Appendix E: OPM

E.1 Introduction

The United States Office of Personnel Management (OPM) "serves as the chief human resources agency and personnel policy manager for the federal government" [48]. Between 2014 and 2015, the OPM suffered from a series of cybersecurity failures that amounted to one of the largest data leaks in US government history. The vulnerability exploits compromised sensitive data for government employees, including information that could be threatening to national security. The exfiltrated data contained personally identifiable information (PII) from over 21 million government employees, including personnel files, detailed information from background security investigations required for security clearances, and biometric fingerprint data. As a government agency, the OPM is highly regulated, particularly by the Federal Information Security Modernization Act (FISMA), and the data it was responsible for was also highly protected.

"Background investigations conducted on these individuals are designed to identify the type of information that could be used to coerce an individual to betray their country" [16]. Ergo, the compromised data could be used to coerce an individual to betray the United States.

The OPM suffered two breaches that compromised the data as a result of multiple, ongoing failures to secure vulnerabilities. Starting in 2005, the OPM "assumed responsibility for the processing and storage of federal background investigation" and had to clear a back-

log of investigations that had impacts on their resources for years to come [16]. In 2013, leadership changed, including a new Director in May and a new CIO (Chief Information Officer) in December. In March 2014 a "significant data breach at the agency" occurred, and despite efforts from the OPM, federal authorities, and outside cybersecurity companies, vulnerabilities were exploited until May 2015. The breaches in 2014 were identified, but security teams were unable to identify the full extent of the exploits, which led to them persisting through 2015, resulting in a second overall data breach. In response to the incidents there was comprehensive regulatory enforcement, including by the US House of Representatives and federal agencies, as well as a successful class action lawsuit against OPM and its software vendor, KeyPoint. OPM provided credit data monitoring for affected victims and reformed their cybersecurity efforts as a result of the incident.

This case is extremely valuable to investigate because of its scale, the involvement of regulators, and, especially, the cyclical nature of the incidents themselves. This case is comprised of two separate but related incidents, each with their own precursors and outcomes. Following the first incident, there were dedicated response, recovery, and remediation efforts. However, they were inadequate, and a second breach occurred, resulting in further actions and outcomes. The precursors to each incident are important factors, and there is effectively double the amount of data to analyze before and after the incidents. Afterwards, the consequences shaped data security and privacy, particularly in the federal government, as we know it today.

These vulnerabilities and failures, as well as their outcomes, are detailed in a 241-page report from the 7 September 2016 US House Oversight and Government Reform Committee, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation* led by Representative Jason Chaffetz. This report is valuable for its forensic detail, and it is referenced heavily in this analysis. There are other artifacts used for analysis, and the report does not document all of the events pertinent to the case.

However, it includes details that are not found elsewhere, clarifies key information, and has reliable data such as testimony from individuals involved in the incidents, and results from investigations by the House of Representatives and other government agencies.

E.2 Cyber Social Context

The cyber social context comprises the environments for the stakeholders before a cybersecurity incident. In this case, the software producer, the Office of Personnel Management (OPM) implemented technology to manage employment data for end users including government employees, and deployment users such as other government agencies. As a government agency, and due to the protected nature of the data, the OPM is regulated by a wide-ranging regime, including oversight by Congress. User data included PII and sensitive background investigation information as well, and end users are represented by organizations like labor unions, as well as privacy advocates.

E.2.1 Software Producer

The software producer in this case is the OPM, a federal agency that supports other federal agencies' human resources needs. Their role includes managing employment data for millions of people, mainly government employees, including background checks for security clearance. This is highly sensitive data, and of keen interest to threat actors. The OPM, as well as other federal agencies, had been under threat from attacks for many years prior to the incidents that began in 2014. Their oversight comes from a variety of rules enforced by internal and external regulators within the federal government.

Operational Environment

According to the Government Accountability Office, in 2017, the OPM was the

> central human resources agency for the federal government, overseeing all policy to support federal agencies' human resources departments—from classification and qualifications systems to pay, leave, and benefit policies. In addition, the agency provides investigative products and services for more than 100 federal agencies to use as the bases for suitability for employment and security clearance determinations ... It also provides more than 95 percent of the government's background investigations, conducting approximately 2.2 million investigations a year. The agency had a fiscal year 2016 discretionary budget authority of about $245 million and around 5,300 full-time equivalent employees.

[52]

The product for background investigation was known as the Personnel Investigations Processing System (PIPS), which at the time included "approximately 15 million records of investigations conducted by and for OPM, the Federal Bureau of Investigations, the US Department of State, the US Secret service, and other customer agencies" [16]. Starting in 2004, this service fell under OPM's Federal Investigative Services (FIS) division after it was moved from the Department of Defense through an act of Congress. This was a significant increase in scale of their mission as an agency, although it fell within their typical operations. To manage this, OPM worked with a variety of contractors, including KeyPoint (which was later absorbed by a company known as Peraton) and US Investigations Services, LLC (USIS), both of which also performed background investigations. USIS was formerly an office of OPM but was privatized in 1996 [14]. They also relied on cybersecurity technology from vendors and other federal agencies, such as US-CERT, to maintain the data security of their products.

The transition of the background investigation services led to a backlog of applications

which took years to clear. By 2008, audits began to indicate that the OPM was suffering from weaknesses that could compromise their security [16]. In particular, the supervision of these operations fell under both the OPM Director and the Office of the CIO (OCIO), which includes both a CIO and a CISO at the helm. In 2009 there were leadership changes, including a new Director. However, there was an 18-month period where a permanent Senior Agency Information Security Official went unfilled. Audits from the Inspector General continued to highlight deficiencies in the cybersecurity operations of the agency, including PIPS, in 2010, 2012, and 2013 [16]. In 2013, both a new Director, Katherine Archuleta, and CIO, Donna Seymour, were installed just months prior to the first incident. Archuleta discussed addressing cybersecurity issues in her Senate confirmation hearing, including modernizing IT [16].

As described in the next section, this era of cybersecurity operations for federal technology producers was typified by "playing catchup" according to a subject matter expert [2]. New best practices, requirements, and technologies were being put in place, and OPM in particular was dealing with antiquated systems that needed to be secured.

Regulatory Environment

The OPM is governed by a variety of regulators both internal and external, mandated by a handful of laws and rules. Internally, their most important stakeholder is probably the Inspector General, who at the time was Patrick McFarland, who had held the position for 26 years before resigning in 2016. The IG as an internal watchdog was codified in law in the Inspector General Act of 1978 to "provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies" in federal agencies and is responsible "not to any individual, but to the public interest" (Chaffetz, 2016; IG Act of 1978). It was his audits and memoranda that since 2009 had

announced issues with cybersecurity at the agency. The Office of the Inspector General (OIG) is tasked with supporting law enforcement authority and investigation, is meant to be an integral part of incident response, and has oversight for contractors and procurement, according to OPM's own internal rules [16]. At OPM there is also a Management Review Board, which includes the CISO, Deputy CISO and other leaders, that supports managing information security risks (GAO, 2016).

Externally, the regime under which the OPM operates, specifically regarding its security, is most closely tied to the Federal Information Security Modernization Acts of 2014 and 2002 (FISMA). This law "is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets" (GAO, 2016). It includes requirements for agency leaders regarding security protections, as well as agency-wide cybersecurity programs. It is the law that requires agencies to comply with NIST standards, and authorizes a central security incident center, the DHS US-CERT (GAO, 2016). FISMA audits within OPM are conducted by the OIG, and are required at least every year for overall security controls, and at least every three years for systems in operation in order to be authorized to operate (ATO). Additionally, the Federal Information Technology Acquisition Reform Act has implications for security, and uses a "scorecard to assess agencies' implementation of this law" [16].

As a federal agency, OPM is also subject to oversight from Congress, including the Committee on Oversight and Government Reform, which in 2016 was chaired by Representative Jason Chaffetz. There are also multiple examples of guidance and directives from other responsible agencies, such as the Office of Management and Budget (OMB).

Employees of the federal government also have protections that OPM must comply with, such as those established by unions. There are a variety of unions that represent government employees, including the American Federation of Government Employees

(AFGE) and the National Treasury Employees Union (NTEU) among others. In recent years, unions have started to include data privacy and security as part of their portfolio of protections for their members, which also benefits other non-union employees as well when employers implement those protections.

Threat Environment

Since at least 2005, federal agencies have been under threat from Advanced Persistent Threat (APT) attacks, which focus on high-value targets and physical systems. This includes agencies that hold sensitive employee information, as well as their contractors. OPM itself was breached in 2012 when a database was compromised and user IDs and passwords were stolen. By the time of the breaches in 2014, "[t]he threat of APTs was well-known throughout the federal government and OPM was a prime target given the sensitive information it held on current and former federal employees and contractors" [16]. Between 2009 and 2014, the number of cybersecurity incidents at federal agencies involving PII more than doubled, reaching 27,624, among over 67,000 total incidents reported in 2014, according to the US-CERT [51]. The cybersecurity vulnerabilities at OPM were also well documented in audits for years.

In fact, OPM contractor USIS encountered a sophisticated breach in 2013 that was similar to what OPM would later experience [16, 35]. USIS at this time was a company providing background investigations services for OPM, but it was previously an office within the agency before being privatized in 1996.

The PIPS system used to handle background investigation itself stored information gathered from the SF-86 form, described as "some of the government's most valuable PII" as it requires disclosure of "intimate and potentially embarrassing aspects of a person's life" [16].

In general, OPM should have been very familiar with the threats they faced, and many of their security staff and contractors were. However, their capacity to implement the required practices were documented as lacking.

E.2.2 Regulators

There is a network of regulators that support the regime in this case. Federal agencies, the legislature, internal regulators, and third-party organizations all contribute to the rule-making process, and the enforcement of those rules. They have a wide range of experience, but many are highly focused on cybersecurity because of the sensitivity of the data at the OPM.

Regulatory Environment

In 2005, there were two major initiatives that kicked off years of regulatory action and a growing regime that governed federal software security. One was the US-CERT Technical Cyber Security Alert that put all agencies on watch. The other was the Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12), which set years of cybersecurity action in motion. In 2002, Congress passed FISMA and updated it in 2014. FISMA required agencies to manage their own systems and authorized other agencies to support broader cybersecurity functions [13, 16, 51, 51].

Courts also offer important safeguards for victims of data breaches. In an Amicus Curiae brief filed during the class action lawsuit following the breach, EPIC, a privacy advocacy organization, highlighted cases like *NASA v. Nelson* in 2011, which supported the right to privacy regarding employment records collected by the government following a data breach [11].

Operational Environment

The network of regulators is strongest at the federal level, as many agencies worked together to establish and enforce a regime of cybersecurity regulations. Agencies like the Department of Homeland Security and its US-CERT, the Office of Management and Budget, Government Accountability Office, as well as Congress, and the President were all active in cybersecurity operations for federal software and IT systems. There was near constant activity in supporting cybersecurity efforts beginning around 2005, when the threat of APTs became clear.

Much of the operational activity, and authorization to do so, had been at the hands of two agencies, OMB and DHS at this time. The OMB, for example, issued multiple rounds of guidance and directives, including support for implementation of HSPD-12 [16, 51]. Additionally, FISMA authorized OMB to oversee and monitor agency implementation of security requirements, provide operational and technical assistance, as well as enforcement. In 2014, FISMA was updated to authorize DHS to support OMB in their efforts [13, 51].

Given the seriousness of threats and severity of incidents, it seems that enforcement of cybersecurity requirements was not effective enough in the years leading up to the OPM breach. The OMB Annual FISMA report in 2013 showed agencies' heterogeneous levels of compliance with the law, and while OPM seems to report that they were making progress in cybersecurity compliance, the results do not seem to support their self-assessments [26]. Across all of these reports, year to year, the overarching theme is that there is always more to do to secure federal software systems, regardless of the measures in place. Even in 2020, a GAO report was released, titled "Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity" [15].

Threat Environment

The threat environment for regulators specifically refers to their familiarity with the threats that they are responsible for mitigating through regulations. In this case, regardless of operational capability or capacity, it is clear that these agencies were intensely familiar with the vulnerabilities that needed to be addressed by their constituent software producers. Each agency had an immense repository of knowledge and support mechanism to address threats from APTs starting at least in 2005. DHS with support from US-CERT and OMB with technical capacity from NIST showed clear knowledge of the issues at hand. However, they may have lacked some capacity to enforce compliance to meet the increasing threat from APTs.

E.2.3 Users

In this case the users are comprised of two categories, the government agency deployment users of OPM's personnel systems (especially PIPS), and the employee end users whose data was managed in those systems. Deployment users were largely regulated under the same regime as OPM with regard to cybersecurity and protection of employee PII. End user personnel, whose PII was compromised in the breach, would also have regime protections, engaged with the software, and had advocacy organizations helping represent them during situations like these data breaches.

Regulatory Environment

Information about personnel is protected as PII, and employers, including the federal government, are required to keep it secure. OPM carried information not only about their own employees, but at other agencies as well. Data including Social Security numbers,

residency and education history, employment history, information about immediate family and other personal and business acquaintances, criminal and financial history, job assignments, performance ratings, training information, and fingerprints, were all required to be secured by OPM, but were later compromised [16, 51].

Deployment users of the OPM software are likely to be required to use OPM's services and products as government agencies, and probably were protected from any adverse behaviors by OPM for which they could not be held accountable.

Threat Environment

The scale and sensitivity of the data about these employees made this a very risky threat environment. This high value data, in a centralized system, is a clear target, and had been sought after on many occasions by APTs [35]. End users had no way of advancing their security protections through the OPM software, so their familiarity was largely irrelevant. Deployment users also were not responsible for any critical actions to improve security in their use of the OPM software, other than following standard procedures.

Operational Environment

The heterogeneous practices of the deployment users, that is the various ways in which they need the OPM software, increased the variety of data being stored by OPM, and increased its value. For example, when OPM took over the background investigation data through its PIPS software, this increased the level of risk. Agencies that relied on OPM to manage its biometric fingerprint information also increased the value of the data. Not all agencies used the software for the same purposes, but overall every agency used the system for a variety of purposes related to personnel management.

End users include government personnel and job applicants who would have used the

OPM software for HR purposes, in particular, background checks. These end users would have entered various data such as tax, healthcare, and retirement information on a regular basis. Additionally, those completing background security checks would have used the software directly to answer questions and submit supporting documentation that would have been required for their roles.

Advocacy groups were active in attempting to protect employee data at this time, including privacy organizations like EPIC, as well as unions like AFGE and NTEU. These civil society groups were available to support personnel that were affected by incidents like the OPM data breach.

Ultimately all the data that was at risk at the OPM was furnished by its users because they were required to use OPM's software to perform their duties and meet their needs as government employees.

E.3 Operating & Precursors

Analysis of the operating behaviors and precursor states of the stakeholders in this incident are weighted heavily towards the software producer and regulators. The investigation by Chaffetz et al (the House Oversight Committee) provides detailed information about the actions preceding the incident, and regulatory participation at this stage was also very involved. While users were going about their normal business, the OPM and its regulators were in constant motion, including some friction, which presaged the massive data breach that occurred.

This case is also distinguished by its dual incidents, which offers two stages of antecedent factors, those that led up to the first breach, and the responses to it, which then become the operations and precursors that led to the second breach. While they were thoroughly connected, they do appear to be two individual incidents to analyze. This is

valuable for several reasons, but mainly because it clearly illustrates examples of behaviors that failed to address key issues after a breach and immediately resulted in another.

E.3.1 Software Producer

OPM went through a variety of changes in the decade leading up to the breach, including taking over the responsibility for managing security clearances for government employees following the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). This legislation, partly a response to the attacks of 9/11, sought to address a backlog of security clearances necessary for government personnel and contractors [16, 21]. This added thousands of staff to OPM's office, and further needs to process clearances more quickly drastically altered the business processes at OPM. During this time, cybersecurity failures began to appear, with multiple documents detailing the specifics.

Human Resources in the Federal Government

The Office of Personnel Management was created as part of the Civil Service Reform Act of 1978 to "oversee federal workforce management." They were preceded by the Civil Service Commission which was created in 1883 [49]. OPM's duties include programs typical of any HR department, including retirement, healthcare, diversity and inclusion, and supporting hiring and employee management practices. In addition, it has some unique responsibilities, including the on-and-off-again processing of security clearances and background investigations, or Personnel Security Investigations (PSI) [3, 41, 44].

The management of PSIs at OPM has a confusing timeline. From the 1970s, the task was split between the Department of Defense and the OPM. In 1996, the office of the OPM that handled PSI was spun off into a private company called US Investigative Services (USIS). Throughout all this time, the PSI function was chronically delayed, underfunded,

and understaffed. According to Clearance Jobs, a private job board, delays in processing clearances cost the government $920 million per year in lost productivity [3]. By 2004, the backlog for contractors had reached over 188,000, and the average processing time was 375 days [16, 21].

In 2004, Congress passed the IRTPA which required under Title III that all PSIs be consolidated into one agency, the OPM, both to improve performance for processing and for security reasons. This resulted in migrating the DoD's Defense Security Service, including their 1,850 employees, to OPM's Federal Investigative Services division (FIS). At the time, OPM had about 3,000 employees, 170 of whom worked on PSIs, including managing external contractors (such as USIS) that supported processing clearances [22]. To meet the needs of the government, the goal was to reduce processing times to within 60 days and potentially expand OPM's staff to over 7,500 by 2009 [16, 21]. Following these changes in operations, they may have met their business needs, by 2012 they reduced the average initial investigation to 36 days, and raised the workforce headcount to over 9,000 people internally and externally [21]. However, criticism about their approach exploded when two events, the leaks from Edward Snowden and a shooting attack at the Navy Yard, led to concerns that the government may have "heedlessly prized speed over quality [21]. Crucially, the focus on processing times may have given way to capacity issues in complying with cybersecurity best practices.

According to the House Oversight Committee's report, starting in 2005, the Office of the Inspector General began identifying security weaknesses that were included in reports to Congress. This persisted under three directors until the breaches, Linda Springer, John Berry, and Katherine Archuleta. At Berry's confirmation hearing, Congress asked specifically about managing the PSI caseload, but did not ask about information security, although he did testify later about the need to upgrade security practices shortly thereafter [16]. During this time, the OIG's reports indicated issues with cybersecurity leadership, including

unfilled positions for key roles, issues with the authority of the OCIO to "manage security matters effectively," and security officers that had limited experience in information security, as well as a lack of "fully documented information security policies and procedures," all of which threatened the capacity of OPM to secure its implementation of services [16]. By the end of FY2013, concerns about OPM's internal compliance, capacity, security, as well as their budget, had been thoroughly documented. At this point, a FISMA audit by the IG revealed a more specific threat to the PIPS software, which supported the PSI function, including its interfaces with other software applications. The report explicitly referred to security controls that were never tested. [16].

This FISMA audit was released just as the new Director, Katherine Archuleta, and the new CIO, Donna Seymour, were being onboarded in 2013. They immediately announced that in their first few months, they would release a "Strategic Information Technology Plan" as a key artifact to improve security and compliance operations. They released this plan on time in March 2014, at which point they discovered the first data breach. Seymour testified before Congress in June 2014 about the plan, but, crucially, did not mention the data breach [16].

While budget limitations were highlighted and are likely a factor in the ability to enhance cybersecurity, the 2012-2014 Congressional Budget Requests (CBJ) from the office of the CIO did not vary widely. For 2014 (released in April 2013) the CIO request was just over $51m, for 2013 (released in 2012) was $53.3m, and for 2012 (released in 2011) it was $52.3m [37–39]. Starting with the CBJ report for 2016, after the first incident had been mitigated, and while the second one was underway, the CIO request seems to have increased to $77m [43]. It is important to note that these requests may not account for all of the OCIO's budget authority. Regardless, the House Oversight report indicates that data from the OMB shows that OPM consistently spent less than other agencies on cybersecurity, and affirms that the 2016 budget request was "too little, too late" [16].

Unaddressed Failures and Weaknesses Part 1

Courtesy of the House Oversight Committee investigation, and other artifacts included therein, we have thorough details of the specifics of the unaddressed failures and weaknesses at OPM that preceded the breach, including technical, management, leadership, and compliance breakdowns. The report titles one of the sections on these shortcomings "OPM Failed to Prioritize the Security of Key Data and Systems" [16].

The investigation, including details from US-CERT, the OIG, and other experts, concluded that OPM had not appropriately implemented multifactor authentication, encrypt critical data, properly authorize 11 of their 21 systems, or implement access-control capabilities, among other issues, all of which were required for regulatory compliance and data security best practices [16].

Multifactor authentication would have best been implemented with Personal Identity Verification (PIV) through cards for staff to access software and data. However, an OMB report in 2015 reported that OPM was one of the "weakest" in implementing such a system, with only one percent of staff required to use them [16]. These failures included the ability for a hacker to pose as an employee for contractor KeyPoint, which was the first step in exploiting the vulnerabilities within OPM's network in the second breach, despite efforts to secure their systems following the first breach [16].

The authorization of their systems is a requirement that should result in a Security Assessment and Authorization, or ATO, to operate their IT systems and help prevent security breaches. In particular, among the systems without proper ATOs were PIPS, the Enterprise Server Infrastructure, and the Local Area Network/Wide Area Network (LAN/WAN), all of which were critical weaknesses that led to the data breach being so extensive [16]. The PIPS system "is a mainframe application on the OPM environment that stores the background investigation information provided by employees and prospective employees on

forms SF-86, SF-85, and SF85P" [16].

Unaddressed Failures and Weaknesses Part 2

A new phase of operations began after the activities and outcomes resulting from the first breach, which was eradicated 27 May 2014. The correcting activities and transformations (discussed in later sections) included working with a new network of vendors and procuring new software to support security. These can be considered cyclical inputs back into operations activities like implementing and securing, resulting in precursors such as business change and capacity, as well as unaddressed failures and weaknesses.

Note: If you prefer to follow along chronologically, skip this section, and return after you have completed Section 3, Incident and Impacts, and Section 4, Recovery and Outcomes.

The procurement of new security software starting in June 2014, such as those by a company called Cylance, were met with "bureaucratic hurdles" and led to OPM purchasing a product that could detect, but not prevent, malicious behavior, despite that feature being readily available. Disagreements between different technical teams went unaddressed, leading to the procurement decision. Additionally, there were compliance issues with their ability to purchase the software to improve their capacity: Cylance did not have the correct approval through FedRAMP to supply federal agencies. However, this did not stop OPM from purchasing the limited version of their software, only the more advanced version. They claimed that although they had already broken the rules, they did not want to continue breaking them by making the additional purchase [16].

Eventually, once the upgraded tools were implemented around April 2015, including Cylance, as well as CyTech and Websense, all indicated that a second "severe attack" was underway. At this point, OPM was working with a network of "interagency partners,

government contractors, and private sector incident responders" to manage the incident. It is during the analysis of the second breach that OPM and these partners discovered that compromised login credentials from PSI contractor KeyPoint (Peraton) were the culprit for the installation of a sophisticated set of malware.

Compliance Behaviors

Particularly following the second breach, but also in response to the first, OPM's compliance behaviors regularly conflicted with the expectations of their OIG. The OIG described four situations where the OCIO did not "cooperate fully" which indicates a weak adherence to regulations prior to the breaches. The House report includes these four examples as reported by the OIG in a memorandum of concern to the new Director, Beth Cobert, in July 2015: failure to appropriately notify the IG of the April 2015 intrusion detection, failure to notify the OIG of the loss of background investigation data in a timely manner, failure to notify the OIG about the 2014 incident, and meetings with federal law enforcement agencies (which included multiple accusations of interference by the OCIO in the OIG's required participation with such meetings) [208].

As this case is cyclical, these compliance behaviors, and others, will be detailed again in the RRR section. This is because while they were in part Operations and Precursors to the second breach, they also demonstrate a pattern of weak compliance after the breaches.

E.3.2 Regulators

As discussed, the involvement of regulators both internal and external in the cybersecurity of OPM was quite thorough. Data from a variety of artifacts including scholarship and government documents detail a variety of rulemaking and enforcement actions that resulted in a comprehensive regime governing OPM and a strong capacity to respond to

issues. However, it seems that some of the capacity to respond with action was limited, as although regulators were able to identify the issues, they persisted, and adequate changes were not made to prevent the data breaches.

My analysis has already included mentions of a variety of legislation and case law that is pertinent to this case, and there are even more. Federal regulators created new agencies, mandated structural changes to existing agencies, created guidance, supplied support resources, and more all in the name of improving cybersecurity for the federal government and national security. Suffice it to say, this demonstrates a very active rulemaking environment, and strict regimes, particularly with the regulators that are externally responsible for OPM. However, the enforcement capabilities of the regulators may have been lacking in ways that could have prevented the OPM breaches. Federal authorities at this time did not have as strict methods for compelling agencies to comply as they did with conducting oversight and rulemaking.

Internally at the OPM, the OIG, whose responsibilities extend beyond just investigating cybersecurity issues, requested budgets of $25m - $26m for fiscal years 2013 – 2015, a meaningful amount of money to carry out their duties [38–40]. As required by law, the OIG submitted both its Semiannual Reports and annual FISMA audits, which were included and cited extensively in the House Oversight investigation. Again, we see active internal regulatory operations and strict regimes. The OIG also began active observation and documentation of OPM's compliance behaviors following the first data breach, which resulted in some formal reprimands later on, including a memorandum of concern regarding the CIO on 22 July 2015.

Courts were also very active in deciding on protections for privacy violations like those suffered by the OPM data breach. Cases like TransUnion v. LLC v. Sergio L. Ramirez and NASA v. Nelson, despite their heterogeneous outcomes, all demonstrated the growing importance of privacy litigation [11, 12, 20].

E.3.3 Users

The users affected by the data breach include over 22 million people who suffered unauthorized access to and theft of their data. A portion of these people include users whose especially sensitive security background clearance data was affected. As current, former, and prospective government employees, these users submitted their information to the OPM system so that their employers could rely on OPM as the central human resources agency for federal employers.

The number of users participating in the PSI system was so large that the demand for budget and staff to address it was a constant struggle [21]. This change in operational needs both for the employers that deployed the software, and the end users submitting their data, is what helped drive the shift to consolidating PSI processing to one software provider.

The capacity of these users to protect their privacy and secure their data was limited, and was primarily, if not entirely, under the control of OPM. In fact, compared to other industries that manage data on general consumers, the federal government has a strong national security interest in securing this data, as demonstrated by the strict regime they have in place.

However, privacy advocacy for employees does exist in civil society, outside of the federal employment network. This advocacy helps enhance the capacity of government employees as software users to protect their privacy. In particular, privacy advocacy groups and unions have the resources to help ensure these users can pursue compensation for harms, primarily through litigation. While not all employees are members of unions, class action lawsuits can still provide for other people who might have been affected by privacy breaches. While these groups can also help support security hygiene best practices, in this case, those efforts would have done nothing to improve security because the data breach was not influenced by the security behaviors of the employees themselves, only those of

the software producer. However, their ongoing efforts, particularly in privacy litigation, is a key element of users' capacity to help ensure that data privacy and security regulation continues to be active.

E.4 Incident and Impacts

The anatomy of the data breach and its immediate impacts are, per usual, detailed very thoroughly in the House Oversight Committee report, based on detailed documentation, testimony, and expert input from actors involved in the data breach. This is comprehensive information that would be difficult to find elsewhere in this case, and impossible to find in similar data breach cases, especially those in the private sector. In general, it would be impractical to find such a level of detail for research purposes.

E.4.1 The First Breach: 2014

On March 14, 2014, OPM was notified by US-CERT that data had been exfiltrated from OPM systems. This would have kicked off first a detection & analysis phase, followed by a containment, eradication, and recovery phase, based on the NIST Incident Response Life Cycle, which is the cybersecurity guidance document for federal agencies [25].

Within a week of detection, OPM, DHS, FBI, and NSA cybersecurity teams began to document and address the issue, and by March 25 they had made a " 'full determination on the who and what' of the data breach, to know where the hackers are 'going, what they are seeing,' and most importantly 'what [the hackers] are interested in" [16]. As they observed that the attacker was interested in the PIPS system, the outside cybersecurity teams also became aware that OPM had severely limited security measures, including their ability to secure that system. These security limitations included the use of a legacy mainframe and lack of use of PIV/multifactor access controls. The incident also indicated that OPM may

not have been able to observe other behaviors by the attackers, and US-CERT reported that attackers had access since 2012. Other exfiltrated documents also included details (manuals) about OPM's software which would help hackers to gain and maintain access for nefarious purposes.

Once they had fully analyzed the "tactics, techniques, and procedures" of the attacker, they were ready to begin eradicating and remediating in a process they called "Big Bang," which also included outside security firm Mandiant [16]. This phase concluded on May 27, 2014.

In June, following the eradication of the threat, US-CERT issued an Incident Report with recommendations based on their observations throughout the process. US-CERT's involvement, as well as that of other cybersecurity teams, is not simply part of the cybersecurity capability of the software producer, they also have a regulatory responsibility, as demonstrated by the use of their documentation in the Oversight Committee's investigation.

E.4.2 The Second Breach: 2015

While the first breach unfolded, attackers set the stage for another breach a year later, infiltrating a part of the OPM system that could not be monitored adequately. In fact, details from cybersecurity exports indicate that the attacks were "likely connected, possibly coordinated" [16]. In the first breaches, the data stolen included overviews of various systems and the people who had access to those systems, which would have been useful for future attacks, and "could explain the speed with which the 2015 attacker was able to establish access, orient themselves, escalate network authorities, and penetrate the most highly sensitive data repositories on OPM's network" [16]. Ultimately, following the attempted remediation of the first breach, attackers were still able to exploit vulnerabilities, and continued exfiltrating through spring 2015. They were discovered on April 15 and the incident

was disclosed in June and July, 2015.

The second breaches were largely discovered as OPM began the expansive corrections to their security situation after the first breach. Upgrades to their cybersecurity software began to indicate new malicious behavior. When they received a product demo from a potential contractor, the software immediately indicated a swathe of vulnerabilities actively being exploited. Between April 15 and April 25, software updates improved their ability to identify and analyze the threats, detecting incredibly dangerous tools like Trojan viruses. They were able to quarantine the exploits on April 24. After this, they realized that since June 23, 2014, attackers had unauthorized access to the OPM mainframe, which included background investigation data. Files were exfiltrated in part through access to outside servers, with surreptitious names like "opmsecurity.org" and "opm-learning.org" to hide their behaviors.

From April to August 2015, OPM worked to collect forensic information about the attacks, which suffered some setbacks, while the disclosure of the breaches reached national news.

E.5 Response, Remediation, and Recovery

Following the first breach, there was a massive undertaking to recover and remediate the insecure systems. Regulators became involved heavily at this point, including Congressional testimony from OPM leadership. Following the second breach, similar efforts were made, as well as major changes to leadership, and new legislation to again split the PSI system between OPM and another new agency.

E.5.1 Software Producer

Following the incidents of spring 2014, OPM began activities to correct their "very insecure, insecurely architected network" based partly on US-CERT's recommendations [16]. To help address this, OPM contracted with a handful of outside companies to enhance their security measures. However, US-CERT's observations also described concerns with leadership that led to the security issues, not just technical problems. Meanwhile, their efforts were later shown to fall short, as a second breach was imminent. Additionally, OPM leadership's reporting to Congress regarding the incidents also added to their problems.

Follow-up to the second breach was more severe, including compensation for affected users, formal complaints about leadership, leadership changes, and ultimately establishing entirely new federal agencies to manage the software systems. In fact, to the extent that the OPM data breach is well-known, it is primarily the second breach that the public is familiar with.

Security Through Procurement

In June 2014, CIO Donna Seymour began a new project with an outside company to improve OPM's software, focused on four phases: securing the legacy IT environment, creating a new data center and IT architecture, migrating all legacy IT to the new architecture, and decommissioning legacy hardware and systems. As part of this process, they pursued additional contracts to expand their capabilities, including with Cylance and CyTech, as well as updates to other services with vendors like Websense. The House Oversight report includes intricate details about this process, including internal documents and even some colorful language used by the vendors that is expected in difficult situations like this, but normally impossible to get hold of.

The involvement of these outside companies was rife with issues as they began to grap-

ple with the situation at OPM. In 2014 OPM purchased a tool from Cylance called V, a detection tool. However, due to "internal bureaucratic hurdles" (see Section E.3.1) they did not purchase the additional software package called Protect, which would have helped prevent malicious activity, not just detect threats once they are already in place [16]. OPM's security teams also upgraded their existing product, Websense. It was upon implementing these two tools, in April 2015, that they became aware of the second breach.

Problematic Posturing and Concerning Compliance

As part of their regulatory compliance requirements, OPM's leadership regularly reported to Congress, among other reporting duties. In June 2014, CIO Donna Seymour testified before Congress about the Strategic Information Technology Plan developed with Director Archuleta over the first few months of her tenure. However, Seymour at this juncture did not bring up the data breach and remediation efforts that had occurred just weeks before. In a later testimony, they also misled Congress about the nature of the data that had been stolen [16]. The House Oversight Committee also documented "five incorrect and/or misleading statements to Congress" regarding the data breaches and the security state of OPM.

Later, when information about some of the security operations with the contractor CyTech were published in The Wall Street Journal, there was also some dispute about the nature of CyTech's involvement, which OPM seemed to try to diminish. OPM's effort to deny CyTech's involvement went as far as testimony to Congress in which both Archuleta and Seymour denied the involvement of the company in the detection of the second breach, which appears to be objectively false [16].

Of note are the OIG's required Semiannual Reports to Congress for April 1 2014 – September 30, 2014 (during the first breach) and October 1, 2014 – March 31, 2015 (im-

mediately prior to detection of the second breach). The first report stated that they "did not detect any instance of non-compliance with regards to the major categories of FISMA requirements reviewed" and in the second report, they noted some opportunities for improvement, specifically for OPM to seek active Authorizations (ATOs) (OPM OIG, 2014; OPM OIG, 2015). In addition to the OIG's Semiannual Reports to Congress, the agency is also required to prepare a "Management Response" for that reporting period. In the same reporting periods (Apr – Sep, 2014; Oct 2014 – Mar 2015), the Management Responses did not mention the data breaches [42, 45].

Only in the April 1, 2015 – September 30, 2015 Management Report by OPM, following detection of the second breach, were the breaches mentioned. In the next report (through March 31, 2016), it was also omitted [46, 47]. The OIG Semiannual Report continued to address the breach and cybersecurity concerns in later reports [29]. This corresponds with the House investigation and the testimony given by IG McFarland, in which he stated that the OCIO "failed to provide timely notification concerning the breach" in 2014, and that he was actually notified by another agency [16]. He also testified that his notifications for the 2015 breach were accidental [16]. In short: OPM was lackluster at best in required disclosures about their data breaches.

It seems worth noting that the first 2014 Management Response report was the earliest report available via the OPM website, but also coincided with the breach, fortunately for my data collection. However, the OIG Semiannual Reports go back to 2000.

The posturing maneuvers here, to deflect some of the issues, are in some ways typical of software producers that suffer a breach. However, when it comes to Congressional testimony, and reporting to the OIG, it would seem that OPM were being noncompliant with their governing rules.

Following these Posturing and reporting incidents, it appears that OPM was able to get increased resources to meet cybersecurity requirements. According to interviewee O005,

they eventually "made the case" for how they were understaffed and underfunded, and convinced congress and the Obama administration to increase resources for them and other agencies [2]. This coincided with the broader campaign to improve federal cybersecurity, such as the 30-Day Sprint, described later.

"Failure to Cooperate"

What fits into my model under Compliance Behaviors following an incident, may not be strictly legal terms per se. Instead, such behaviors were officially documented as a "failure to cooperate fully" and "incorrect or misleading statements" by the OCIO [16]. The House report includes four examples of this as reported by the OIG in a memorandum of concern to the new Director, Beth Cobert, in July 2015 : failure to appropriately notify the IG of the April 2015 intrusion detection, failure to notify the OIG of the loss of background investigation data in a timely manner, failure to notify the OIG about the 2014 incident, and meetings with federal law enforcement agencies (which included multiple accusations of interference by the OCIO in the OIG's required participation with such meetings). These were discussed briefly in the Operating & Precursors section, but I will include more details now.

The first compliance concern was in response to the first breach. The OIG's Special Agent in Charge (SAC) testified in Congress that the OCIO did not notify the IG of the first breach in a timely manner and that it was not "in keeping with OPM policy and rules governing notification to the OIG." The SAC also testified that they only learned of the detection of the 2015 breach by accident when they ran into a colleague in a "chance encounter." In a similar situation, the SAC also testified that they only learned about the loss of background data in another "right place at the right time situation" (Special Agent Testimony in [16]).

Lastly, the IG, Patrick McFarland, and the SAC both stated that OPM's OCIO violated the terms of the Inspector General Act by preventing the OIG from participating in law enforcement support for incident response. In 2014 when the OIG was trying to investigate a breach of OPM contractor KeyPoint, the OCIO delayed the investigation for over three months. Then, in 2015 when the FBI and US-CERT were working on response measures, OPM Director Archuleta tried to delay and/or prevent the OIG from participating, as required by law [16].

Compensating

The OPM provided voluntary compensation for victims through identity theft monitoring. Following a successful class action lawsuit, they were also required to pay up to $63 million in damages to affected individuals.

Credit monitoring services have been provided by companies that suffered data breaches both voluntarily and by court order [152]. In August 2015, OPM worked with the Defense Department to award a contract to ID Experts (later called IDX) to provide credit monitoring, identity monitoring, and identity restoration services to individuals affected by the breaches [18]. Those services lasted for 10 years and are scheduled to close to new enrollments for the OPM breach in 2026, although the government also uses IDX to handle identity theft monitoring for other government breach victims, costing the government tens of millions of dollars per year [23]. IDX reported in 2019 that it had enrolled millions into its system, responded to millions of calls, and issued "over a hundred million routine credit and identity monitoring alerts" [17].

Additionally, OPM was required to pay up to $63 million as the result of a settlement agreement following a lawsuit on behalf of the victims [4, 19]. However, due to the terms of the settlement, only about 7% of the total fund was claimed, around $4.8 million. This

money was distributed to over 5,000 individuals, among the 22 million total victims and 27,000 who filed claims. While victims could claim up to $10,000 for harms directly attributable to the breach, proving those harms can be difficult, which may explain the low expenditure compared to the settlement total sum. In early 2025, the case was closed and the remaining balance returned to the Treasury Department [19].

E.5.2 Regulators

Regulatory actions were heavy-handed in this case. Multiple agencies took impactful actions and cooperated closely with each other to respond. The courts were also involved following class action litigation that required appeals before deciding in favor of the plaintiffs.

Federal Executive & Legislative Regulatory Response

Regulators had been involved in the incident through cybersecurity partners like US-CERT, as well as internal bodies like the OIG. However, involvement soon expanded to Congress and the GAO following the first and second breaches. Ultimately the House Oversight and Government Reform Committee, chaired by Jason Chaffetz, launched a full investigation including multiple hearings, and released a scathing report. The Committee report included important data that would have been nearly impossible to obtain otherwise such as previously redacted information, testimony from key individuals, unreleased internal documents, and email messages.

The OPM Office of the Inspector General was heavily involved in compliance efforts following the breaches, although, as discussed earlier, they were also thwarted at times by OPM staff. They conducted extensive investigations and enforcement efforts as part of their mandated duties and supported corrective measures by OPM like implementing new

security policies and procuring additional resources.

The GAO also conducted investigations and issued reports with information critical to understanding the regulatory compliance behaviors of OPM before and after the breach. The GAO released a 2015 Testimony to the House of Representatives Committee on Homeland Security about OPM's data breach and broader concerns with government cybersecurity, and a 2017 Report about OPM's improvements following the 2014 and 2015 breaches [51, 52]. The 2017 report is titled "OPM Has Improved Controls, but Further Efforts Are Needed" and discusses multiple remediation behaviors that needed to be completed, and/or were not handled properly. The report states that OPM had 19 recommendations from US-CERT to improve their cybersecurity practices, but at that point had only completed 11. The GAO concluded that OPM had not "consistently updated milestones for outstanding US-CERT recommendations or complied with its own plan for conducting periodic control assessments" and "key security controls on selected contractor-operated systems have not always been comprehensively tested" [52].

The Senate Financial Services and General Government Subcommittee also held a hearing on data security at OPM on June 23, 2015, which included testimony from Director Archuleta, Assistant IG Michael Esser, and an expert witness in the cybersecurity field [36].

On June 12, 2015, the Obama Administration announced a "30-Day Cybersecurity Sprint" along with OMB and DHS, a whole-of-government effort to "further protect Federal information and assets and improve the resilience of Federal networks" [32, 34]. The sprint involved pushing federal agencies like OPM to correct shortcomings and introduce monitoring methods, which they would then report to OMB and DHS at the end of the 30 days for evaluation. The recommendations for correcting activities included "dramatically accelerating implementation of multi-factor authentication" including PIV cards, "tightening practices for privileged users," and "patching critical vulnerabilities without delay"

[34]. These recommendations match verbatim some of the failures detailed in the OPM data breach case, and the effort was directly linked [28]. Following the sprint, both the status and progress of agencies' actions were assessed and resulted in recommendations documented in a 2015 memorandum from the OMB, as well as a $1.4 billion proposed budget increase to improve cybersecurity [27, 28, 32].

Eventually, these investigations required regulators like the OIG and House of Representatives to posture themselves against OPM for their failures through critical statements. And, ultimately, they moved beyond posturing into punishment enforcement actions, including calls for the Director and CIO to resign [8] and the IG's memorandum of concern to that effect [16]. Director Archuleta resigned in July 2015 and was replaced by former OMB Director Beth Cobert as Acting Director. During Cobert's tenure, calls continued for CIO Donna Seymour to resign, and she eventually retired just before the House Oversight Committee hearing in February 2016 [7].

Judicial Involvement

The court decisions following the lawsuit brought by unions representing the victims of the breach were important, in part because the plaintiffs received a settlement, but also because the initial complaint was dismissed, then overturned.

Initially, the lawsuit filed by the NTEU and AFGE unions representing victims of the breach entered the U.S. District Court for the District of Columbia. However, there are issues in data privacy breach litigation around the country regarding what is called Article III standing. Article III is a legal rule that determines whether a plaintiff has standing to sue in court, based on three elements: they have suffered an "injury in fact"; the injury is fairly traceable to the challenged action of the defendant; and it is likely, not merely speculative, that the injury will be redressed by a favorable decision. This rule has been

identified as a key factor in data privacy litigation and is a determining factor in the success of plaintiffs in such cases, although it presents a "tricky conundrum" [1, 12, 20]. This case was no different, except that it was initially dismissed for lack of Article III standing but was granted on appeal in the US Court of Appeals for the District of Columbia Circuit. This led to the $63 million settlement agreement between the plaintiffs and OPM. This reversal is not necessarily consistent with decisions in other cases, so while it does not definitively amend the current regime, it could have implications for future litigation.

E.5.3 Users

Users primarily got involved following the second breach, mainly through representation from the NTEU and AFGE unions, and support from a privacy advocate, the Electronic Privacy Information Center (EPIC). The most prominent action was their class action suit against OPM and their vendor, KeyPoint (now known part of Peraton). But they were also involved in supporting compensation through credit monitoring at OPM's expense by submitting testimony to the Senate's hearing on OPM [4, 24] .

The plaintiffs, along with the NTEU and AFGE sued OPM and Peraton in the DC District Court. First, the case was dismissed, but that decision was later reversed on appeal. In support of that appeal, EPIC and the US Chamber of Commerce provided input through amicus curiae briefs in favor of the plaintiffs, and advocating for improved data security [9, 11]. Eventually, they won up to $63 million, of which about $4.8 million was eventually claimed.

Interestingly, there were two quantitative studies of the emotions of people affected by the OPM data breach using Twitter (now X) as its data source. The authors published first in 2017 then again in 2022 using a slightly different approach, both times focusing on aggregate emotional responses to the data breach over time. Both papers described feelings

of anger, anxiety, and sadness [5, 6]. The more recent paper added context, and categorized concepts from the tweets to include "lack of agency and control in data breach responses," "decrease of citizen trust in secure digital operations," and "lack of security governance" among others [6].

E.6 Outcomes

The consequences, including a wide variety of Response, Recovery, and Remediation Behaviors after these incidents included some drastic and widespread Outcomes. Major changes to the PSI process include the introduction of a new agency, the NBIS. Furthermore, new cyber enforcement capacity was introduced, including new agencies and regulations. Leadership changes at OPM include a new Director and a new OCIO. Improvements for users are less clear, but, as has been shown, the security requirements for federal agencies to protect such data were already in place, and it was largely a series of compliance failures that led to the breach.

E.6.1 Software Producer

The outcomes from the RRR behaviors led to important transformations and a variety of costs. Between the first and second breaches, their compliance behaviors and security behaviors were partly preserved, but that changed drastically after the second breach, as the visibility and implications of their failures grew in scope, scale, and publicity. Ultimately, the scandal caused by the breaches led to the high-profile resignations of both the Director and the CIO within a year of the second breach.

According to USA Spending.gov, OPM has awarded over $725 million to Identity Theft Guard Solutions, Inc. (known as IDX and ID Experts) for credit monitoring and identity theft protection services since 2016 [50]. They also paid victims $4.8 million as part of the

lawsuit settlement.

In 2014, the OCIO total discretionary resources were $51 million, including $7.6 million for salaries and expenses. In 2023, the OCIO total discretionary resources were $107 million, including $44.9 million for salaries and expenses. The cost of doing business for the OCIO has roughly doubled. However, this includes non-security-related work, but it does show an increase in investment. Additionally, the OPM no longer handles all of the same software, as the background investigation work moved to the Defense Counterintelligence and Security Agency (DCSA) in 2019. In 2023, the DCSA OCIO budget was $59.5 million [10]. It would seem that the DCSA is doing more with less money for data security, but that is not exactly clear, as the overall budget for OPM is around $427 million and DCSA is close to $1 billion.

It is difficult to understate the scope of the changes that OPM was required to make over years to improve their software security. This included 19 critical recommendations from DHS including documentation, personnel changes, technical improvements, technology upgrades, continuous monitoring, overseeing contractor-operated systems, and more [52]. These were incredibly stringent requirements that required a high level of diligence to complete and were supervised closely by regulators.

E.6.2 Regulators

Outcomes for regulators were varied, they largely preserved their role as enforcers and responsible authorities, but introduced new mechanisms for enforcing regulations, as well as some new rules. They forced their constituent software producers to improve their software security across the board as well. The costs to do all this work would certainly be substantial, both in terms of money and human resources. Billions of dollars and uncountable hours spent.

Executive & Legislative

Through the aggressive enforcement of regulations, it is clear that legislative and executive agencies, as well as the House of Representatives, preserved their mandate to continue to enforce regulations by software producing agencies. The GAO and House Oversight Committee were diligent in investigating and bringing OPM into compliance after the breaches, and remediating the security issues that had befallen them. The GAO enforcement also continued to demonstrate the effectiveness of the network between their partners in the DHS, like US-CERT, as well as resources from NIST, and OMB. They supported the OMB in its ability to enforce FISMA regulations, and, later, supported the development of recommendations stemming from the Cybersecurity Sprint.

According to the interview with O005, the shifts in agency responsibility also included more power for regulators to enforce cybersecurity standards and practices, particularly under the authority of the Cybersecurity and Infrastructure Security Agency (CISA), such as through their Continuous Diagnostics and Mitigation Program [2]. The subject explained that while cybersecurity efforts had been ramping up, CISA now had better authority to enforce these practices. These new, more powerful enforcement mechanisms include the Binding Operational Directives and Emergency Operational Directives [2].

Executive responses went even further, either directly or indirectly connected to the OPM breach. On 4 June 2015, the Director of National Intelligence, James Clapper, openly attributed the attacks to China, when placing blame was a rare move [30]. His comments, surprisingly, also showed that he was impressed with the magnitude of the attack. Around the same time, Secretary of State John Kerry proposed introducing a "code of conduct" for state behaviors in cyberspace (BBC, 2015). Additionally, In April 2015, President Obama signed an Executive Order to give the Department of the Treasury the ability to sanction hackers for threats to national security [30]. While no sanctions were imposed for the OPM

breach, the authority has been exercised in other cases.

Judicial

As discussed earlier, the lawsuit brought by the victims was initially dismissed, then overturned in circuit court. While this result is comprised of multiple judicial decisions that require legal theory beyond the scope of this research to understand fully, there are some observable outcomes to note. First, a lawyer writing for The Lawfare Blog, states that while "No two data breach incidents are entirely alike, and given the fact-intensive nature of the standing inquiry, it's difficult to draw decisive conclusions from any single decision ... the majority's opinion suggests that the courtroom doors may be open for plaintiffs ... Without further guidance from the Supreme Court, the D.C. Circuit's approach is likely to influence both litigants and judges in the inevitable lawsuits to come" [33]. This indicates a possible transformation to judicial enforcement in data privacy and security litigation. A somewhat contrasting opinion is that while this may not open a door for other successful lawsuits, at the very least it preserves the complexity in deciding such cases as it "did not help clarify how lower courts should evaluate whether data breach plaintiffs have standing in the future" [1].

Another interesting component, on which I cannot ascribe any legal theory, was in the dissenting opinion to overturn the initial decision, a judge said that identity theft was not likely to occur because of the nature of the hack, which was for espionage [1].

E.6.3 Users

The outcomes for users were limited, although ideally future harms against users will be mitigated from similar attacks. Regardless, those that were affected, particularly government personnel whose background investigation data was compromised, will be at risk

for years to come. Especially anyone who is actively involved in national security for the US.

Compensation was limited, although some individuals were able to collect compensation for direct harms, and those that may have suffered the most economically should have been able to recover the most money thanks to the court settlement, $700 for certain claims, and up to $10,000 for direct costs. That being said, the settlement was almost a lost cause when the case was initially dismissed. Credit monitoring protections could have helped as well, although that is also a cost to the users that now needed to adopt it. Additionally, as noted by a judge, likely the primary reason for the attack was likely not identity theft, but espionage.

Deployment users that relied on the OPM FIS system migrated to the replacement National Background Investigation Services, managed by the DCSA starting in 2019. This too would have had some costs associated with it, but it is unlikely that the existing system with OPM would have remained the same for much longer, and even the NBIS system has been upgraded in that time, as any software would and should, to meet the needs of its users and producers.

E.7 Aftermath

The OPM case had wide-reaching implications for the federal government and US cybersecurity efforts, including in industry. Going forward, the regulatory, threat, and operational environment for stakeholders was substantively altered. This is observable due to the response behaviors by all stakeholders, and their outcomes. This aftermath was driven by new awareness of gaps in enforcement mechanisms, new methods of cooperation to address data privacy and security, and the perception of the critical nature of the incident.

E.7.1

E.7.2 Gaps in Enforcement Mechanisms

In the OPM case, the precursors to the 2014 and 2015 breaches included multiple years of findings by external and internal regulators of failures to comply with cybersecurity regulations. While cybersecurity efforts by the US government, including regulations for federal agencies, had been ramping up for years before, following the OPM breach, there were massive efforts to close gaps in regulations from both the executive and legislative branches. This includes The Computer Information Sharing Act of 2015 and updates to FISMA in late 2014. These acts introduce new enforcement mechanisms for federal agencies, such as Binding Operational Directives and Emergency Orders, which are issued by CISA and "They serve as powerful instruments for standardizing the approach to information security, driving the government to be more responsive and vigilant" as they are enshrined in law [31]. This results in changes to the operational and regulatory environment for regulators and software producers, who have new regimes to comply with.

E.7.3 New Methods of Cooperation

In the OPM case, the legislation that passed soon after the disclosure of the breach, particularly the Computer Information Sharing Act of 2015, established new methods of cooperation to support regulatory enforcement. This act improves the ability of federal agencies to collect and share information about cybersecurity threats to better respond to them by providing an avenue for private companies to submit cybersecurity information. Furthermore, following the breach, the role of CISA to support cooperation between federal agencies continued to increase, including the introduction of more enforcement capabilities, and taking over the oversight role from OMB. This has implications for the threat en-

vironment, particularly the regulators' and software producers' familiarity with the threats. As well as the operational environment, improving capacity for software producers to secure their systems.

E.7.4 Critical Characteristics

In this case, the response from federal agency leaders appeared to be a realization that they could not simply rely on the technical teams, and that they would have to lead with cybersecurity in mind or face national security consequences, if not their own jobs. The data that was compromised could have national security implications at a very high level, and future incidents could also face the same threats.

E.8 Case Bibliography

Bibliography

[1] In re U.S. Office of Personnel Management Data Security Breach Litigation. *Harvard Law Review*, 133(3):1095–1102, January 2020. Recent Case.

[2] Interview with participant o005, 2026.

[3] The brief history of the security clearance process. ClearanceJobs, n.d. Source file: The Brief History of the Security Clearance Process.pdf.

[4] American Federation of Government Employees. Statement for the record regarding opm information technology spending and data security, June 2015. Source file: afge-data-breach-testimony-6-23-15.pdf.

[5] Eric Bachura, Rohit Valecha, Rui Chen, and H. Raghav Rao. Data breaches and the individual: An exploratory study of the opm hack. In *ICIS 2017 Proceedings*, 2017. Source file: Data Breaches and the Individual_ An Exploratory Study of the OPM.pdf.

[6] Eric Bachura, Rohit Valecha, Rui Chen, and H. Raghav Rao. The opm data breach: An investigation of shared emotional reactions on twitter. *MIS Quarterly*, 46(2):881–910, 2022. Source file: OPM Data Breach Investigation of Shared Emotional Reactions on Twitter.pdf.

[7] Aaron Boyd. Opm cio seymour resigns days before oversight hearing. *Federal Times*, February 2016. Source file: Boyd - OPM CIO Seymour resigns days before Oversight hearing.pdf.

[8] Jedidiah Bracy. 21.5 million breached in second opm hack; director resigns. *IAPP*, 2015. Source file: Bracy - 21.5 Million Breached In Second OPM Hack; Director Resigns _ IAPP.pdf.

[9] Chamber of Commerce of the United States of America. Brief of amicus curiae the chamber of commerce of the united states of america, 2018. Source file: US Chamber Amicus Brief.pdf.

[10] Defense Counterintelligence and Security Agency. Dcsa op-5. Technical report, Department of Defense, n.d. Source file: DCSA_OP-5.pdf.

[11] Electronic Privacy Information Center. Brief of amicus curiae electronic privacy information center (epic) in support of appellants, May 2018. Source file: in-re-opm-EPIC-amicus.pdf.

[12] Ellis Fenske, Christopher W Brown, and Jeff Kosseff. Courting consensus: How class

action lawsuits shape data privacy rights and obligations in the us. In *Proceedings of the 23rd Workshop on Privacy in the Electronic Society*, pages 172–185, 2023.

[13] Zachary Figueroa. Time to rethink cybersecurity reform: The opm data breach and the case for centralized cybersecurity infrastructure. *Catholic University Journal of Law and Technology*, 24(2):433–467, 2016. Source file: Figueroa - Time to Rethink Cybersecurity Reform.pdf.

[14] Amruta Gayathri. Usis that vetted snowden under investigation overlooked snowden resume discrepancies. *International Business Times*, n.d. Source file: USIS That Vetted Snowden Under Investigation Overlooked Snowden Resume Discrepancies _ IBTimes.pdf.

[15] Carol C. Harris. Information technology: Agencies need to address shortcomings in modernizing legacy systems. Technical Report GAO-20-691T, U.S. Government Accountability Office, 2020. Source file: GAO - Harris 2020.pdf.

[16] House Committee on Oversight and Government Reform. The opm data breach: How the government jeopardized our national security for more than a generation. Technical report, U.S. House of Representatives, September 2016. Source file: The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[17] Identity Theft Guard Solutions, Inc. U.s. office of personnel management awards id experts identity protection services contract, n.d. Source file: IDX - U.S. Office of Personnel Management Awards ID Experts Identity.pdf.

[18] Eric Katz. Government awards $133m contract to protect 21.5m victims of opm hack. *Government Executive*, September 2015. Source file: Government Awards

$133M Contract to Protect 21.5M Victims of OPM Hack - Management - Government Executive.pdf.

[19] Eric Katz. Feds claims just 7% of available funds from opm breach settlement, remainder returns to treasury. *Government Executive*, January 2025. Source file: Feds claims just 7% of available funds from OPM breach settlement, remainder returns to Treasury - Pay & Benefits - Government Executive.pdf.

[20] Jeff Kosseff, Chris Brown, Ellis Fenske, and Don Needham. Not easily dismissed: The growing importance of data breach litigation in cybersecurity. *Boston University Journal of Science & Technology Law*, 30:189–222, 2024.

[21] Rebecca LaFlure. How congress screwed up america's security clearance system. *Foreign Policy*, October 2013. Source file: How Congress Screwed Up America's Security Clearance System – Foreign Policy.pdf.

[22] David McGlinchey. Opm set to absorb defense security clearance agency. *Government Executive*, n.d. Source file: OPM set to absorb Defense security clearance agency - Government Executive.pdf.

[23] Jason Miller. Opm bringing protections for data breach victims to an end. *Federal News Network*, October 2025.

[24] National Treasury Employees Union. Opm renews contract for protecting data breach victims. 2025. Source file: OPM Renews Contract for Protecting Data Breach Victims - National Treasury Employees Union - NTEU.pdf.

[25] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, and Karen Scarfone. Incident response recommendations and considerations for cybersecurity risk management: A

csf 2.0 community profile. Technical Report NIST Special Publication (SP) 800-61r3, National Institute of Standards and Technology, Gaithersburg, MD, April 2025.

[26] Office of Management and Budget. Fiscal year 2013 annual report to congress: Federal information security management act. Technical report, May 2014. Source file: fy_2013_fisma_report_05.01.2014.pdf.

[27] Office of Management and Budget. Memorandum m-16-04: Cybersecurity strategy and implementation plan (csip) for the federal civilian government. Technical report, Executive Office of the President, October 2015. Source file: OMB CSIP - GOVPUB-PREX2-PURL-gpo114663.pdf.

[28] Office of Management and Budget. State of federal it report: Cybersecurity. Technical report, 2016. Source file: 02.05.cybersecurity.pdf.

[29] Office of the Inspector General. Semiannual report to congress: October 1, 2015 – march 31, 2016. Technical report, U.S. Office of Personnel Management, 2016.

[30] Damian Paletta. U.s. intelligence chief james clapper suggests china is suspect in cyber hack. *Wall Street Journal*, June 2015. Source file: WSJ James Clapper.pdf.

[31] Kat Samiljan. Binding operational directives guide federal agencies through maze of cybersecurity. *Government Technology Insider*, January 2024.

[32] Tony Scott. Strengthening and enhancing cybersecurity for the 21st century. CIO.gov, n.d. Source file: Scott - Strengthening and Enhancing Cybersecurity for the 21st Century _ CIO.GOV.pdf.

[33] Benjamin Sobel. Recent decision: D.c. circuit rules that opm breach victims have standing to sue. *Lawfare*, n.d. Source file: Sobel - Recent Decision_ D.C. Circuit Rules That OPM Breach Victims Have Standing to Sue _ Lawfare.pdf.

[34] The White House. Fact sheet: Enhancing and strengthening the federal government's cybersecurity, 2016. Source file: FACT SHEET_ Enhancing and Strengthening the Federal Government's Cybersecurity _ whitehouse.gov.pdf.

[35] ThreatConnect Research Team. Opm breach analysis: Update. Technical report, ThreatConnect, June 2015. Source file: OPM Breach Analysis_ Update _ ThreatConnect.pdf.

[36] United States Senate Committee on Appropriations. Hearing on opm information technology spending and data security, June 2015. Source file: Hearing _ Hearings _ United States Senate Committee on Appropriations.pdf.

[37] U.S. Office of Personnel Management. Congressional budget justification fiscal year 2013. Technical report, U.S. Office of Personnel Management, 2011.

[38] U.S. Office of Personnel Management. Congressional budget justification fiscal year 2013. Technical report, U.S. Office of Personnel Management, 2012.

[39] U.S. Office of Personnel Management. Congressional budget justification fiscal year 2014. Technical report, U.S. Office of Personnel Management, 2013. Source file: opm_fy_2014_cbj_final_v4__pickens___4-09-13__-_to_print_v2__1_.pdf.

[40] U.S. Office of Personnel Management. Congressional budget justification fiscal year 2015. Technical report, U.S. Office of Personnel Management, 2014. Source file: opm_fy_2015_cbj__master__3_09_14_855pm_final.pdf.

[41] U.S. Office of Personnel Management. Fy 2013 annual performance report. Technical report, U.S. Office of Personnel Management, 2014. Source file: 2013-annual-performance-report.pdf.

[42] U.S. Office of Personnel Management. Semiannual report response: October 2014. Technical report, Merit System Accountability and Compliance, 2014. Source file: sar-response-oct-2014.pdf.

[43] U.S. Office of Personnel Management. Congressional budget justification fiscal year 2016. Technical report, U.S. Office of Personnel Management, 2015. Source file: congressional-budget-justification-fy2016.pdf.

[44] U.S. Office of Personnel Management. Fy 2014 annual performance report. Technical report, U.S. Office of Personnel Management, 2015. Source file: opm_2014_apr_v15_508.pdf.

[45] U.S. Office of Personnel Management. Semiannual report response: April 2015. Technical report, Merit System Accountability and Compliance, 2015. Source file: sar-response-april-2015.pdf.

[46] U.S. Office of Personnel Management. Semiannual report response: October 2015. Technical report, Merit System Accountability and Compliance, 2015. Source file: sar-response-oct-2014.pdf.

[47] U.S. Office of Personnel Management. Semiannual report response: April 2016. Technical report, Merit System Accountability and Compliance, 2016.

[48] U.S. Office of Personnel Management. About us, n.d. Source file: About Us - OPM.pdf.

[49] U.S. Office of Personnel Management. Mission & history, n.d. Source file: Mission & History.pdf.

[50] USAspending.gov. Federal awards: Advanced search results for identity theft guard

solutions, inc., 2025. Source file: Federal Awards _ Advanced Search _ USAspending.pdf.

[51] Gregory C. Wilshusen. Cybersecurity: Actions needed to address challenges facing federal systems. Technical Report GAO-15-725T, U.S. Government Accountability Office, 2015. Source file: gao-15-725t.pdf.

[52] Gregory C. Wilshusen and Nabajyoti Barkakati. Information security: Opm has improved controls, but further efforts are needed. Technical Report GAO-17-614, U.S. Government Accountability Office, 2017. Source file: gao-17-614.pdf.