves and all others similarly situated

Plaintiff(s)

v.

United States Office of Personnel Management; Katherine Archuleta; Donna Seymour; and Keypoint Government Solutions

Defendant(s)

Civil Action No. 1:15-cv-1015

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* KeyPoint Government Solutions
1750 Foxtail Drive
Loveland, CO 80538

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Gary E. Mason
Whitfield Bryson & Mason LLP
1625 Massachusetts Ave. NW, Ste. 605
Washington, DC 20036
Telephone: (202) 429-2290

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: 06/29/2015

Signature of Clerk or Deputy Clerk

Civil Action No. 1:15-cv-1015

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Columbia

American Federation of Government Employees, AFL-CIO; Robert Crawford; and Adam Dale; on behalf of themselves and all others similarly situated

Plaintiff(s)

v.

United States Office of Personnel Management; Katherine Archuleta; Donna Seymour; and Keypoint Government Solutions

Defendant(s)

Civil Action No. 1:15-cv-1015

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* United States Office of Personnel Management,
1900 E. Street, NW
Washington, DC 20415

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Gary E. Mason
Whitfield Bryson & Mason LLP
1625 Massachusetts Ave. NW, Ste. 605
Washington, DC 20036
Telephone: (202) 429-2290

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: 06/29/2015

Signature of Clerk or Deputy Clerk

Civil Action No. 1:15-cv-1015

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Columbia

American Federation of Government Employees, AFL-CIO; Robert Crawford; and Adam Dale; on behalf of themselves and all others similarly situated

Plaintiff(s)

v.

United States Office of Personnel Management; Katherine Archuleta; Donna Seymour; and Keypoint Government Solutions

Defendant(s)

Civil Action No. 1:15-cv-1015

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Donna Seymour
Chief Information Officer
United States Office of Personnel Management
1900 E. Street, NW
Washington, DC 20415

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Gary E. Mason
Whitfield Bryson & Mason LLP
1625 Massachusetts Ave. NW, Ste. 605
Washington, DC 20036
Telephone: (202) 429-2290

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: 06/29/2015

Signature of Clerk or Deputy Clerk

Civil Action No. 1:15-cv-1015

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset