Global Information Assurance Certification Paper

An Approach to Reducing Federal Data Breaches

GIAC (GSEC) Gold Certification

Author: David Thomas, david.thomas@pcmg.com
Advisor: Dr. Kees Leune
Accepted: 10 May 2016

Template Version September 2014

Abstract

In 2015, The United States Office of Personnel Management (OPM) publicly disclosed a loss of 21.5 million Americans personally identifiable information (PII). What are the lessons learned from this breach and can other federal CIOs use these lessons within their own organization to prevent a similar loss of PII? An open source chronological timeline of events is presented leading up to the 2015 OPM disclosure and post disclosure events. The critical security controls (CSCs) that applied to the OPM breach are evaluated to demonstrate how each one could have reduced the risk of a breach or the scale of the breach. A practical application of an open source hashing tool is offered to the reader to implement within their organization. The result of reviewing the events that led to the OPM disclosure, the evaluation of the CSCs, and implementation of a practical approach can reduce the risk of another federal organization experiencing a breach similar to OPM.

1. Introduction

In July of 2015, The United States Office of Personnel Management (OPM) disclosed a series of data breaches, collectively referred to as the OPM data breach, that exposed the personally identifiable information (PII) of more than 20 million of American citizens (Bisson, 2015). The OPM not only collect's the PII of those who apply for a security clearance, but those of their family, friends, and coworkers. The loss of PII of an applicant and those closely related to that person makes this breach different from other high-profile breaches. To better understand how this PII became exposed the actions or inactions taken by the various OPM chief information officers (CIOs) are considered within the context of the support required to the bigger mission of OPM. The OPM CIO is ultimately responsible for supporting the OPM mission; which includes safeguarding the PII entrusted to this agency. A key to understanding the priorities of support given to safeguarding the PII collected by OPM is to review the annual budget requests. These requests give an understanding as to what is important and what is not important to an organization based on the items that receive funding from year to year. Another objective measure considered are the annual Federal Information Security Management Act (FISMA) Audits conducted for OPM. The results of the FISMA audits clearly documented the significant risk OPM posed to the current operations and safeguarding of the PII stored within their databases. The lack of budget for IT security and the results of the FISMA audits clearly document the lack of attention given to safeguarding the PII held by OPM.

The applicable Critical Security Controls (CSCs), published by the Center for Internet Security (CIS), that could have been used to reduce the risk of the breach are reviewed. Of the twenty possible CSCs, the author evaluates the applicable CSCs and argues for a deeper consideration as to why three of them would have been instrumental in preventing or significantly reducing the scale of the OPM breach. Other well-known and practical IT security concepts are compared for their applicability in reducing the risk of The OPM breach. Given the known facts of the OPM data breach, these well-known approaches are eventually reduced to one. Free to use open source tools are presented to support help support the implementation of this approach. From the various arguments

and open source tools presented in this paper, other federal CIOs have the potential to reduce the risk or significantly reduce the scale of a future breach.

1.1. Mission of OPM

To understand a governmental organization, first consider their mission statement. OPM's mission is to "recruit, retain, and honor a world-class workforce to serve the American people" (OPM, 2014). OPM is one of several US Federal government agencies authorized to retain the PII created during the course of the background check. OPM (2016a) "provides human resources, leadership, and support to federal agencies and helps the federal workforce achieve their aspirations as they serve the American people." Leaders from within OPM direct the efforts of OPM's personnel by focusing them on four "pillars" that directly support the mission. The fourth pillar is the key to understanding why OPM gathered such the PII of millions of Americans. OPM defines this pillar as, "We assist Federal agencies in hiring new employees, provide Federal investigative services for background checks…"(OPM, 2016a). More importantly, OPM keeps PII of those that have applied for a security clearance, the PII of the numerous individuals interviewed on behalf of these applicants, and those with an approved security clearance necessary to access secret or top secret information. OPM receives a substantial amount of information per application. To keep up with the demand required to create, search, and evaluate each potential candidate OPM contracted several companies to assist them during this time. Two of the most notable companies contracted by OPM include The US Investigations Services (USIS) (Gough, 2014) and KeyPoint (Sternstein, 2015).

1.2. CIO Efforts to Support OPM

For almost twenty years OPM entrusted three CIOs with the responsibility of safeguarding the PII of millions of Americans. The first CIO of OPM was the Honorable Janet Barnes. According to the OPM (2016b) biography, her tenure started in 1996 and lasted thirteen years. As the first CIO, she supported OPM's mission through numerous efforts focused on increasing the efficiency of the organization. OPM's second CIO, Matthew Perry, served 25 years in the United States Army before eventually taking over the role of CIO in February of 2010 (CIO.GOV, n.d.). During his three years at OPM

Perry made efforts to focus on saving OPM money. Perry (2011) noted his accomplishment to push services to the cloud and how this effort would save OPM hundreds of thousands of dollars per year. Perry was the first to focus on IT security as CIO at OPM; though the impacts of these efforts are not clearly documented in the annual budget requests. OPM's third CIO, Donna Seymour, started her tenure in July of 2013 (US, OPM, 2014) and ended less than two years later. Of the three OPM CIOs, Seymour's vision is the clearest as to how she will support the mission of OPM and incorporate IT security. In her first 100 days, she published this vision incorporated in The OPM's Strategic IT Plan (US, OPM, 2014). 95% of the total pages written clearly focused on supporting the mission of OPM compared to the reminder which focused on IT security.

1.3. OPM Priorities by the Numbers

James Frick (Wei, 2016), the director responsible for soliciting donations for Notre Dame University for nearly 30 years, once "Don't tell me what your priorities are. Show me how you spend your money and I'll tell you what they are." Using this insight, the author downloaded from the OPM website the available fiscal year (FY) budget requests, available to the public, starting in FY 2007 and ending FY 2017. FY, followed by a calendar year, denotes a US Federal calendar year that begins on 1 October and ends on 31 September. These budget requests are written in the prior FY and request financial resources deemed necessary by OPM to support the agency's mission in the next FY. Each line item in the FY budget request lists a resource name and an amount requested. According to James Frick, by reviewing OPM's budget requests it is possible to understand what the agency valued from one FY to another FY.

In order to understand the importance of IT security, each budget was opened and a simple search for the terms "IT security", "Cyber", and "security software maintenance" was conducted. Appendix A includes a complete list of instructions and a graphical representation of the results. The total count of each return was added together and the aggregate of these results are referred to as "IT Security Terms Mentioned."

The results of this search did not yield any references to any of the IT Security Terms Mentioned for FYs 2007 through 2010. Starting in the FY 2011 budget request,

the words "IT security" were mentioned five times, dropping to three times in FY 2012 and then again dropping to only to two times in FY 2013. Starting in FY 2014 the budget request increased the count of "IT security" to four occurrences and for the first time mentioned "Cyber"; twice. This rate of occurrence of IT Security increased in FY 2015 to four times and Cyber increased to three times. Following the disclosure of the OPM breach in July of 2015, the FY 16 budget request references to the IT Security terms tripled. The FY 2017 budget request almost doubles the previous year's mention of IT security terms.

Appendix B includes an analysis of the explicit IT Security budgets found in the FY budget requests. Except for the ambiguous references made in FY 2011 through 2015, this simple comparative analysis yielded predictable results. The total IT Security Terms Mentioned were then correlated to the amount of money explicitly noted for the IT Security budget. As the number of IT Security Terms Mentioned increased from one FY so did the size of the IT security budget request. The largest request for IT security funding occurred after the disclosure of the OPM breach in FY 2015. In FY 2016 (US, OPM, 2015) an additional $21,000,000 was explicitly requested to support "security software maintenance." In FY 2017 (US, OPM, 2016) increases the IT security budget request by an additional $16,000,000.

1.4. Annual FISMA Audits by Office of Inspector General

Mark Twain wrote, "The best predictor of future behavior is past behavior" (Yaniga, 2015). Another key to understanding an organization's past behavior are the metrics used to evaluate them. Michael Esser, Assistant Inspector General for Audits, included the following background information in each of the audits FISMA Audits conducted to measure OPM's IT security posture:

> On December 17, 2002, the President signed into law the E-Government Act (Public Law 107- 347), which includes Title III, the Federal Information Security Management Act (FISMA). FISMA requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies" (Esser, 2012).

Michael Esser (2012) further went on to explain, “At OPM, security responsibility is assigned to the agency’s Office of the Chief Information Officer (OCIO). FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.” The publically available FY 2012-2015 FISMA Audits reveal serious gaps in IT security almost every audit. Esser (2012) reported these gaps in IT security starting in FY 2007 and continuing through FY 2013 in the various FISMA audits authored in his report.

Esser (2012) believes these gaps led to the loss of several smaller disclosures of PII prior to the 2015 OPM breach. Incredulously the acting OPM CIO Matthew Perry refuted Esser’s FISMA report of OPM losing any PII during that year. Esser (2012) responded to Perry with the following statement, “Contrary to the OCIO’s statement that there was no financial or PII loss in FY 2012, there were, in fact, numerous information security incidents that led to the loss or unauthorized release of mission-critical or sensitive data. Several of these security incidents were reported by the media.” Several news articles corroborate Esser’s account of events when compared to Perry’s account of the same events. These smaller incidents lead to the 2015 OPM breach. Following the disclosure of the OPM breach, numerous politicians and news agencies lambasted OPM because of the “audits by the Office of the Inspector General had found systemic weaknesses in OPM’s security infrastructure…" (Fisher, 2015). Michael Mimoso (2015), a journalist covering the OPM data breach, noted, "The results of the FISMA audit come down hard on OPM in a number of areas…”

1.5. Open Source Compromise Timeline

David Bisson (2016), a writer for the online website Tripwire, published an article that eloquently arranged the key events that led up to the breach and the events that followed it shortly after:

March 2014, "Chinese hackers infiltrate the OPM’s computer systems, presumably to collect information on federal employees who had applied for top security clearance in the past. The agency informs federal, state, and local government officials

that they were able to thwart the attack using intrusion detection "systems (IDS) installed on its network, which leads the Obama administration to believe that no personally identifiable information was compromised by the incident. No mention of the attack is therefore made to the public" (Bisson, 2015).

June 2014, "The United States Investigation Services (USIS) discloses a breach of 25,000 government employees' personal information to the OPM and sends out a memo on June 17 (2014) notifying 15 large federal agencies of the intrusion" (Bisson, 2015). In the wake of this disclosure, Christian Davenport (2014) noted in his article, published in the *Washington Post*, the decision by OPM not to renew their contracts with USIS in September of 2014.

9 July 2014, "The New York Times runs an article that reveals the OPM attack for the first time to the American public" (Bisson, 2015). A month after this notification, "Multiple news outlets report on the USIS June breach, with the contractor reportedly having stated that the intrusion "has all the markings of a state-sponsored attack." By this time, the DHS has also suspended all contracts with the USIS, and the Federal Bureau of Investigations has commenced an investigation into the incident" (Bisson, 2015).

September 2014, "Federal investigators detect a data breach affecting KeyPoint Government Solutions, a provider of investigative services for the U.S. government. It is believed that as many as 390,000 current and former DHS employees, contractors, and even job applicants may have had their private data compromised by the intrusion" (Bisson, 2015).

4 June 2015, "U.S. officials reveal the breach of the OPM's computer systems to the public and state that the agency will begin sending out notifications to 4 million former and current federal employees warning them that their personal information might have been compromised" (Bisson, 2015). Followed shortly by "Officials close to the investigation uncover a second breach that is believed to have compromised computer systems containing information related to the background checks of former, current, and prospective federal employees, suggesting that the OPM breach is likely much larger than originally expected" (Bisson, 2015).

9 July 2015, "The OPM concludes its investigation of the breach it discovered in June of 2015 that affected its background check systems and reveals that 19.7 million individuals (as well as 1.8 million non-applicants, including spouses and partners) were affected by the incident. This is in addition to the 4.2 million people whose information was compromised in the personnel data breach that was discovered back in April of the same year" (Bisson, 2015).

1.6. Technical Details of the Breach

At this time, the exact technical details of how the breach occurred are not fully known to the American public. Evan Perez and Shimon Prokupecz (2015) attribute KeyPoint credentials were used to gain access to the OPM database. Fisher (2015) wrote, "The details of the OPM breach, scant as they are at the moment, paint an ugly picture of the security practices inside the agency." Mimoso (2015) noted, "11 of its systems are operating without valid authorization that certifies that controls meet security requirements for the system in question. OPM has come up short in this area since 2010." It is easy to understand the lack of difficulty an adversary would have in gaining access to OPM's data especially when they have access to valid credentials and eleven systems that are poorly secured. As well as open source documentation in the form of FISMA audits that document a history of poor performance.

1.7. How is this breach different?

The OPM data breach is not the largest data breach according to Nate Lord (2015) the Experian credit check service potentially exposed over 200 million records compared to OPM's 20 million. OPM is not the most expensive data breach in history according to Lori Widmer (2015), she credits the Epsilon Company who exposed the PII of several large companies to a potential loss of $4 billion. Bridget Bowman (2015) credits OPM with only costing the US taxpayers a little over half a billion dollars in the form of credit monitoring services and post-breach services. The OPM breach is different because it exposed the PII of the individuals who are entrusted with a security clearance that allows access to secret and top secret information. This type of information is defined by Executive Order 12356, Fed. Reg., 47, 14874 (1982). Executive Order 12356 (1982) defines "Secret" information as the "unauthorized disclosure of which reasonably could

be expected to cause damage to national security" and "Top Secret" information as the "unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security."

David W. Belangia (2014) noted in his paper as of October 2013 there are over three million individuals who have access to classified information. Any victim of the OPM breach or relation to the victim kept within OPM's database, now has the potential to fall prey to coercion assuming their PII is used against them. Shane Harris (2014) noted the PII collected on those who applied for a security clearance documented their own account of infidelity, drug or alcohol abuse, and crushing debt. Any individual compromised in the OPM breach, who has access to classified information, could have any one, or a combination of negative PII used against them by an adversary of the United States in an effort to gain access to either secret or top secret information. By using coercion to gain access to this information, this would cause damage or exceptionally grave damage to national security. In the terms of the potential loss of human life, agents of the government working abroad in foreign countries now have a much higher potential for compromise because their PII and fingerprints were taken in the OPM Breach (Lesniewski, 2015). Potentially the financial investments made into the secret and top secret programs could fall into the hands of a US adversary negating strategic return on investment.

2. Federal CIOs can Significantly Reduce their Organization's Risk

2.1. Why use the Critical Security Controls (CSCs)

With the numerous evaluation methods available in the market today why use The CSCs? Corey M. Dennis and David A. Goldman (2013) list the various laws Congress has passed to protect PII. Each one of these laws did little to prevent the data breach experienced by OPM. The annual FISMA audits that stem from these laws did not prevent the breach experienced by OPM. The critical security controls (CSCs) that applied to the OPM breach are individually evaluated, and the applicable

sub-controls of those that applied to The OPM breach are further used to explain how they could have reduced the scale and risk of the breach.

According to the CIS (2015) website, these CSCs are a "recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks… In fact, a study by the Australian (Signals Directorate)… indicates that 85% of known vulnerabilities can be stopped by deploying the Top 5 CIS Controls." The CSCs were developed to provide a practical guide to securing an enterprise by a diverse group of security professionals working in government, private, military, civilian and educational organizations. As threats continue to evolve the recommendations are changed to counter those threats and the Center for Internet Security (CIS) publishes the updated recommendations. The strength of the CSCs are in the fact they are continuously kept up to date by a variety of contributors from various IT security backgrounds and supported by an established organization solely dedicated to cyber security. Another advantage of the CSCs are their diversity and adaptability in almost every environment. The CIS publishes this guide and the metrics to measure almost every CSC. These objective measurements enable a vendor neutral approach.

A vendor neutral approach is advantageous as it reduces the ambiguity created by IT security vendors. Competing vendors create different terminology and metrics to describe and measure similar security concepts. Either intentionally or unintentionally these competing concepts and measures create confusion in a technical industry. To negate this problem, The CIS circumvents these ambiguous IT terms and measurements. CIS created the *Measurement Companion to the CIS Critical Security Controls* (CIS, 2015). This vendor neutral approach is critical for objectively measuring the progress and validating the effectiveness of IT security controls. From these objective and tangible metrics, IT security professionals have the potential to demonstrate to their organization's decision makers the effectiveness of the resources they have committed to the IT security efforts.

The intangible benefits of implementing the CSCs could include the confidence felt by decision makers as now they have the ability to grasp something

tangible in IT security. This confidence from an organization's management is crucial before, during, and after an incident. Decision makers have the potential to begin to understand the value of IT security because of the ability to measure security initiatives with confidence. If an incident such as a breach were to occur, these decision makers could present tangible metrics to support their decisions. The ability to defend these decisions based on these metrics is critical to saving an organization's personnel from getting fired; as in the case of the OPM CIO and Director at the time of the 2015 disclosure.

2.2. The Applicable CSCs

The following CSCs were considered as applicable candidates from the list published by the CIS. Further research is recommended for the other CSCs not considered in this paper.

CSC four addresses the "Continuous vulnerability assessment and remediation" (CIS, 2015). Several of Michael Esser's (2012) FISMA document OPM conducted scans of their network, found vulnerabilities, but not remediate them to an acceptable risk level. Dr. Cole (2015), a SANS GSEC instructor with several decades of IT security experience, noted several times in his lecture's that an organization is more effective when they conduct remediation rather than more scans. Each subsequent scan does not produce value from the one previously unless some form of remediation has taken place.

CSC nine elaborates on the "Limitation and Control of Network Ports, Protocols, and Services" (CIS, 2015). Again, the FY FISMA Audits conducted by Esser (2012) detail the numerous insecurities of the OPM networks. These networks had multiple entry points in which an attacker could gain access through and traverse the internal networks. Sub controls of CSC nine would have reduced the entry points and pivot points, but a nation state with enough time and resources would eventually mitigate these measures. Once adversaries overcome these measures they would have access to the data.

CSC fourteen, "The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification" (CIS, 2015). CSC

14.6 and 14.7 could have prevented the breach, but the FISMA audits documented OPM conducted this logging. CSC 14.6 states, "Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data" (CIS, 2015). However, in this specific case, an attacker compromised a legitimate credential and gained access to these critical assets.

CSC nineteen, "Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems" (CIS, 2015). In a heavily redacted memo written by Patrick McFarland (2015), Inspector General working at OPM, noted the OCIO was aware of the breach at KeyPoint but waited a week to report the findings to his office. Any loss of PII should have been immediately reported to him. Instead, the OPM CIO requested a delay in a scheduled audit. According to McFarland (2015) it was only by chance he became aware of the breach at KeyPoint and only at that time could he begin to coordinate with law enforcement organizations. This CSC would not have reduced the breach nor prevented it, but it is indicative of the lack of an overall IT security strategy AT OPM to respond to such a breach.

Based on the open source these CSCs could have applied to the OPM data breach, but it would not have prevented or reduced the scale of the breach. It is the author's opinion to focus on three CSCs that would have the biggest impact in preventing or significantly reducing the scale of breach experienced by OPM. The CSCs that would have the most impact in reducing the risk of a breach at the OPM include CSC thirteen; Data Protection, sixteen; Account Monitoring and Control, and CSC twenty; Penetration Tests and Red Team Exercises. Several of the CSCs may have reduced the risk of the data breach experienced by OPM, but only three would have reduced the scale of the breach.

2.2.1. CSC 13 Data Protection

The CIS recognized the difficulty in preventing access to a network. They recognized the larger return on investment for preventing a breach is to secure the data

from leaving the network. CSC 13 is the most applicable to preventing or significantly a breach on the scale of OPM. CSC 13 (CIS, 2015) focused on “controls should also be put in place to mitigate the threat of data exfiltration in the first place.” The CIS (2015) defined the concept of data loss prevention (DLP) as “a comprehensive approach covering people, processes, and systems protect data in use, data in motion, and data at rest DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.” This CSC would have prevented the OPM breach or significantly reduced the loss of PII to an acceptable level.

Several technical controls developed by CIS (2015) include CSC 13.1 "Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.” A cost analysis of the value of the data or the potential cost of post-breach services would have easily justified the cost of a DLP solution. CSC 13.3 “Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel” (CIS, 2015).

OPM could have significantly reduced the scale of the breach by implementing CSC 13.6. CIS (2015) defined CSC 13.6 as a method “to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them." Building in thresholds would have prevented the scale of the breach even if an adversary had access to valid credentials. Had OPM monitored the network for anomalous traffic most likely would have prevented the exposure of millions of Americans PII.

A known weakness of this CSC includes encrypting the sensitive data before sending it out to the perimeter. The CIS (2015) recognizes “Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system." By encrypting the data, it renders these scanners useless

from preventing the sensitive data from leaving the network. Dr. Cole (2015) recommended creating a rule for firewalls within the network attempting to make an outbound connection resonating from certain hosts inside the network. Given this approach, if a legitimate user were to require an encrypted channel to transfer data they could potentially call a network administrator who could manually allow such a request. If an attacker were trying to create the same encrypted channel automatically their attempts to leave the network would be blocked.

The CIS (2015) created the following three questions to measure this concept: "13.1 How many unauthorized data exfiltration attempts have been detected recently by the organization's Data Loss Prevention (DLP) system (by business unit)? 13.2 How many plaintext instances of sensitive data have been detected recently by the organization's scanning software (by business unit)? 13.3 How many attempts to access known file transfer and email exfiltration websites have been detected recently (by business unit)?" By measuring these questions, a CIO has the potential to demonstrate the effectiveness at preventing the loss of data or justify the DLP policy enforcement.

2.2.2. CSC 16 Account Monitoring and Control

The CIS recognizes the importance of actively managing the accounts that have access to the data. The effort to define, secure, and prevent the data if the accounts authorized to access the data are not properly maintained or monitored. The CIS (2015) recognized the need to manage these accounts, "in order to minimize opportunities for attackers to leverage them." According to the FISMA inspections conducted by Michael Esser (2012), OPM did have a policy to maintain the authorized accounts within OPM's network. Evan Perez and Shimon Prokupecz (2015) wrote in their article for CNN that investigators close to the breach noted valid of KeyPoint credentials were used to gain access to the data stored by OPM. This policy did little to monitor the activities of the KeyPoint credentials credited with accessing the network and exfiltrating the PII of millions of Americans. CSC 16.10 (CIS 2015) advocates that each profile should have a "typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who logged in during unusual hours or

have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works."

CSC 16.11 (CIS 2015) "Require multi-factor authentication for all user accounts that have access to sensitive data or systems." Michael Esser's (2012) report noted the requirement for use of multi-factor authentication by "OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV (personal identity verification) credentials for multi-factor authentication by the beginning of FY 2012… However, as of the end of the FY 2012, none of the 47 major systems at OPM require PIV authentication." According to the report published by Esser (2012), this is the response from the OCIO, "'*OPM has achieved 100% PIV usage for all remote connections and are implementing PIV usage within the OPM population based on its current project plan. OCIO plans to have to achieve 50% compliance by Q3 FY13.*'" If this timeline were accurate, it did little to prevent access to the PII stolen from OPM's database.

The measures, metrics, and thresholds associated with CSC 16 most likely would not have been effective in the case of the OPM because valid credentials were compromised. As the CIS (2015) CSCs included the following questions: "16.1 How many invalid attempts to access user accounts have been detected recently? 16.2 How many accounts have been locked out recently (by business unit)? 16.3 How many attempts to gain access to password files in the system have been detected recently (by business unit)?" However, federal CIOs can add the thresholds necessary to prevent another breach similar to OPM.

2.2.3. CSC 20 Penetration Tests and Red Team Exercises

Trust but verify is a critical concept for those working in any industry. The CIS (2015) uses CSC 20 to advocate for "Red Team" exercises as they "take a comprehensive approach at the full spectrum of organization policies, processes, and defenses in order to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels." Building upon CSC 20 internal Red Team Exercises can assist an organization by helping them understand their gaps in IT security. Furthermore, organizations can conduct no cost internal "sand table" exercises and

leverage the expertise of IT security professionals that the CIS (2015) believe "provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future implementation."

The technical sub-controls developed by CIS (2015) include and applied to the OPM include 20.1 "Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks." Had The OPM management conducted such exercises it could have noted the numerous avenues of approach an outside attacker would have utilized to gain access to the valuable data. From these exercises, solutions could have been derived that would have prevented such attacks. Similar to CSC 20.1, the CIS (2015) developed CSC 20.6 to use "The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts." A good starting point for an internal Red Team could have been the numerous FISMA audits and the numerous scans conducted by OPM of their network.

The CIS Critical Security Control defines one measure: 20.1 "How many technical penetration tests have been performed by external penetration testers recently within the organization (by business unit)?" Again federal CIOs must work with their organizations to understand the value penetration tests and red team exercises bring to the organization. Paul Henry (2015), an IT forensic expert and GIAC GSEC instructor with over twenty years of experience, acknowledges the initial expense in bringing in an outside expert to assist in leading an internal Red Team, but these efforts could eventually transition to the Red Team. Another approach that does not cost an organization money are to leverage the free technical white papers, such as the one written by N. Dean Sapp (2014). He specifically wrote how to gain access to databases. Recommendations, approaches of the attack, and lessons learned are included in the paper written by Sapp (2014).

3. Catching an Adversary

3.1. The right concept

Dr. Cole (2015) stated in his lecture after explaining the CSCs that "Prevention is ideal, but detection is a must." Cole (2015) went on to explain, "If you want to catch a compromised system you have to be able to find anomalies." Based on the guidance of Dr. Cole, it is imperative to create an effective method of detection and monitoring. An effective detection and monitoring solution could have prevented the scale of the breach experienced by OPM.

A senior security professional working within the online gaming industry offered the following solution for preventing a data breach after reviewing the background of the OPM data breach. The security researcher offered the approach of using the concept of least privilege and a technical approach of a proxy server to limit the attack surface for an attacker. In his approach, a proxy server is setup to only allow explicitly permitted requests to the database, the use of RFC 1918 non-routable IP addresses are strictly adhered to, two-factor authentication is implemented, and a separate service put into place to monitor the database requests and flow of data in and out of the database. This approach reduces the number of avenues to available for an attacker to gain access to data.

Furthermore, this senior security researcher advocates the removal of all non-production data to a database that is not connected to any network and would require physical access. The CIS (2015) supports this approach with CSC 14.7, "Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed." A further reduction in the number of potential records exposed, limitations to the number of personal able to access the non-production data and a requirement for physical access creates a significant reduction in risk for any organization.

Why take the advice from an IT professional working in the gaming industry? In his experience, hackers have an affinity to practicing on the gaming networks that are

relatively secure. These same hackers are treated by the public as relatively benign when compared to those that target financial or governmental organizations. These types of attacks, unless financial data is compromised, are seen at worst by the public as an inconvenience to gamers. The gaming industry in stark contrast to this view has spent hundreds of millions of dollars hardening their networks against cyber security attacks. Large vendors such as Microsoft; provider of the Xbox network, Sony; provider of the Playstation network, Riot Games; developer of League of Legends (LoL) and the network to support the game, among hundreds of other developers are investing heavily in security to prevent denial of service attacks, loss of financial information, or other incidents that would prevent investors from investing or users from playing on their perceived unreliable networked games. Notable outages of experienced by these providers include the day after the 2014 Christmas holiday in which both the Sony and Xbox networks were taken down (Rkaina, 2014). The free to play LoL game has experienced numerous outages and Riot Games confirmed a specific incident by an attacker in December of 2013 (Bogos, 2013). These examples are just a few of the high-profile incidents confirmed by these big named vendors. These outages undermine the credibility required to maintain a presence in a highly competitive online gaming industry. Another advantage of targeting gaming networks is they offer a hacker a diverse set of hardware, coupled with a large user base, and the advantage of media credibility without severe reprisals from the public.

The first concept considered by a majority of individuals is to encrypt the database to prevent access to the data. In the case of the OPM data breach, the use of encryption would not have prevented the attacker from gaining access to the unencrypted the data. The compromised accounts allow a user to gain access to the unencrypted data.

Using the idea of a honeypot, retired accounts whose PII was stripped out and replaced with bogus information or specific accounts created as “beacons” was considered. However, given the relatively large number of accounts, it would have been difficult to create these beacons at an effective scale. The return on investment for storing these dummy accounts and the number of false positives would have rendered this solution difficult to implement and manage.

A third consideration a recommendation was made by the senior IT security professional working in the online gaming industry to remove all accounts and records of those that are no longer in the service of the government. Belangia (2014) noted in his paper as of October 2013 there are over three million individuals who would need to have their data kept in this active status. This is a plausible approach and a potential drop in the 20 million Americans who did have their PII stolen, but the exposure time of the remaining active accounts would remain active for the service life of the individual still requiring access to classified information. Potentially some of these accounts remain active for forty years or more.

3.2. The right tool

The WinMD5Free v1.20 hashing tool, presented in the GSEC Boot Camp, is essential to hashing the configuration files of a known good configuration. From this known good hash a change detection tool can be run against them. Any changes that are detected could indicate a compromise of the system. Every configuration file used in a server, firewall, router, switch, etc. could have a known good baseline. The activities required by an attacker would most likely change one or more of the files during the course of an attack.

The WinMD5Free hashing tool is not without its limitations. First, the tool can only create MD5 checksum values. There exists the possibility of creating the exact same hash value from a malicious file created by an attacker. Paul Henry (2015), A SANS instructor and IT forensic expert, confirmed the existence of research that does support the possibility of two files having the same MD5 checksum value. To prevent this problem, Henry (2015) recommend that a hash created by the MD5 hashing algorithm also have a corresponding Secure Hashing Algorithm (SHA) 1 hashes. By using these two different hashing algorithms it is statically infeasible to have two files with the exact same corresponding hashes according to Henry (2015). This approach would significantly lower the probability an attacker is able to successfully modify a file without one of the two hashes matching. It would also provide a backup in the event one of the two tools is unavailable.

The second drawback of using the WinMD5Free tool is only for doing one file at a time. The feasibility of managing the numerous configuration files across a large enterprise is possible but very difficult. The time required to manually enter each file would potentially leave a larger exposure window than if the user were to use an automated tool. It is possible to write scripts to do this automatically in the Windows operating system. However, the time required to scale this across an enterprise such as OPM and manage could potentially create longer exposure times. These exposure times from misconfiguration could give adversaries the time needed to move throughout the network looking for ways to circumvent these controls.

3.3. The right monitoring solution

An example of an automated tool used to monitor changes in hash checksum values is Tripwire. The advantage of using Tripwire is the automated feature to reduce the time of exposure, second the ability to hash and monitor large numbers of files, and third an open source program is available for download or a company built upon this platform is available for purchase. An article published by UpGuard (n.d.) compared the various features of the open source Tripwire and the commercially supported Tripwire. At no cost to the organization, the open source version of Tripwire could be used to monitor the critical files required to modify in order to gain access to a network. A CIO could leverage the results of these exercises as a justification to buy the commercial version of the software.

4. Conclusion

Acting OPM CIO, Donna Seymour, stepped down at shortly after the disclosure of the OPM was made public (Mitchell, 2016). The words of philosopher George Santayana, “Those who cannot remember the past are condemned to repeat it” are applicable to the OPM breach (Clairmont, 2013). Federal CIOs have the potential to learn several lessons from the OPM data breach. Understanding the mission of OPM, the annual budget requests to support that mission, the actions and inactions recorded in the annual FISMA Audits are presented for other federal CIOs to draw parallels to their

organization. By reviewing the timeline history and the available technical details of the breach any CIO can learn from the mistakes that occurred at OPM.

It is the responsibility of the CIO to implement controls to safeguard the mission of their organization. The CSCs were presented to demonstrate how the OPM could have benefited from implementing them. The data and information from each of these frameworks are critical to preventing future data breaches. By applying only three of the CSCs, OPM could have significantly reduced their level of risk. Open source hashing tools could have been used to detect The OPM Breach before the PII of millions of Americans were lost.

CIOs need to understand the value of the data they have on their networks and effectively communicate the level of safeguard needed to reduce the risk to an acceptable level. Personnel working within their organization often focus on the resources they do not have as a reason to not implement security. CIOs need to consider the cost of the data they are responsible for protecting and implement the necessary security solutions prior to a data breach. Unfortunately it is only after an organization experiences a breach, that the CIO and the rest of the organization become fully aware of the value of their data. Often these costs are attributed to the post breach resources necessary to recover from the breach and pay for the damages of the loss. CIOs have the power to understand that potential value of their data and work to influence their organization to spend the tangible amount of money required to safeguard the data and save the intangible image of their company. Using the lessons learned from OPM, CIOs have the opportunity to use them to prevent a similar event from happening to their organization.

References

Belangia, D. W. (2014). That's where the Data is! Why Break into the Office of Personnel Management Systems - Because That Is Where the Sensitive Information for Important People Is Maintained! (Unpublished doctoral dissertation). The SANS Institute. Retrieved February 19, 2016, from https://www.sans.org/reading-room/whitepapers/bestprac/data-is-break-office-personnel-management-systems-35577

Bisson, D. (2015, June 29). The OPM Breach: Timeline of a Hack. Retrieved February 20, 2016, from http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/

Bogos, S. (2013, December 31). Update: Hackers Bring Down LoL, DoTA 2, Blizzard, EA Servers. *Escapist Magazine*. Retrieved April 1, 2016, from http://www.escapistmagazine.com/news/view/130941-Update-Hackers-Bring-Down-LoL-DoTA-2-Blizzard-EA-Servers

Center for Internet Security (CIS) (2015, October 15). *The CIS Critical Security Controls for Effective Cyber Defense*. Retrieved 17 December 2016 from https://www.cisecurity.org/critical-controls/

CIO.GOV. (n.d.). Matthew E. Perry, Author at CIO Council. Retrieved March 27, 2016, from https://cio.gov/contributor/matthew-e-perry/

CIS (2015, October 15). *Critical Controls Overview*. Retrieved April 1, 2016 from https://www.cisecurity.org/critical-controls.cfm

CIS (2015, October). *A Measurement Companion to the CIS Critical Security Controls VER 6.0 10.15.2015*. Retrieved December 17, 2016 from https://www.cisecurity.org/critical-controls.cfm

Clairmont, N. (2013, January 31). "Those Who Do Not Learn History Are Doomed To Repeat It." Really? Retrieved April 03, 2016, from http://bigthink.com/the-proverbial-skeptic/those-who-do-not-learn-history-doomed-to-repeat-it-really

Cole, E. (2015). SANS GSEC Boot Camp. Retrieved from The SANS Institute: https://www.sans.org/download2.php?licenseid=113537

Corey, D., & Goldman, D. (2013). Data Security Laws and the Cybersecurity Debate. *Internet Law, 17*(2), 8-11. Retrieved February 19, 2016, from http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=89679374&S=R&D=iih&EbscoContent=dGJyMMTo50Sep7c4xNvgOLCmr06eqK9Ssa64S7CWxWXS&ContentCustomer=dGJyMOzpsEy1q69IuePfgeyx44Dt6fIA

Davenport, C. (2014, September 9). OPM to end USIS contracts for background security checks. Retrieved April 11, 2016, from https://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts-for-background-security-checks/2014/09/09/4fcd490a-3880-11e4-9c9f-ebb47272e40e_story.html

Esser, M. R. (2012, November 5). FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2012. Retrieved March 8, 2016, from https://www.opm.gov/our-inspector-general/reports/2012/federal-information-security-management-act-audit-fy-2012.pdf

Executive Order 12356, Fed. Reg., 47, 14874 (Apr. 6, 1982). Retrieved 31 March, 2016, from http://www.archives.gov/federal-register/codification/executive-order/12356.html

Fisher, D. (2015, July 10). OPM Hack Expands to Include Data of 21.5 Million People; Director Archuleta Resigns. Retrieved February 28, 2016, from https://threatpost.com/opm-hack-expands-to-include-data-of-21-5-million-people/113717/

Gough, K. (2014, August 26). US Investigations Services (USIS). Retrieved February 20, 2016, from https://www.privacyrights.org/content/us-investigations-services-usis

Harris, S. (2015, June 24). Hackers Stole Secrets of U.S. Government Workers' Sex Lives. Retrieved March 21, 2016, from http://www.thedailybeast.com/articles/2015/06/24/hackers-stole-secrets-of-u-s-government-workers-sex-lives.html

Henry, P. (2015). SANS GSEC Boot Camp. Retrieved from The SANS Institute: https://www.sans.org/account/vlive-course/87455

Lesniewski, N. (2015, September 23). With All Eyes on Pope, OPM Drops Bad News on the Hack. Retrieved February 20, 2016, from http://www.rollcall.com/hill-blotter/opm-hack-more-fingerprints-stolen/?dcz=

Lord, N. (2015). The History of Data Breaches. Retrieved March 30, 2016, from https://digitalguardian.com/blog/history-data-breaches

McFarland, P. E. (2015, July 22). Serious Concerns Regarding the Office of the Chief Information Officer. Retrieved March 27, 2016, from https://www.opm.gov/our-inspector-general/special-reports-and-reviews/serious-concerns-regarding-the-office-of-the-chief-information-officer.pdf

Mimoso, M. (2015, June 08). OPM Warned About Governance Weaknesses, System Vulnerabilities Prior to Hack. Retrieved February 28, 2016, from https://threatpost.com/opm-warned-about-governance-weaknesses-system-vulnerabilities-prior-to-hack/113209/

Mitchell, B. (2016, February 22). Office of Personnel Management CIO Donna Seymour retires. Retrieved March 27, 2016, from http://fedscoop.com/opm-cio-seymour-retires

OPM (2014) OPM Mission, Goals, and Priorities. Retrieved March 28, 2016, from https://www.opm.gov/about-us/budget-performance/goals-priorities

OPM (2016a) Our Mission, Role & History What We Do. Retrieved March 28, 2016, from https://www.opm.gov/about-us/our-mission-role-history/what-we-do/

OPM (2016b) Our People & Organization Senior Staff Bios. Retrieved March 26, 2016, https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/janet-barnes/

Perry, M. (2011, June 06). IT Reform at the Office of Personnel Management - CIO Council. Retrieved March 27, 2016, from https://cio.gov/it-reform-at-the-office-of-personnel-management/

Perez, E., & Prokupecz, S. (2015, June 23). U.S. government hack could actually affect 18 million. Retrieved February 28, 2016, from http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion/

Rkaina, S. (2014, December 26). Christmas 'ruined' after hackers suspected of bringing down Xbox Live and PSN. Retrieved April 03, 2016, from

http://www.mirror.co.uk/news/world-news/christmas-ruined-gamers-after-hackers-4878774

Sternstein, A. (2016, February 22). Heated House Hearing Offers New Clues Into How Hackers Broke Into OPM Networks. Retrieved March 27, 2016, from http://www.nextgov.com/cybersecurity/2015/06/heated-house-hearing-offers-new-clues-how-hackers-broke-opm-networks/115474/

United States, The Office of Personnel Management (Future citation reference US, OPM). (2006). *FY 2007 Office of Personnel Management Congressional Budget Justification* (pp. I-120). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2007-budget.pdf

US, OPM. (2007). *FY 2008 Office of Personnel Management Congressional Budget Justification* (pp. I-92). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf

US, OPM. (2008). *FY 2009 Office of Personnel Management Congressional Budget Justification* (pp. I-133). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2009-budget.pdf

US, OPM. (2009). *FY 2010 Office of Personnel Management Congressional Budget Justification* (pp. I-119). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2010-budget.pdf

US, OPM. (2010). *FY 2011 Office of Personnel Management Congressional Budget Justification* (pp. I-145). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2011-budget.pdf

US, OPM. (2011). *FY 2012 Office of Personnel Management Congressional Budget Justification* (pp. I-172). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2012-budget.pdf

US, OPM. (2012). *FY 2013 Office of Personnel Management Congressional Budget Justification* (pp. I-161). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2013-budget.pdf

US, OPM. (2013). *FY 2014 Office of Personnel Management Congressional Budget Justification* (pp. I-163). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2014-budget.pdf

US, OPM. (2014). *FY 2015 Office of Personnel Management Congressional Budget Justification* (pp. I-282). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2015-budget.pdf

US, OPM. (2015). *FY 2016 Office of Personnel Management Congressional Budget Justification* (pp. I-282). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2016-budget.pdf

US, OPM. (2016). *FY 2017 Office of Personnel Management Congressional Budget Justification* (pp. I-280). Washington DC, D.C.: OPM. Retrieved March 27, 2016, from https://www.opm.gov/about-us/budget-performance/budgets/2017-budget.pdf

US, OPM. (2014, February). *Strategic Information Technology Plan* (pp. I-69). Washington DC, D.C.: OPM. Retrieved April 10, 2016, from https://www.opm.gov/about-us/budget-performance/strategic-plans/strategic-it-plan.pdf

UpGuard. (n.d.). Tripwire Enterprise vs. Tripwire Open Source. Retrieved April 10, 2016, from https://www.upguard.com/articles/tripwire-enterprise-vs.-tripwire-open-source

Wei, Jessica (2016, January 8). Inspirational Finance Quotes. Retrieved 28 March, 2016, from https://due.com/blog/dont-tell-me-where-your-priorities-are-james-w-frick/

Widmer, L. (2015, July 18). The 10 most expensive data breaches. Retrieved March 30, 2016, from http://www.lifehealthpro.com/2015/06/18/the-10-most-expensive-data-breaches?t=life-practice-management

Yaniga, Jeff (2015, January 12). Three Predictions for Private Exchanges: Version 2015. Retrieved March 26, 2016, from http://www.privatehealthcareexchanges.com/blog/three-predictions-for-private-exchanges.php

Appendix A

BUDGET CORRELATION

Data

Name	IT Security Terms Mentioned	IT Security Budget Request
FY 2007	0	$0.00
FY 2008	0	$0.00
FY 2009	0	$0.00
FY 2010	0	$0.00
FY 2011	5	Undetermined
FY 2012	3	Undetermined
FY 2013	2	Undetermined
FY 2014	6	Undetermined
FY 2015	7	Undetermined
FY 2016	24	$21,000,000.00
FY 2017	44	$37,000,000.00

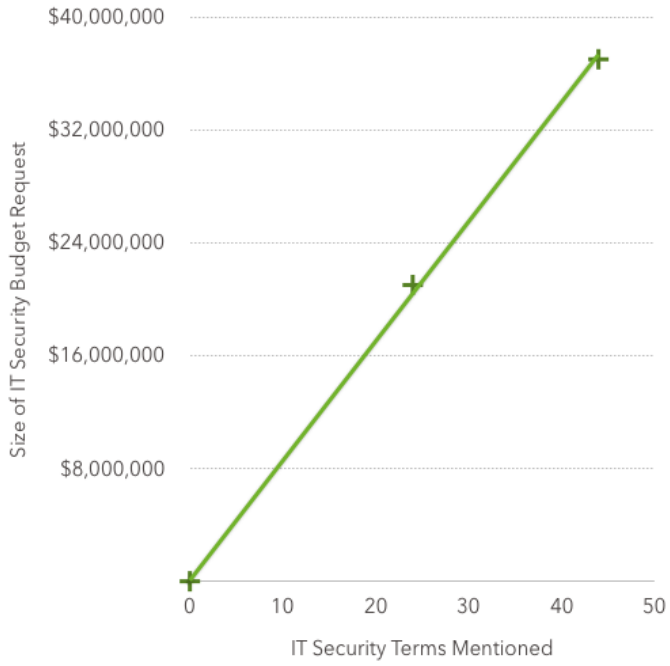
Is there a correlation between the number of IT Security Terms Mentioned and the size of the IT Security Budget request?

Scatter charts map correlation between two variables. The closer the points are to forming a diagonal line, the stronger the correlation!

Instructions:

1. Download the FY budget requests located here: https://www.opm.gov/about-us/budget-performance/budgets/#url=Congressional-Budget-Justification
2. Open each budget request and search for the following terms "IT security","Cyber", or "security software maintenance"
3. Record the number of times either term is mentioned and add together to form "IT Security Terms Mentioned"
4. Review each budget request to record the explicit amount of the IT Security budget request

Results



David Thomas, Thomas.1597@gmail.com

Appendix B

OPM's FY 2016 request is $32 million above our FY 2015 appropriation. Most of these funds will be directed towards investments in IT network infrastructure and security. As a proprietor of sensitive data -- including personally identifiable information for 32 million federal employees and retirees – OPM has an obligation to maintain contemporary and robust cybersecurity controls. The infiltration of our network last year underscores the importance of these investments.

It has been a year since OPM developed and launched its FY 2014 - 2018 Strategic Plan. The budget proposal that we have outlined in this document is aligned to that plan, and will allow OPM to maintain its operations and continue with the execution of its mission priorities.

I appreciate the opportunity to respond to your interest in this matter. If you have any questions, please contact Angela Kouters, OPM's Director of Congressional, Legislative and Intergovernmental Affairs, at (202) 606-1300.

Sincerely,

Katherine Archuleta
Director

United States, The Office of Personnel Management. (2015, Director's Comments)

OPM's FY 2016 request budgets $21,000,000 to implement and sustain agency network upgrades initiated in FY 2014 and security software maintenance to ensure a stronger, more reliable, and better protected OPM network architecture. This requested funding provides critical support to defend the OPM IT network against attacks like the cybersecurity incident recently brought to light in 2014, and positions OPM to maintain the critical updates being deployed in FY 2014 and FY 2015. This updated network must be maintained over time to ensure that OPM's system does not revert to antiquity and insecurity. It must also continue to employ the best security tools to protect OPM's IT infrastructure from ever-increasing and exponentially sophisticated network attacks. As a result, additional funding is needed to support operations and maintenance of the additional hardware, software, and staff.

United States, The Office of Personnel Management. (2015, p. 2)

Details of Cybersecurity Costs for FY 2017

Description	Scope	Cost
Distributed applications (non-mainframe) thru 2019	Mostly re-engineering of existing systems such as USAJobs and, USAStaffing, etc. that do not require extensive work to transition to the new Shell environment	$10,054,514
Total FY 2017 Migration Costs		**$10,054,514**
Shell infrastructure	Hardware, software, FTEs and contract services associated with maintaining Shell and supporting system transitions.	$13,286,084
Quality Assurance	Resources to stand up quality assurance division and enterprise PMO for release management	$2,654,025
Enterprise Architecture (EA) and Governance	Resources to continue management of OPM's EA using Troux and performing Control gate reviews for all investments	$1,497,622
Total FY 2017 Dual Environment Operations Costs		**$17,437,731**
Legacy Network Management costs	Includes software costs for existing legacy NM, FTEs, mobile device management, annual laptop refreshes	$9,507,755
Total FY 2017 Request		**$37,000,000**

Note 1: All transitions will require data migration, interfaces and change management

Note 2: Modernize = re-engineer or replace

United States, The Office of Personnel Management. (2016, p. 4)