IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLORADO

Civil Action No. _____

THE HONORABLE TERESA J. MCGARRY
on behalf of herself and all others similarly situated,

Plaintiffs,

v.

THE UNITED STATES OFFICE OF PERSONNEL MANAGEMENT,
KEYPOINT GOVERNMENT SOLUTIONS, INC., a Delaware corporation, and
THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY,

Defendants.

COMPLAINT

Plaintiff, The Honorable Teresa J. McGarry, individually and on behalf of the proposed class described below, brings this action for injunctive relief, and actual and statutory damages against Defendants United States Office of Personnel Management ("OPM"), the United States Department of Homeland Security ("DHS"), and KeyPoint Government Solutions ("KeyPoint") (collectively "the OPM Defendants"), and alleges as follows:

I. SUMMARY OF THE CASE

1. This case arises out of at least two cyber-breaches of OPM's systems that compromised the security of up to 21.5 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"). Plaintiff and Class members include current, former, and prospective employees and contractors ("federal applicants") of the U.S. government.

2. 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.

OPM maintains this data in a "system of records," which is an organized system that places data in accordance with employee name, date of birth, etc.

3. As part of OPM's security clearance protocol, applicants applying for security clearance ("security applicants") must submit Standard Form 86 ("SF-86") or Standard Form 85P (SF-85P). Both are detailed forms that include questions regarding applicants' financial histories and investment records, children's and relative's names, foreign trips taken, contacts with foreign nationals, past residences, schools, names of neighbors, and close friends such as college roommates and coworkers. An applicant also signed blank forms allowing access to medical records and financial records. Fingerprints can also be a part of this data collection. Items required in the above forms are often used as security questions by other employers both inside and outside government. All of this data is part of OPM's system of records and therefore OPM is responsible for maintaining and safeguarding the data.

4. Since at least 2007, OPM has been on notice of significant deficiencies in its cyber security protocol. OPM's Office of Inspector General ("OIG") was required under federal law to, and did, conduct annual audits of OPM's cyber security program and practices, identifying "material weakness[es]" as far back as 2007. OPM not only failed to cure the weaknesses, but OIG found that in many areas 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 OPM offices to authorize the [software] systems they own."

5. From 2007 to the present, OPM, Chief Information Officer for OPM Donna Seymour ("Seymour"), and Director Katherine Archuleta ("Archuleta")—who served as OPM's director from November 2013 until resigning on July 10, 2015—repeatedly failed to comply with federal law and to make the changes required by OIG's annual audit reports. Specifically, 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, OIG identified multiple cyber security deficiencies that "could potentially have national security implications" and are core to OPM's violation of the Privacy Act. These included OPM's decentralized structure, poor risk management, high rate of false security alerts, security issues with remote access sessions, failure to test contingency plans, and failure to use Personal Identification Verification ("PIV") Cards for multi-factor authentication in all major software systems. As a result, OIG concluded that OPM's software systems were so vulnerable that Archuleta and OPM should consider largely shutting the system down.

7. OPM continued to ignore OIG's reports. 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 OPM would notify 48,439 federal workers that their information may have been exposed. After the OPM Breach became public, however, Archuleta and OPM identified the misuse of a KeyPoint user's credential as the source of the breach.

8. KeyPoint President and Chief Executive Officer ("CEO") Eric Hess responded to Archuleta's contention on June 24, 2015 in 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 knowledge of the recent KeyPoint Breach and OIG's explicit warnings about deficiencies in cyber security protocol and the dangers associated with those deficiencies, the OPM Defendants elected not to shut down OPM's software systems. On June 4, 2015, OPM announced that it had been the subject of a massive cyber attack that compromised millions of federal applicants' personally identifiable information ("PII")[1], records, and sensitive information.

10. After OPM announced that its systems 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—

[1] 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.

chairman of the House Oversight and Government Reform Committee—likened 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."

11. On July 9, 2015, OPM issued a second news release confirming that a significantly greater number of individuals were affected by a "separate but related" cyber security breach. OPM announced that records of 21.5 million individuals had been stolen, including, "identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal acquaintances; health, criminal and financial history; and other details. Some records also include findings from interviews conducted by background investigators and fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."

12. OPM confirmed that 19.7 million of those affected were federal applicants who applied for a background investigation, and another 1.8 million were non-applicants, including family members, spouses, co-habitants and other close contacts of federal applicants, who never applied for a position with the U.S. government. In addition, approximately 1.1 million of the stolen records included fingerprints. Notification letters on the second breach have been mailed as of the end of July 2015 and offer the recipient three years of service by a hired contractor who will watch accounts registered with the company.

13. Besides OPM and KeyPoint, the United States Department of Homeland Security ("DHS") was uniquely situated to protect the Plaintiff and Class Members' information from being compromised. The United States Government, in the early 2000s, invested in a multibillion-dollar cyber traffic monitoring system known as "EINSTEIN." DHS was

responsible for overseeing EINSTEIN. The system was created to detect and prevent intruders from compromising the cyber security of federal governmental databases, including those housed at OPM and other governmental agencies. DHS failed as EINSTEIN did not prevent intruders from breaching the OPM network and extracting sensitive files pertaining to millions of current, former, and prospective federal employees and contractors.

14. As a result of Defendants' conduct, Plaintiff 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. Plaintiff and Class members request damages to compensate them for their current and future losses and injunctive relief to fix OPM's security protocol, implement OIG's latest audit instructions, provide adequate credit monitoring services for the lifetimes of each Class member and their family members, and to provide after-the-fact identity repair services and identity theft insurance to protect Class members and their family members from fraud or identity theft.

II. PARTIES

A. Plaintiff

16. Plaintiff, The Honorable Teresa J. McGarry, is a resident of the state of Florida. Judge McGarry has over 30-years of government service, including military service and time working as a federal prosecutor. She currently works as an Administrative Law Judge in Jacksonville, Florida, with the Social Security Administration. Judge McGarry has had at least two background investigations, submitting a SF-86 or the SF-85P as a condition of her

employment. Additionally, she has been interviewed during her current spouse's 2009 background investigation and for friends, who listed her as a reference. She has received the initial breach letter regarding the scope of the OPM Breach. Based on OPM's public statements regarding the scope of the OPM Breach and the initial breach letter, Judge McGarry's PII, personal records, and sensitive information were all compromised as a result of OPM's breach.

B. Defendants

17. Defendant OPM is an Agency of the United States government with headquarters at 1900 E. Street, NW, Washington, DC 20415. 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, OPM collects and maintains federal applicants' records including PII, background investigations, and security clearance forms. OPM conducts more than two million background investigations annually, provides critical human resources services to other government agencies, and audits agency personnel practices.

18. 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, a Delaware corporation, maintains its corporate headquarters and principal place of business 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 OPM as "provid[ing] fieldwork services for background investigations." According to one

report, KeyPoint is the federal government's largest private provider of background investigations.

19. Defendant DHS is a Department of the United States government with headquarters at 245 Murray Lane SW Washington, DC 20528. DHS's stated mission is to "secure the nation from the many threats we face." To execute this mission, DHS has hundreds of thousands of employees in jobs that range from aviation and border security to emergency response. Core to DHS's mission is implementing a digital strategy, which meets the needs of a rapidly changing electronic landscape and ensures the protection of federal information technology.

III. JURISDICTION AND VENUE

20. 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 this lawsuit has been brought as a class action, the aggregate claims of the putative class members exceed $5 million exclusive of interest and costs, and one or more of the members of the putative class is a resident of a different state than Defendants.

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

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

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

24. The Court has personal jurisdiction over Defendants pursuant to Colo. Rev. Stat. Ann. § 13-1-124 because Defendants transacted business, committed tortious acts, and possessed

property in the State of Colorado sufficient to support jurisdiction. Defendants work with, monitor, oversee, and maintain relationships with the citizens of this state and thus have substantial, continuous, and systematic contacts with the State of Colorado.

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

25. OPM is an independent government agency that manages the civil service of the U.S. government. 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.

26. OPM collects and stores huge amounts of government-wide human resources data. OPM manages the electronic Official Personnel Folder ("eOPF"), a software system that provides on-demand web-based access to personnel folders and 24/7 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.

27. Through its Federal Investigative Services division, 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 a purported secure electronic repository for personal investigative data, which is supposed to allow for the imaging, transfer, and secure disposition of highly sensitive information.

28. Some aspects of EPIC contain information that is so sensitive that EPIC 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.

B. OPM's Weak Cyber Security Measures

29. Pursuant to the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541, *et seq.* ("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.

30. In accordance with FISMA, OIG conducts annual, independent audits of OPM's cyber security program and practices. DHS's Office of Cybersecurity and Communications

issues Inspector General FISMA Reporting Instructions. Using these guidelines, OIG reviews the OPM's FISMA compliance strategy and documents the status of its compliance efforts. Chief among the cyber security issues that OIG reviews is risk management, incident response, remote access, and incident reporting programs.

31. As director of OPM, Archuleta was under a mandate pursuant to FISMA 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."

32. OPM repeatedly failed to meet FISMA guidelines. OIG found that OPM was not in compliance with several standards promulgated under 40 U.S.C. § 11331, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, contractor systems, security capital planning, and contingency planning.

33. In OIG's most recent 2014 audit, it concluded that OPM lacked a centralized cyber security team responsible for overseeing all of OPM's cyber security efforts. OPM has had a decentralized cyber security governance structure since at least 2009. In 2012, OPM attempted to centralize the Designated Security Officer ("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, OPM only partially implemented the centralization. Although OPM designated four centralized officers to oversee DSO's work, OIG identified many software systems that were not centralized.

34. In addition, OIG found that OPM was not in compliance with the OMB's requirements, which mandate the use of PIV Cards for multi-factor authentication in all

major software systems. Multi-factor authentication requires more than one form of independent credentials to verify a 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). OIG found that none of OPM's major applications required PIV authentication in the identification process.

35. Also in its November 2014 audit report, OIG found that a critical flaw was OPM's Security Assessment and Authorization—its process of certifying a software system's security controls. The OMB requires all federal software systems to have a valid authorization—that it meets all security requirements. Despite these OMB requirements, OIG found that only 10 of 21 software systems due for authorization were completed on time. The rest were operating without valid authorization, meaning that those software systems had not been checked to determine whether they were vulnerable to a data breach. 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 throughout OPM, including the offices of the Chief Information Officer; Federal Investigative Services; Human Resources Solutions; Inspector General; and Chief Financial Officer.

36. 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 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." OIG stated that "[a]ny weaknesses in the [software] systems supporting this program office could potentially have national security implications."

37. Because of the significant flaws in OPM's cyber security systems, 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, OIG noted that 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."

38. The significant flaws in OPM's cyber security systems left the personal data of millions vulnerable to a cyber attack. While many viable improvements to OPM's data network existed, one easy fix was for OPM to eliminate all personal data upon completion of a security check. Once an individual is granted security clearance there is little value for highly sensitive personal information. Information such as fingerprints is available elsewhere, and signed forms, personal history, comments, and most of the background material serve no purpose after clearance has been granted. Thus, OPM could have had a mandatory destruction cycle with a short time frame for all data on the SF-85, SF-85P, and SF-86. OPM could retain hard copies and eliminate the electronic version upon the approval or denial of a security clearance. Since all security clearances require periodic renewal, OPM could compare any newly submitted electronic information with the retained hard copy. But because OPM electronically stored all forms submitted for security clearance, any breach left highly confidential information vulnerable to detection by a cyber-hacker.

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

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

40. In 2009, OIG first recognized a material weakness in OPM's "overall [cyber] security governance program," noting that OPM failed to fill key cyber security leadership positions. The absence of leadership meant that OPM did not have the necessary oversight to correct system-wide cyber security issues. Furthermore, OIG found that 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.

41. In 2010, OIG again found"material weakness" in OPM's cyber security governance, meaning that OPM's employees did not have guidance on how to prevent software systems from being hacked. In addition, OIG added Security Assessment and Authorization as a material weakness finding that the quality of the authorization process had worsened from the previous two years. OIG noted that OPM lacked the staff to ensure that all software systems had cyber security measures necessary to fend off cyber-hacks.

42. In 2011, OIG again labeled OPM's cyber security governance a "material weakness," noting that OPM continued to lack staff in key cyber security leadership positions, and that the DSOs did not have the technical skill to effectively determine whether a software system was vulnerable to attack. Furthermore, 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.

43. In 2012, OIG continued to recognize a "material weakness" in OPM's cyber security governance, finding that though OPM had hired a Chief Information Security Officer ("CISO")—a key leadership position in its cyber security team—OPM did not give the CISO any authority to oversee the DSOs. This meant that the new position failed to centralize OPM's security personnel and provide an oversight structure to ensure that software systems were secure. 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 OPM's database and posted 37 user IDs and passwords online. 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.

44. In 2013, despite years of documented problems regarding cyber security governance at OPM, 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 OPM's ability to manage major software systems. OIG also found that 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 a PIV card.

45. In its 2014 audit report, OIG similarly found that OPM's noncompliance 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."

46. As a result, in 2014, OIG recommended introducing administrative sanctions to combat instances of willful non-compliance with FISMA requirements. 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 information systems they own."

D. The KeyPoint Hack and DHS's failure to Detect and Prevent the Breach

47. In December 2014, 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, OPM's spokesperson, stated that there was "no conclusive evidence to confirm sensitive information was removed from the [software] system."

48. KeyPoint became the largest government contractor performing private employee clearances after its predecessor, USIS, was terminated following 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 voiced her concern: "Can [KeyPoint] even handle the influx of these new employees and all the work that gets dumped on them by OPM?"

49. In the wake of the KeyPoint Hack, and in view of the OPM Breach, it has become apparent that KeyPoint and OPM could not handle the workload and protect Plaintiff 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 DHS's 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."

50. After the KeyPoint hack, DHS and other agencies began helping OPM with its network monitoring. According to DHS spokesman S.Y. Lee, DHS and "interagency partners" were helping OPM improve its network monitoring "through which [the] OPM detected new malicious activity affecting its [software] systems and data in April 2015." 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 OPM's software systems and data center. But DHS's help came too late.

51. DHS's role in data breach detection was well established. In the early 2000s, Congress and presidential action established EINSTEIN. In establishing EINSTEIN, Congress sought to create a system that defends civilian agency networks from cyber threats. Currently, there are three versions of EINSTEIN (E^1, E^2, and E^3) all aimed at protecting the federal computer networks and the delivery of essential government services. Specifically, Congress created EINSTEIN to determine if the government was under cyber attack, alert all impacted federal agencies, and prevent any personal data from being stolen.

52. EINSTEIN is intended to perform a cyber security function by collecting data

from all civilian agencies and comparing that data to a baseline—how the system should function if there are no abnormalities. In an ideal world, EINSTEIN would detect a cyber event by referring to the incoming flow data and assist in resolving the breach. If a particular agency was experiencing an attack, EINSTEIN would determine if the incident was across the board or isolated and then stop the attack.

53. DHS's EINSTEIN failed to detect and prevent the cyber attack on OPM's security systems. If EINSTEIN was operating in accord with its Congressional mandate, DHS would have detected the breach, informed OPM, secured all federal networks, and protected the security of the 21.5 million federal applicants' personnel and security files.

54. Even in light of the above, Seymour—in an e-mail to colleagues at OPM—praised OPM's commitment to cyber-security measures, stating: "security of our network 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, OPM was not in compliance with the FISMA or OIG's recommendations and had not been for years. And despite the KeyPoint hack, OPM continues to this day to use KeyPoint as its security clearance contractor.

E. The OPM Breach

55. On June 4, 2015, 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, OPM admits that it detected the intrusion as early as April 2015. 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, OPM issued guidance to

individuals to monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.

56. In order to access OPM's database, hackers installed a malware package that industry analysts opine was likely delivered via an e-mail "phishing" attack within 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 to capture OPM 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 valid OPM credentials to get into the software system, hackers could sneak data out of the network over the Internet, hiding their activity internally among normal traffic. It was only when OPM was assessing its software systems to actually implement continuous monitoring tools, as required by FISMA, that it discovered that something was wrong.

57. 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 for government employee and background investigations.

58. On July 9, 2015, OPM confirmed "a separate but related cybersecurity incident[]" that affected 21.5 million individuals. OPM's news release stated that OPM "has now concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominately spouses or co-habitants of applicants. As noted above, some records also include findings from interviews conducted by background investigators and

approximately 1.1 million include fingerprints. . . . If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF-85, SF-85P, and SF-86 for a new investigation or periodic reinvestigation), it is highly likely that the individual is impacted by this cyber breach. If an individual underwent a background investigation prior to 2000 that person may still be impacted, but it is less likely."

59. OPM further confirmed that the stolen records included "identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health criminal and financial history; and other details. Some records also include findings from interviews conducted by background investigators and fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."

60. As a result, OPM increased its offer of credit monitoring and identity theft insurance and recovery services to affected individuals "for a period of at least 3 years, at no charge."

F. Public Consensus—OPM is to Blame

61. 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 and take anything.

62. In testimony before the Subcommittee on Information Policy, Census and National Archives Committee on Oversight and Government reform, Daniel Bertoni, Director of

the United States Government Accountability Office ("GAO") pointed out the current and future harm to individuals as a result of OPM's Breach, "[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- 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."

63. The OPM Breach is particularly troubling because the records stolen have national security implications. The hackers accessed EPIC, a background investigation toolset, and stole SF-86 forms that 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 employee's] security clearance," said Jeff Neal, a former DHS official and a senior vice president at ICF International. "It's really a personal document."

64. OPM's failures have consequences that will last for years to come. 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 [soon after the breach] from a number of government offices across the U.S. According to Roberts, "[t]he recent OBM breach was identified, noted and the credentials and identities have been discovered online and are being traded actively."

G. OPM's Evolving Public Reaction to the Breach

65. OPM and Archuleta did not disclose in a timely or adequate manner the facts surrounding how the breach happened, why it happened, who was affected, and what was stolen.

66. 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."

67. 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."

68. Despite OPM's "history of struggling to comply with FISMA requirements" and failure to take recent steps to secure its software systems, OPM continued 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 job some 18 months ago. She claimed that 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."

69. 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. 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."

70. When asked why Archuleta did not shut down software systems despite 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." Actually, Ars Technica counters, 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."

71. Most recently, 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 retreat from 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."

72. 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 OPM: "[t]o be clear, the employee was working on OPM's systems, not KeyPoint's."

73. According to the Air Force Times, KeyPoint and Archuleta's comments amount to a statement that "no one person was responsible." But 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 OPM's software systems in late 2014—in contravention of OIG's instructions—that led directly to the OPM Breach.

74. OPM continues to actively attempt to disclaim liability. In a letter sent to people affected by the breach, OPM offered 18 months of credit monitoring services, but stated that the "services are offered as a convenience to you," and asserted that "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."

75. On July 10, 2015, one day after revealing that more than 22 million people had their data stolen in a pair of massive cyber attacks on the agency, Archuleta announced her resignation as director of OPM.

V. PLAINTIFFS' DAMAGES

76. Due to Defendants' willful, intentional, and flagrant disregard of Plaintiff's and Class members' privacy rights, and the OPM Defendants' failure to implement OIG's detailed recommendations and instructions—including shutting down OPM's software systems to prevent the breach—Plaintiff 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 OPM for the purpose of deriving employment from OPM and with the understanding that 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, friends, 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 OPM's possession and is subject to further breaches so long as KeyPoint and OPM fail to undertake appropriate and adequate measures to protect the PII in their 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;
- costs in terms of time, effort, and money associated with purchasing a comprehensive package of credit monitoring services that includes monthly social security number monitoring, ID theft victim's assistance, lost-wallet protection, 3-Bureau credit monitoring, ID password protection, and ID theft insurance for the remainder of the lives of the Class members and their families; and
- reasonable attorney fees and other litigation costs reasonably incurred in the pursuit of this action.

77. Plaintiff herself has expended time and money to acquire credit monitoring and protection services to protect herself and her family from the effects of the OPM Breach.

VI. CLASS ACTION ALLEGATIONS

78. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of a class of similarly situated persons, which Plaintiff initially proposes 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 breaches that OPM has announced.

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

80. 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).

81. 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 Plaintiff at the present time and can only be ascertained through appropriate discovery, Plaintiff believes that there are 21.5 million or more members of the class located throughout the United States. It would be impracticable to join the class members individually.

82. 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 OPM's conduct violated the Privacy Act of 1974;

(ii) whether 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 OPM disclosed Plaintiff and Class members' PII without their prior written consent;

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

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

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

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

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

(ix) whether DHS's conducted violated the Privacy Act of 1974;

(x) whether DHS 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;

(xi) whether DHS disclosed Plaintiff and Class members' PII without their prior written consent;

(xii) whether DHS's conduct was willful or with flagrant disregard for the

security of Plaintiff and Class Members' PII;

(xiii) whether DHS's conduct violated the Administrative Procedure Act;

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

83. Typicality—Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of the claims of the members of the class. Among other things, Plaintiff 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 OPM.

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

85. 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. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

86. In the alternative, the class may be certified under Federal Rule of Civil Procedure 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).

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

87. Plaintiff incorporates each and every allegation above as if fully set forth herein.

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

89. 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 . . ."

90. 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."

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

92. OPM is therefore prohibited from disclosing federal applicants' PII pursuant to 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" pursuant to 5 U.S.C. § 552a(e)(10)."

93. OPM is, and at all relevant times was required by law to comply with both FISMA and the Modernization Act. 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.

94. However, dating back to at least 2009, through a continuous course of conduct, OPM intentionally, willfully, and with flagrant disregard failed to comply with FISMA and demonstrated multiple "material weaknesses." Thus, OPM 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 OIG's annual audit reports have consistently recognized OPM's noncompliance with FISMA.

95. OIG explicitly recognized that OPM failed to comply with FISMA each year from 2009-2014 (see paragraphs 39-46, *supra*).

96. Specifically, OPM was required—but failed—to take several steps to comply with applicable security rules and regulations (see paragraphs 29-38, *supra*).

97. OIG found that one of the "core causes" of 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, OIG recommended introducing administrative sanctions to combat instances of willful non-compliance with FISMA requirements.

98. From 2009 to 2014, OIG also found that 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.

99. Through a continuous course of conduct, OPM has 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."

100. OPM's history of non-compliance with FISMA's legal requirements that culminated in Archuleta's decision not to follow OIG's 2014 instruction to shut down information systems that did not have current and valid authorizations resulted in (1) the disclosure of Plaintiff 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 Plaintiff and Class members against which 5 U.S.C. § 552a(e)(10) is designed to protect.

101. As a result of OPM Defendants' conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the Privacy Act. Such damages are alleged in paragraph 76, *supra*. Plaintiff 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 Plaintiff and Class members against DHS)
VIOLATION OF UNITED STATES PRIVACY ACT OF 1974, 5 U.S.C. § 552a ("PRIVACY ACT")

102. Plaintiff incorporates each and every allegation in paragraphs 1 through 86, above, as if fully set forth herein.

103. DHS is an "agency" within the meaning of the Privacy Act.

104. 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 . . ."

105. 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."

106. DHS was responsible through EINSTEIN to preserve Plaintiff and Class members' PII, including SF-86 and other records, in a system of records during the recruiting and security check processes.

107. DHS is therefore prohibited from disclosing federal applicants' PII pursuant to 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" pursuant to 5 U.S.C. § 552a(e)(10)."

108. DHS is, and at all relevant times was required by law to comply with both FISMA and the Modernization Act. DHS 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.

109. However, dating back to at least 2002, through a continuous course of conduct, DHS intentionally, willfully, and with flagrant disregard failed to comply with FISMA. Thus, DHS knew that OPM's 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 OIG's annual audit reports had consistently recognized OPM's noncompliance and yet DHS did not ensure that EINSTEIN was equipped to protect against any "material weaknesses" in OPM's cyber security system.

110. OIG explicitly recognized that OPM failed to comply with FISMA each year from 2009-2014 (see paragraphs 38-45, *supra*).

111. Specifically, OPM was required—but failed—to take several steps to comply with applicable security rules and regulations (see paragraphs 29-37, *supra*).

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

113. From 2009 to 2014, OIG also found that 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.

114. From 2002 on, DHS knew that EINSTEIN was supposed to provide cyber security for all federal employee sensitive information. Yet, in light of all the OIG reports, DHS did not strengthen EINSTEIN or move quickly to implement E^3. Rather, DHS stood idly by as OPM's security concerns mounted, leading to the largest security breach in our nation's history. EINSTEIN was designed to detect and protect against just such a breach.

115. Through a continuous course of conduct, DHS has 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."

116. DHS's history of non-compliance with FISMA's legal requirements that culminated in the OPM Breach resulted in (1) the disclosure of Plaintiff 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 Plaintiff and Class members, against which 5 U.S.C. § 552a(e)(10) is designed to protect against.

117. As a result of DHS's conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the Privacy Act. Such damages are alleged in paragraph 71, *supra*. Plaintiff and Class members are thus entitled to relief pursuant to 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

COUNT THREE
VIOLATIONS OF THE ADMINISTRATIVE PROCEDURE ACT
(5 U.S.C. § 701, *et seq*.)
(On behalf of Plaintiff and Class members against the OPM Defendants)

118. Plaintiff incorporates each and every allegation in paragraphs 1 through 86, above, as if fully set forth herein.

119. 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 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 39-46, *supra*, from 2009 to 2014, through a continuous course of conduct, 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.

120. OPM Defendants' non-compliance with FISMA 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 was required to oversee OPM's compliance with both. 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 OPM's noncompliance with FISMA and the Modernization Act resulted in the Privacy Act violations at the center of this lawsuit

121. In each of the OIG's annual audit reports issued from 2009 to 2014, OPM's noncompliance with FISMA is evident. As is alleged at paragraphs 39-46, *supra*, in each of the OIG's audit reports, OIG advised 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, OIG informed 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, OIG specified: "OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."

122. Unfortunately, OPM's continual failure to comply with FISMA culminated in Archuleta's choice not to follow OIG's November 2014 instruction to shut down several of its compromised software systems. In the 2014 audit report, 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. OIG instructed Defendants to shut down "[software] systems that do not have a current and valid authorization." However, 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."

123. Failing to comply with FISMA constitutes final agency action because OPM's decisions were the consummation of OIG's decision-making process, were not of a merely tentative or interlocutory nature, and denied Plaintiff and Class members the right to protection of their PII, including SF-86 and other records. Because OPM Defendants' willful and intentional continuous course of conduct resulted in the OPM Breach by which Plaintiff and Class members' PII was compromised, the OPM Defendants continuous string of decisions not to comply with FISMA caused violations of the Privacy Act and damages to Plaintiff and Class members.

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

125. Through a continuous string of decisions, OPM failed to comply with FISMA. Their actions were arbitrary, capricious and otherwise not in accordance with law were in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; and were without observance of procedure required by law.

126. Because of the OPM Defendants' decisions not to comply with FISMA, OPM Defendants violated the Privacy Act and as a result, Plaintiff 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 in the SF-86.

127. Plaintiff and Class members are thus entitled to declaratory and injunctive relief.

COUNT FOUR
(On behalf of Plaintiff and Class members against KeyPoint)
NEGLIGENCE

128. Plaintiff incorporates each and every allegation in paragraphs 1 through 86, above, as if fully set forth herein.

129. 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 Plaintiff and Class members' PII.

130. KeyPoint owed Plaintiff and Class members a duty to take reasonable steps to maintain and protect against any dangers to Plaintiff 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 Plaintiff and Class members from unauthorized access, and taking reasonable steps to ensure that hackers did not compromise KeyPoint employees' credentials.

131. KeyPoint owed a duty of care to Plaintiff 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 Plaintiff 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 OPM and its contractors, and yet KeyPoint failed to take reasonable precautions to safeguard the PII of federal applicants.

132. A finding that KeyPoint owed such a duty to Plaintiff 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 Plaintiff and Class members by KeyPoint's failure to take such steps.

133. In December 2014, 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 22 million federal employees.

134. 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 Plaintiff and Class members.

135. But for KeyPoint's failure to implement and maintain adequate security measures to protect Plaintiff and Class members' PII and failure to adequately log security intrusions into its software systems, the PII of Plaintiff and Class members would not have been stolen, Plaintiff and Class members would not have been injured, and Plaintiff and Class members would not be at a heightened risk of identity theft in the future.

136. KeyPoint's negligence was a substantial factor in causing harm to Plaintiff 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 Plaintiff and Class members was accessed by cyber attackers who can use the compromised PII to commit identity theft and various varieties of serious fraud.

137. As a result of KeyPoint's negligence, Plaintiff and Class members have suffered damages as alleged in paragraph 76, *supra*.

COUNT FIVE
(On behalf of Plaintiff and Class members against KeyPoint)
DECLARATORY JUDGMENT

138. Plaintiff incorporates each and every allegation in paragraphs 1 through 86, above, as if fully set forth herein.

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

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

141. At all times material hereto KeyPoint continued to work as OPM's security clearance contractor, in which capacity it maintained Plaintiff and Class members' PII. KeyPoint is thus under a continuing obligation to take reasonable cyber-security measures to maintain and protect against dangers to Plaintiff and Class members' PII presented by potential cyber attacks.

142. 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 Plaintiff 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.

143. Plaintiff and Class members 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 Plaintiff and Class members.

144. Specifically, Plaintiff 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 Plaintiff 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 OPM's then-current 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 OPM's current and former employees.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and Class members pray for judgment as follows:

(a) Certify this case as a class action, appoint Plaintiff as class representative, and appoint Plaintiff's counsel to represent the class;

(b) Award Plaintiff 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 Plaintiff 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.

VIII. JURY TRIAL DEMANDED

Plaintiff and Class members hereby demand a trial by jury on all issues so triable.

Dated: August 7, 2015

s/ Daniel M. Reilly
Daniel M. Reilly
dreilly@rplaw.com

s/ Ellie Lockwood
Ellie Lockwood
elockwood@rplaw.com

Reilly Pozner LLP
1900 Sixteenth Street, Suite 1700
Denver, Colorado 80202
Telephone: 303-893-6100
Fax: 303-893-6110

Jon Rosenthal
1835 NE Miami Gardens Drive #149
North Miami Beach, Florida 33179
Telephone: 954-322-0065
jrosenthal@bellsouth.net

Joseph C. Kohn
Denis F. Sheils
Barbara L. Gibson
KOHN, SWIFT & GRAF, P.C.
One South Broad Street, Suite 2100
Philadelphia, PA 19107
Telephone: (215) 238-1700
Facsimile: (215) 238-1968
jkohn@kohnswift.com
dsheils@kohnswift.com
bgibson@kohnswift.com

Attorneys for Plaintiff The Honorable Teresa J. McGarry and for the Proposed Class