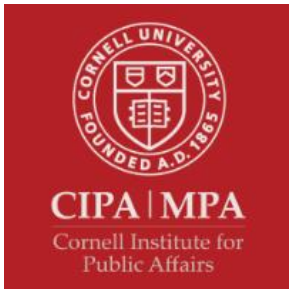

Report
In Consultation with the United States
Government Accountability Office

FEDERAL WORKFORCE

Attracting and Retaining Talent in the Field of Cybersecurity

Research conducted by Kate Bedding and
Marijke de Jongh, Fellows,
Cornell Institute for Public Affairs

May 2017

Acknowledgements

This report discusses a project carried out in consultation with the U.S. Government Accountability Office. The authors would like to thank the following people who contributed their time, ideas, and guidance to this project.

GOVERNMENT ACCOUNTABILITY OFFICE

Justine E. Augeri, Ph.D., Analyst, Strategic Issues
John J. Barrett, Senior Analyst, Natural Resources & Environment
Robert Goldenkoff, Director, Strategic Issues
Amanda Goolden, Analyst, National Resources & Environment
Chelsa Gurkin, Assistant Director, Strategic Issues
Shelby Kain, Analyst-in-Charge, Strategic Issues
Jennifer E. Kamara, Analyst, Financial Markets & Community Investment
Christine M. Ramos, Senior Analyst, Financial Markets & Community Investment

CORNELL INSTITUTE FOR PUBLIC AFFAIRS

Kayla Kirchner Malone, MPA, Engaged Learning Associate
Laurie Miller, Associate Director for CIPA Public Engagement and Capstone Instructor
Tom Worhach, Capstone Teaching Assistant

OTHER INDIVIDUALS AND ORGANIZATIONS

Seth Harris, former United States Deputy Secretary of Labor
Michael Jabbour, Chief Information Officer at New York City Department of Homeless Services
Jane Holl Lute, former Deputy Secretary of Homeland Security
Ronald Rigoles, Transformational Business Advisor

Table of Contents

Executive Summary

Why the Cornell Institute for Public Affairs Conducted This Research

This report was carried out in consultation with the U.S. Government Accountability Office (GAO) as a preliminary inquiry into the challenges and opportunities surrounding the cybersecurity workforce in the Federal Government.

The report was supported through the Cornell Institute for Public Affairs (CIPA) Capstone course, which provides CIPA Fellows the opportunity to engage with external clients on various projects to gain professional exposure and experience.

This report examines how the Federal Government currently attracts and retains cybersecurity talent as well as explores various employment models that may assist with or improve attraction and retention in the future. The report is limited in its discussion of the federal workforce to the field of cybersecurity but will make recommendations for future research that can be conducted by additional teams to broaden the scope of the project.

This initial research into federal hiring and retention practices in the field of cybersecurity will provide the GAO with insight into challenges facing federal agencies as they attempt to build and improve cybersecurity initiatives. It will also help inform upcoming GAO reports on the federal workforce. Many of the lessons and best practices highlighted in this report may be applicable to the Federal Government as a whole. It is the hope of this research team that the best practices they identify for the Federal Government will be selected for future research by the GAO and eventually included in the hiring and retention practices of the federal workforce.

This report identifies not only potential employment models but also discusses any barriers to implementation, as some employment models are more applicable to certain sectors or agencies over others. The team has endeavored to identify a wide variety of options that could be applied across the federal workforce with regard to cybersecurity.

For this report, the team has not made recommendations for which best practices or employment models to implement. This report is, instead, an exploration of the many options available to the Federal Government and provides an unbiased evaluation of the benefits, challenges, and feasibility of implementing each model.

Research Questions

The GAO is interested in public sector workplace employment models,

especially in the STEM field of Information Technology and Cybersecurity and how federal agencies can remain or become competitive in the labor market, especially with regard to acquiring new talent and developing existing talent. The team was tasked with answering two questions with regard to the federal cybersecurity workforce:

> ***Q1:*** *How do selected federal agencies recruit and retain talent in the field of cybersecurity?*
>
> ***Q2:*** *What employment models will allow federal agencies to become or to remain competitive in this labor market while fulfilling all of the requirements of their current missions?*

To answer these questions, the research team conducted an in-depth study of both the current state of the federal workforce as well as current and possible future employment models. The team also used the close examination of two case study agencies as well as expert interviews to further inform its research.

Summary of Findings

In surveying the landscape of the federal cybersecurity workforce, it became clear that, while the Federal Government seems to have a strong understanding of the importance of cybersecurity and supporting cybersecurity work, many issues remain regarding actually attracting and retaining top cybersecurity talent. For example, since the Internet took off in the 90s, the cybersecurity talent pipeline has been unable to keep up with demand in either the public or private sector (Callahan, 2016, p. 1). There are many more cybersecurity positions available than there is talent to fill them. Federal agencies have taken steps to address this problem through education initiatives and workforce development, but demand still far outstrips supply. The Federal Government has recognized that this is also an issue in the private sector and has taken steps to partner with companies to invest in developing cybersecurity talent.

While the common perception is that government jobs do not pay as much as private sector jobs, data from the Congressional Budget Office (CBO) showed that this problem is more complex than it appears on the surface. Government professionals with high school and bachelor's degrees actually earned more than their private sector counterparts while those with advanced degrees earned less. Since many top cybersecurity candidates fall into the category of having advanced degrees, the Office of Personnel Management created flexible compensation options for federal agencies to utilize when hiring or retaining cybersecurity professionals.

Additionally, the federal hiring process is slow and complex, making it even harder for the Federal Government to compete with other sectors for top talent. Cybersecurity is especially difficult in this regard because many cybersecurity jobs require a security clearance, which can take months and even years to complete. During this time, candidates may find other jobs or choose not to work in the government. Although some agencies have been granted flexibilities and exemptions around hiring cybersecurity experts, overall this is still a major issue for the government at large.

Finally, the government does not have a cohesive, coordinated strategy around cybersecurity workforce planning. Cybersecurity jobs are not well defined, and agencies differ in how they prioritize, recruit, and retain cybersecurity professionals. As a result, some agencies appear to have stronger cybersecurity workforces than others. A cohesive, government-wide strategy may help all agencies better plan for their cybersecurity workforce.

The following paper will address a variety of employment models currently being implemented on a small scale within the Federal Government, as well as on a larger scale in the private sector. By identifying many options for professionals in the field of cybersecurity in the federal workforce, this paper provides a lens into opportunities for improvement in the hiring practices and workplace models of the government to assist with the growth of an effective workforce. The authors provide case studies on two agencies to help inform the discussion. They also explore factors and alternative models of employment (listed below). These employment models address, to varying degrees, the issues identified above, including the cyber talent pipeline, the complex federal hiring process, and the need for comprehensive, strategic cybersecurity workforce planning.

Pay & Benefits
Flexible Hours
Gig Economy
Fellowships
Public-Private Partnerships
Shared Services & Centralized Workforce
Culture and Corporate Social Responsibility
Flexible Retirement Plans
Outsourcing & Crowdsourcing
Shortened Hiring Timeline
Education & Training

Introduction

With the transition of administration, there are numerous opportunities to change the design and composition of the federal workforce. The January-April 2017 hiring freeze exempted "positions (within the Department of Defense) required for cybersecurity and cyberspace operations and planning" (Work, 2017), signaling an acknowledgment by the top leadership in the country of the importance of crafting a robust cybersecurity workforce. By facilitating cooperation between the private sector, academia, nonprofits, labor advocacy groups, and the public sector, the Federal Government can influence both civilian and government employment models. As the Federal Government identifies best practices and new initiatives, it has the opportunity to share this information and knowledge among the federal workforce and the American workforce as a whole.

With this, Katherine Archuleta, the Director of the Office of Personnel Management (OPM) has specified that one of OPM's goals is to "help agencies create inclusive work environments where a diverse federal workforce is fully engaged and energized to put forth its best effort, achieve its agency's mission, and remain committed to its mission" ("A More Efficient," 2014, p. 4). This open acknowledgment by and willingness of the Federal Government to investigate and possibly implement fundamental changes to its hiring practices and work environments opens the doors for a rejuvenation of the workforce. Previously, the government has affected quick change in its workforce with the use of Special Hiring Authorities and Flexibilities to provide pay and leave incentives for new employees. While this system is effective in the short term, it is not a sustainable measure and is not as effective in the aggregate as it is in individual sectors (Reinhold, 2015).

One of the largest sectors that has been utilizing the Special Hiring Authorities (SHAs) is the cybersecurity sector. The civilian cyber sector represents about one out of every twenty-two government employees, or 92,863 employees government-wide (Partnership for Public Service, 2015, p. 4). Currently, SHAs allow employers to provide pay and leave incentives to attempt to close the gap between cybersecurity positions in the federal workforce and the private sector. The need for well-trained and talented cybersecurity employees cannot be overstated: as the government follows the private sector further into the wireless age, the effect on Federal systems and agencies is growing at a rapid rate (Reinhold, 2015).

Federal agencies are responsible for a vast amount of information, ranging from personnel data files to classified military and defense security documents. Agency cooperation is vital to the successful mission completion of these agencies, but this collaboration can be loaded with pitfalls for government cybersecurity professionals. Agencies are not

directly connected to one another; they do not share networks, and many of them remain segregated behind many layers of encrypted firewalls. This ensures greater security of each individual agency, as there exist fewer potential failure points and opportunities for exploitation, but it can make coordination, when necessary, very difficult.

In 2015, President Obama included the importance of shared services in his Management Agenda and soon after the Office of Management and Budget (OMB) and the General Services Administration (GSA) devised a "shared services Management and Oversight operating model" to promote government wide-shared services. Under this model, OMB assumed leadership of a Shared Services Governance Board and the GSA established a Unified Shared Services Management (USSM) office (Mader & Roth, 2015). As the Federal Government makes a large-scale shift toward increased cooperation and data-sharing between agencies, it is incumbent upon the cybersecurity professionals to ensure the networks are secured from potential attacks.

As agencies attempt to recruit the necessary talent to support their cybersecurity demands, they encounter many challenges. These challenges range from the length of time required to fill a position in the federal workforce to the length of time it currently takes to apply for and receive a security clearance. In addition, the federal General Schedule pay scale struggles to compete with the pay incentives offered in the private sector for top employees with advanced degrees. According to the Bureau of Labor Statistics, candidates in the private sector with advanced degrees can expect to earn at least twenty-four percent more than their government counterparts (Falk, 2017, p. 2). For candidates with a high school, associate's, or bachelor's degree, federal employment on average pays higher than the private sector. However, the opportunities for advancement can be limited and the rate of advancement much slower than the private sector. While SHAs have assisted with some of these challenges, they cannot address all of the causes, and a culture shift and renovation of the federal workforce hiring practices and employment models is necessary.

Defining the Issues

Background

A 2007 report by the U.S. Merit Systems Protection Board identified a variety of challenges with increasing the federal workforce. As identified ten years ago, "there is growing concern about the Government's ability to compete with the private sector and other public sectors" (US Merit, 2007, p. 10). The Board also identified a list of recruitment challenges facing the Federal Government that are still applicable today. These challenges included:

- *Length and complexity of the hiring process*
- *Poor image of the Federal Government as an employer*
- *Competition among agencies*
- *Budget constraints and uncertainties*
- *Perceptions of noncompetitive salaries*
- *Regulatory obstacles to entry- level hiring*
- *Labor market shortages*
- *Diminishing HR capacity*

(US Merit, 2007, p. 12)

Ten years later, overall, the Federal Government is still struggling to attract and retain top talent. According to the Partnership for Public Service, young professionals are exceedingly underrepresented in the Federal Government as compared to other sectors. Additionally, "it is challenging for government to attract and hire mid- and senior-level talent from outside government, who could bring fresh perspectives and innovations from other sectors to solve federal challenges" ("Federal Hiring," 2017). This becomes especially problematic in the field of cybersecurity, which is constantly evolving and requiring top talent to implement best practices and present against the newest threats.

There are many difficulties facing employers, both in the private and public sector, as they try to create and build effective cybersecurity programs. The need for workers outweighs the available supply, and much of the education currently being provided to prospective employees is basic and lacking in depth. In fact, "most entry-level [cybersecurity] staff lack the necessary technical skills and, as a result, 86 percent of employers must provide on-the-job training" (Commission on Enhancing National Cybersecurity, 2016, p. 33). In addition, despite the fact that cybersecurity pays a higher salary than most other IT jobs, there has not been enough talent to fill available cybersecurity roles, and it is anticipated that globally there will be a demand for 1.5 million more cybersecurity employees by 2020 (Commission on Enhancing National Cybersecurity, 2016, p. 33).

As was explained in the expert interview with Mr. Michael Jabbour, Chief Information Officer for the New York City Department of Homeless Services, many of the older networks for the city, state and federal agencies were reliant on older, wired LAN systems. When that was largely the case, threats to the network were more easily controlled and prevented. However, as the transition was made to wireless networks with remote servers and storage on 'the cloud,' there arose an increased need for more advanced data protection. The need for more effective electronic data protection, later termed 'cybersecurity', largely coincided with the movement from Local Area Networks (LAN) to wireless networks and storage on the "cloud."

The cybersecurity workforce is of particular importance to companies and governments alike, as the world becomes more interconnected and dependent on technology. According to the McKinsey Global Institute (MGI), this increased digitization in all sectors increases vulnerability to cyber-attacks as it becomes a challenge to remain ahead of the ever changing and increasingly sophisticated hacking that presents a danger to the information security of these agencies. These cyber-attacks are expensive, and have resulted in total costs in excess of $400 billion dollars to the global economy. These costs are incurred as companies try to prevent, combat, and meet the challenges of protecting themselves from data breaches, theft, and various financial crimes. A talented cybersecurity workforce is necessary to address these challenges, and "governments will need to work closely with their global counterparts and with the business community to stay on top of new threats and share technology solutions" (Manyika et al., 2016, p. 18).

With the various challenges facing the field of cybersecurity, the federal government, through DHS, began to provide grants and funds to government agencies to assist with building their cybersecurity programs and staff investments. These grants were crucial in the early creation of many cybersecurity staffs and cohorts, but were not able to be sustained long term, and have left some agencies scrambling for funding as they attempt to continue to focus on and invest in cybersecurity (Powner, 2016, p. 33).

Unlike many other issues within the government, cybersecurity was one area where the traditional problem-solution model was not as applicable. In previous situations, the government and federal agencies saw a significant amount of success with the system of identifying a problem, crafting a solution to that problem, and then incorporating a tool to address that issue or put that identified solution into action. However, cybersecurity is an ever-changing field; tools were only valid for a short amount of time before they were outdated. Threats were constantly

evolving and required workers who could learn and develop in order to continually combat a sea of changing threats.

This required a different caliber of worker, with a different style of education and on-the-job learning. Successful cybersecurity professionals needed to be able to transition from the old model of being reactive, to a new model of being proactive. In their most effective form, this would mean being able to predict problems to stop them before they began. In terms of workforce composition, this created three informal levels of cybersecurity workers: the standard cybersecurity worker, the cybersecurity specialist, and the cybersecurity professional. An effective and robust cybersecurity team would be comprised of all three types of workers, though the government has had difficulty attracting the latter.

The standard cybersecurity worker is characterized by a person who has an extensive knowledge of LAN and networks in general, and can understand the basics of network security and firewalls. They have on the ground network management skills, but do not operate in a predictive manner to prevent issues before they begin. The standard cybersecurity worker is responsive by nature, and while they can manage events as they occur, they are not able to predict the larger issues, and so will always remain just behind the event curve. These workers are characteristically, though not always, middle to older age, with little to no advanced leadership desires. These workers have the basics in training on cybersecurity that may have been added on as an additional training beyond their initial work in the field (M. Jabbour, telephone interview, April 20, 2017).

The cybersecurity specialist can be identified by their ability to understand event management in the case of a cybersecurity threat, and the ability to orchestrate a team to respond to an event. The cybersecurity specialist comes from a range of backgrounds with a range of educational experiences, and is characterized by a person who hopes to make a career out of cybersecurity. They are therefore more focused on building teams and building their career progression, and can often be more academic and less tactical in their responses to critical cybersecurity events.

The final group can be classified as cybersecurity professionals; these are generally younger people who have sought advanced training as white hackers (also known as ethical hackers). They have predictive skills and are characterized by innovative, intuitive, and unique responses to events and threats. They can think like the machine they are combating, and can evaluate an event, triage and control the issues, then develop and implement innovative and predictive controls. While these workers are the most valuable, and crucial to the team, they are amongst the hardest

to recruit into federal service, and to retain in the federal workforce, as many of the opportunities and benefits that they can find in the civilian workforce far outstrip those that the Federal Government can offer.

An additional challenge facing agencies that are trying to build their cybersecurity teams is the issue of training and preparation for the type of work that the workforce will be asked to do. Due to the constantly evolving threats within the field of cybersecurity, training is outdated almost as soon as it is published. The training that is provided by the majority of college programs and degree programs is limited in its scope and does not prepare its workers for the predictive type of thinking required by cybersecurity professionals. Professionals must gain additional knowledge from on-the-job training and event management, as well as from ongoing learning and training that can be provided through a variety of courses. Unfortunately, in order to build a robust and effective cybersecurity program, the cost of training is very high. Training must be provided to all users, not simply the cybersecurity professionals, in order to ensure top-to-bottom compliance with the program and network security.

With the many challenges and barriers facing the implementation of adequate cybersecurity programs, funding remains one of the largest concerns. This paper will not endeavor to solve this problem, but, rather, will seek to identify alternate solutions that may allow the government in securing cybersecurity professionals to protect the United States' constant, rapidly changing networks and data protection needs.

Key Definitions

As the authors examine these issues and their impact on the federal workforce, they will rely on some key definitions. In particular, the team will focus on the following items:

> **Federal Agencies.** The term federal agencies applies to any federally funded government organization. The purpose of this work will be to outline specific best practices that may apply to employment within the federal sector, though the scope of this project will mandate that the team will focus on the Department of Homeland Security and the Office of Personnel Management.
>
> **New Talent.** The term new talent refers to persons who are either joining the workforce immediately after they have completed their training (be that college, or amended vocational training), as well as personnel who have made a career change and are entering the workforce in a new career

for the first time. This term is not limited to any age group or generation, but is limited to those who are searching for and acquiring entry level positions in the cybersecurity workforce. As the authors will discuss, many of these jobs may not be fitting for career building, but rather, may be more appropriate for transitional work or initial entry work, as talented members with current skill sets join the workforce initially, and then move on from the federal workforce to the private sector as they gain more seniority.

Existing model of federal employment. This paper will not spend a significant amount of time characterizing the existing model of federal employment; rather, it will focus on ways in which that model can be updated or modified to better serve and attract the modern workforce. The existing model of federal employment is characterized by a standard eight or nine hour workday in a centralized geographical location. Workers are hired into entry level positions, and gradually progress over many years of work at a single agency. In addition, federal careers are characterized by the awarding of a pension upon retirement. While this is the standard model, it can be augmented by various Special Hiring Authorities, and by the workplace policies of each individual agency.

STEM fields. The scope of this paper will focus heavily on employment within the STEM fields: Science, Technology, Engineering and Mathematics. These fields experience a variety of hiring issues that are unique, largely due to the complicated and ever changing knowledge base required of a worker in these fields. As new technology is developed and new research is conducted, workers in these fields are challenged to stay abreast of the current information. This results in personnel who are often best equipped to handle current issues and challenges when they have most recently received training. This can create a difficult leadership challenge for managers, as they must nurture and empower their subordinates who are better trained and more knowledgeable, while maintaining authority and oversight on the issue and the project.

Information technology. Jobs within the federal workforce that demand a focus on the usage, implementation, and maintenance of electronic communications, such as telecommunications and computers, fall into the category of information technology jobs. Currently, each agency within

the Federal Government staffs and maintains its own information technology department. Jobs in this field are particularly susceptible to the challenges explained above, as the knowledge and technology in the information technology sphere of influence is constantly evolving and changing, often more quickly than adequate training can be provided by the vast majority of institutions. This paper will further explore the challenges surrounding work in the field of Information technology, particularly cybersecurity positions.

Cybersecurity. The field of cybersecurity refers to the workforce that is responsible for ensuring the protection of electronic data. This can refer to personnel data, employment history, Personally Identifiable Information (PII), classified material of all sorts, and any other type of protected record that is sent or stored within electronic networks. Personnel employed in the field of cybersecurity are responsible for predicting, identifying, and responding to threats to this information, in order to protect it from those who do not require or should not have access to this material.

Labor Market. The labor market refers to those persons available for hire, or those who are actively seeking new employment. The labor market within the field of cybersecurity is faced with unique challenges, as many technology skillsets grow outdated quickly in the face of evolving cyber threats. As this paper will discuss, the labor market available in the field of cybersecurity is often smaller than demand for cybersecurity professionals. It is critical, therefore, that the Federal Government consider best practices in attempting to hire and retain these professionals in order to maintain the staff required to effectively protect its interests.

Missions. Each federal agency has a unique mission that directly relates to the type of information the agency must handle and protect, ranging from personnel records to critical classified information. As agencies look to hire cybersecurity professionals, the mission of the agency influences the type of professionals they need. One of the key goals of the Office of Personnel Management is to ensure that each agency is staffed with the employees necessary to complete their mission. For this reason, it is critical to understand the effect these different missions have on employment as well as the types of professionals that are needed to fulfill these missions.

Data Collection and Methodology

To provide a comprehensive snapshot of workplace trends and future opportunities with regard to the federal cybersecurity workforce, the team relied on primary and secondary data collection, including a thorough literature review, informational interviews, and case studies of two federal agencies: the Department of Homeland Security and the Office of Personnel Management. The team opted to focus on data from the last three years, although employment data from as far back as ten years were included, when appropriate, to demonstrate trends.

Literature Review

The literature review consists of academic articles, white papers, agency data and reports, and testimonies before Congress. Included in these sources are articles from academia, government agencies, nonprofits, and the private sector. Per the team's conversation with the GAO, with the exception of background research on the topic, the data has been limited to the last three years because the field of cybersecurity is so rapidly changing and older data may no longer be relevant. The literature review examines both the current state of the federal cybersecurity workforce and current employment models from sources such as President Obama's 2016 Cybersecurity National Action Plan and the Office of Personnel Management's 2016 Investing in Cybersecurity report. The literature review also outlines opportunities for improvement in cybersecurity hiring and recruitment practices based on leading research and best practices from the private, public, nonprofit, and academic sectors. The feasibility of implementing different changes has been explored, and discussions of potential new employment models are provided.

Keywords

The team used the following search terms while conducting the literature review. These terms focused on the main goals of the research question, namely federal cybersecurity employment and retention. *Keywords:* federal employment, cybersecurity employment, comparison of federal workforce to civilian workforce, homeland security, office of personnel management, innovative employment models, flex time, flexible retirement, salary initiatives, innovative hiring practices, innovative employment models, federal employment benefits, thrift savings plan comparison 401K, federal hiring process, cybersecurity best practices.

Expert Interviews

Individuals selected for informational interviews were identified by their expertise or experience in the field of cybersecurity and/or federal hiring and recruitment practices. The interviewees provided first-hand knowledge of trends occurring in both the private and public sectors as

well as many of the key issues and opportunities facing new professionals entering the cybersecurity workforce. The interviews informed the scope and direction of the literature review and corroborated much of the data found by the team.

Mr. Seth Harris, former United States Deputy Secretary of Labor provided the team with extensive insight into the meta problem surrounding the labor market of cybersecurity in the workforce as a whole. He provided key insight that has been incorporated into this research concerning many of the initiatives the Federal Government is already exploring, as well as unique workforce practices that could be incorporated in the future. In addition, Mr. Harris provided critical information concerning many of the barriers the Federal Government faces when attempting to hire cybersecurity and information technology professionals.

Ms. Jane Holl Lute, former United States Deputy Director of Homeland Security, provided in-depth information on the recent initiatives at the Department of Homeland Security (DHS), and the innovative ways DHS is trying to build its cybersecurity workforce. Her information concerning the types of employees needed for effective cybersecurity initiatives and the work streams needed to help acquire those employees provided the team with insight into methodology the Federal Government may consider adapting to overcome their cybersecurity workforce issues.

Mr. Michael Jabbour, Chief Information Officer for New York City's Department of Homeless Services, provided the team with information on the many challenges facing any government entity that is working to develop or grow its cybersecurity workforce. He provided detailed information on initiatives New York City has employed at the local government level and discussed many of the challenges that his agency has faced in filling critical cyber workforce openings.

Case Studies

The two agencies selected for the team's case studies, the Department of Homeland Security (DHS) and the Office of Personnel Management (OPM), were selected according to four criteria:

- Agency size
- Information responsibilities
- Cybersecurity issues and initiatives
- Compliance with FISMA

Agency size was used because the team was interested in understanding if factors relating to size, such as having more employee data to protect or having more employees using technology resources, played a role in how agencies hired and retained cybersecurity employees. As identified by Mr. Michael Jabbour, the larger the number of employees accessing a network, the more opportunities for critical failure or vulnerabilities. Cybersecurity professionals are regularly faced with the challenge of both protecting against external threats and also protecting against threats or mistakes made internally. According to Mr. Jabbour, larger agencies are at a greater risk for information breaches and other exploitations of vulnerabilities, as there are significantly more possible failure points within their networks.

The second criteria, the type of information the agency was responsible for overseeing and protecting, was of interest to the team because the team wanted to explore whether different types of data responsibilities meant different cybersecurity hiring and recruitment practices. Regarding DHS and OPM, the authors wanted to know if defense data may be protected differently from federal employee or citizen data. Each agency's data responsibilities are directly related to their mission and may subject them to different threats. Cybersecurity professionals working with classified information that has critical sensitivities may experience vastly different threats and workloads than those securing personnel files. As such, the hiring initiatives and employment models that may be effective for one agency may not be appropriate for another.

The third criteria applied was cybersecurity issues or initiatives within the agencies. The team was interested in studying agencies that may have had difficulties regarding cybersecurity in the past as well as agencies spearheading new cybersecurity initiatives or making cybersecurity a priority. Early research exposed the importance of culture and mission, and the team was interested to explore if these factors related to agency initiatives around cybersecurity. According to Mr. Jabbour, the most sought after new talent in the cybersecurity workforce are expected to employ creativity and ingenuity in their solutions to cybersecurity challenges; these employees may be more attracted to employment at an agency that mirrors those characteristics.

The final criteria selected by the team was how the agency has complied with federal guidance and regulations, specifically the Federal Information

Security Management Act of 2002 (most recently updated in 2014), otherwise known as FISMA, which requires every federal agency to comply with a minimum standard of information security practices. The aim of gathering this information was to see if compliance (and the degree of compliance) had any effect on or correlation with cybersecurity employment models.

To find information on the four criteria, the team relied on sources such as OPM and the Office of the Inspector General (OIG). The team also referenced previous GAO studies, similar studies conducted by other federal offices, such as the Social Security Administration, and testimonies that have been given before Congress on this topic.

Literature Review

Current State

Cybersecurity policy and strategy in the federal government have both strengths and weaknesses. There have been significant investments made into a myriad of cybersecurity initiatives throughout the years, however, there are still many areas in which federal cybersecurity could be improved. One of these areas is the government's cybersecurity workforce. Despite the fact that federal agencies are reporting increasing numbers of cybersecurity problems and threats, the federal government is struggling to attract and retain top cybersecurity talent to address these issues.

Employment within the Federal Government

To better understand hiring and workforce issues within the federal government, it can be useful to first understand the broad demographics of the federal workforce. According to OPM's website, the average Federal employee is 47.5 years of age, with 13.6 years of service within the Federal Government (OPM, 2016). The Federal Government employs approximately 1.9 million non-postal federal employees, 94% of whom are full-time workers. 71.39% of these workers are employed under the General Schedule pay-system (OPM, 2016).

Full-time employment within the Federal Government is characterized by a forty-hour work week. Full-time non-seasonal employees and full-time permanent employees are categorized as those who are employed with no definitive end date, signifying that they are able to remain employed indefinitely, or as a career (OPM, June 2016, p. 5). 94.94% of the federal workforce are currently employed as full-time employees, with only 2.72% as part-time, and 2.34% as intermittent employees (OPM, September

2016). Many employees who are employed as full-time permanent employees may be working towards retirement goals within the Federal Government.

In fact, 31% of all career employees within the Federal Government will be eligible to retire in 2017 (Goldenkoff, 2014, p. 23). According to the testimony given before Congress by Senator Robert Portman in 2014;

> "*Today, only 14 percent of the two million permanent career employees are eligible for retirement. Over the next three years alone, that number more than doubles, to 31 percent. I think you said 30 percent at DOD. So, this is obviously an issue, of people retiring. Meanwhile, we are not attracting the young people that we should be, and I think the federal workforce now has only 6 per- cent under the age of 30. By comparison, in the private sector, it is about 23 percent. So, this begs the question, why is the Federal Government struggling to attract talented young people in particular?"*
>
> *(A More Efficient, 2014, p. 11)*

A large-scale retirement of federal employees could lead to critical skills gaps and loss of institutional knowledge if the federal workforce is not managed effectively in these situations, especially considering the length of time that it takes to hire and train a new employee.

According to a news release from the U.S. Bureau of Labor Statistics, the number of job openings and available positions for both the private and federal workforce has remained relatively steady. The number of hires, however, varied greatly between the Federal Government and the private workforce. While the number of hires increased in the private workforce, it decreased by 13,000 hires in the Federal Government (BLS, April 2017, pg. 2) due in large part to the 2017 hiring freeze. The total separations in the Federal Government decreased from 39,000 in February 2016 to 32,000 in February 2017, translating to a high rate of retention as compared to the private sector, creating an image of more job stability within federal positions, though this factual representation does not always easily translate to the public perception. These numbers show that while turnover in the Federal Government has appeared to remain steady, budget cuts and hiring freezes can be significantly detrimental to the federal workforce as a whole.

Cybersecurity Employment

As United States Chief Information Officer Tony Scott explained in his 2015 blogpost, cybersecurity threats are constantly growing and evolving, and it will take a coordinated, large-scale effort to be able to meet these threats.

The Cybersecurity Sprint which was launched by the Office of Management and Budget was one of the first steps initiated to meet that threat. It was designed to be an initial step towards improving cybersecurity policies, awareness, and eventual hiring across all federal agencies (Scott, 2015). The Cybersecurity Sprint identified two points of concern regarding the existing Federal cybersecurity workforce:

1. *"Federal agencies' lack of cybersecurity and IT talent is a major resource constraint that impacts their ability to protect information and assets; and,*

2. *A number of existing Federal initiatives address this challenge, but implementation and awareness of these programs are inconsistent."*

(Executive Office, 2015)

As a response to these observations, President Obama's 2016 Cybersecurity National Action Plan (CNAP) was meant to effect large-scale changes through a combination of four initiatives tackling education, training, retention, and efforts to meet the needs of the current Federal workforce. These initiatives included: the establishment of a Commission on Enhancing National Cybersecurity, a $3.1 billion Information Technology Modernization Fund, a campaign to help Americans secure their online accounts, and a $19 billion investment in cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget.

Additionally, the CyberCorps Scholarship for Service program was developed to help standardize and improve core curriculum for cybersecurity training at colleges across the country. This included grants and funds to assist academic institutions in hiring quality professors and educators that could help to build and strengthen the education programs dedicated to cybersecurity nationwide (Cobert, 2017).

To improve hiring and recruiting within not just cybersecurity but also STEM and IT fields, CNAP focused on increasing efforts to recruit a more diverse and better trained workforce. This included a focus on reaching out to veterans, women, and minorities to diversify the force as well as working with academia and the private sector to increase the pathways into federal service from different sources such as underserved communities. CNAP also focused on altering the Presidential Management Fellows program to include a cybersecurity component. The intent behind this was to attract and retain top talent and managers in the field who would be able to craft the high-functioning teams needed in agency cybersecurity departments (Cobert, 2017).

The Presidential Management Fellows (PMF) - STEM Track was an experimental track focused on the grooming and training of key management talent in the STEM fields, in order to close the mission critical skills gaps in science, technology, engineering and mathematics (OPM, November 2016). This was part of the Pathways program, which was developed to provide pathways into federal service for people at all levels of the hiring ladder: college students seeking internships, recent graduates looking for a first job, middle management looking for a career shift or advancement, and even senior management looking to develop further (Cobert, 2017). The PMF STEM Track was piloted with the PMF Class of 2014 and was retired with the class of 2017 due to limitations on appointments and pay rates for those who selected the STEM Track. PMF candidates who chose the STEM option cited the desire for more freedom with their appointments and felt that the STEM Track restricted their options ("2017 Assessment Preparation Guide," 2016, p. 1).

The Federal Cyber Workforce Effort was developed by OPM to create a government-wide orientation program that can be implemented for new employees in all agencies (Cobert, 2017). This would allow for ease of information sharing and the establishment of uniformity and understanding across agencies, as well as create a consolidated training base that each employee can draw on to create understanding across agencies. This would directly tie into the concept of "swarming" and shared services across agencies, as there would be a basic understanding amongst all federal cybersecurity talent. In addition to creating uniform initial training for employees, the Workforce Effort would also focus on increasing the availability and usage of special pay rates, hiring and pay flexibilities, and training and development opportunities that could be critical to increasing the institutional knowledge.

Budget and Resources

The Federal Government seems to recognize the need to recruit and retain a high quality workforce, especially within the realm of cybersecurity. To this end, many government actors and agencies have begun putting resources toward enhancing and supporting the federal cybersecurity workforce. Under the Obama administration, the President's Budget for Fiscal Year 2016, for instance, included $14 billion in cybersecurity funding for initiatives such as increased cybersecurity integration between federal agencies and partnerships with the private sector ("The President's Budget," 2016, p. 2). President Obama's proposed Fiscal Year 2017 budget continued these priorities, setting aside $19 billion for cybersecurity (The White House, 2016).

It is still unclear exactly what kind of emphasis the Trump administration will put on cybersecurity and the federal cybersecurity workforce. According to the Associated Press, President Trump stated that he would be putting together a team to study the issues as well as develop cybersecurity training for all federal employees (Abdollah & Superville, 2016). Regarding the federal workforce more generally, President Trump has stressed the importance of efficiency and a lean government workforce. In fact, within his first one hundred days in office, President Trump implemented a federal hiring freeze, which applied across the Federal Government and exempted only select groups, including Department of Defense cybersecurity professionals as well as national security and military professionals. When the hiring freeze was lifted in April 2017, the Trump administration sent a memo to all federal agencies ordering the development of plans for employment cuts. According to NPR's *Marketplace*, typically when aggressive federal workforce cuts have occurred in the past "the number of government contractors ended up increasing as the number of federal workers got slashed" (Uhler, 2017, p. 2).

Depending on how President Trump chooses to prioritize cybersecurity employees, this could drastically change the hiring landscape for federal agencies seeking to attract and retain top cybersecurity talent. The 2017 Continuing Resolution, federal hiring freeze, and potential government shutdown created a high level of uncertainty with respect to federal employment. In addition, reductions in the federal workforce from both sequestration and "leaning" of the workforce have resulted in a decrease in satisfaction with the Federal Government as an employer (Goldenkoff, 2014, p. 22).

Regulation and Policies

As the government becomes more digitized and reliant on technology, numerous policies and reports have been put forth by the Federal Government outlining cybersecurity strategies and recommendations. Many of these regulations and recommendations include directives about the cybersecurity workforce. For instance, the Cybersecurity Act of 2015 required federal agencies to "identify and mitigate skill shortages" among the federal cybersecurity workforce ("Cybersecurity Act," 2015). Additionally, the White House's 2016 Cybersecurity National Action Plan (CNAP) created long-term cybersecurity strategies, including the creation of the Commission on Enhancing National Cybersecurity, a group containing both industry and academic experts as well as former government officials (The White House, 2016). In its 2016 "Report on Securing and Growing the Digital Economy," the Commission recommended the development of a program to train 100,000 new

cybersecurity professionals by 2020 to meet the nation's projected cybersecurity workforce needs (Commission on Enhancing National Cybersecurity, 2016, p. 34).

The Cybersecurity National Action Plan (CNAP), started in 2016 by the White House Administration under President Obama created a roadmap for increasing the federal cybersecurity workforce, as well as shoring up the nation's cybersecurity defenses. According to Clifton Triplett, the Senior Cybersecurity and Information Technology advisor for OPM, "The CNAP roadmap will better enable OPM to build on our cybersecurity partnerships across government and will fortify our efforts to empower agencies to hire the cyber talent they need" (Triplett, 2017). This will be accomplished through increased collaboration amongst agencies, building off of the start from the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT). This team is an example of the "swarming" concept explained by Ms. Jane Holl Lute in our interview, in which she described the pooling of various agency's cybersecurity resources in a time of crisis to be better able to meet and control threats to the system (J. Lute, telephone interview, April 28, 2017).

In addition, CNAP calls for the establishment and utilization of the shared services model, directing DHS to further increase the availability of these resources to support the Federal Government as a whole. According to Mr. Triplett, "The President wants to take individual agencies like OPM out of the business of building their own new security services or capabilities when there is an opportunity to leverage the collective strength and power of the Federal Government" (Triplett, 2017).

Another important facet of the Cybersecurity National Action Plan is its emphasis on cybersecurity training and education. Government officials at multiple levels have voiced the concern that the basic education in cybersecurity is not sufficient to craft the predictive and responsive cybersecurity force that the Federal Government needs to be able to adequately respond to threats. As Mr. Jabbour noted, the training offered in colleges around the country is basic, and students do not graduate with the skills necessary to handle large events and threats. Students require hands on event management training to be able to properly triage, manage, and respond to an event, however this training is only available when an actual event occurs (M. Jabbour, telephone interview, April 20, 2017). In its research into cybersecurity, DHS identified a select few college programs that were providing the training requisite, such as the University of Tulsa, but those training programs and pipelines do not produce enough graduates to staff the full workforce needed in the public and private sectors. As Ms. Lute identified, one of the best options is to identify the programs that are training very successful employees who

have the attributes necessary to provide high-level cybersecurity support and functionality, and model future programs off of this. (J. Lute, telephone interview, April 28, 2017).

CNAP provides for an additional $62 million dollars in FY 2017 funding specifically allocated for cybersecurity education (Cobert, 2016). If these funds were to be utilized to transfer the best practices found from studying successful programs and promulgating that around the country, the amount of well-trained cybersecurity employees could increase significantly. Additionally, research can identify the attributes and traits found in successful cybersecurity employees, and look for those traits in other career fields. Once potential applicants who embody the necessary skills have been identified, they can be trained using a best-practices training model, and this can significantly increase the workforce and labor market. These, and other tools identified in CNAP, will allow the federal government to increase and scale the workforce (J. Lute, telephone interview, April 28, 2017).

Workforce Planning

According to the GAO, many of the Federal Government's cybersecurity workforce problems stem from the fact that "the federal government needs to expand its cyber workforce planning and training efforts" (Wilshusen, 2017, p. 10). Workforce planning requires both an understanding of the current state of the workforce as well a clear definition of the skills and training necessary for a successful cybersecurity workforce. Although certain departments, such as the Department of Homeland Security, have engaged in some cyber workforce planning, this effort has not been undertaken government-wide. In fact, the Office of Personnel Management is not even completely clear on the number of cybersecurity employees actually in government and "has asked agencies...to begin to inventory the employees who are actually engaged in cybersecurity work" so they can better define the government's cybersecurity workforce needs (Partnership for Public Service & Booz Allen Hamilton, 2016, p. 2). A cohesive strategy and plan is needed to better understand the cybersecurity workforce challenges the government currently faces as well as to better plan for recruiting and retaining talent government-wide.

Case Studies

As referenced in the Data and Methodology section, four criteria were used to select the three case study agencies: size, type of information protected, cybersecurity issues and initiatives, and compliance with federal cybersecurity regulations and guidelines. The regulations and

guidelines that apply to the last criteria include the Federal Information Security Modernization Act of 2014 (FISMA) (which amended the Federal Information Security Management Act of 2002) as well as President Obama's Cybersecurity National Action Plan (CNAP).

FISMA is overseen by the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). OMB is responsible for setting "standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk" (Carper, 2014) while DHS is responsible for overseeing the implementation of these policies. According to the Office of the Inspector General, "FISMA focuses on program management, implementation, and evaluation of the security of unclassified and national security systems. As required by FISMA, each agency must develop, document, and implement an agency-wide security program" (Office of Inspector General, 2015).

President Obama's Cybersecurity National Action Plan (CNAP) outlined additional guidelines and requirements, including requiring agencies to identify and fix their areas of highest cybersecurity risk as well as directing the Department of Homeland Security and the General Services Administration to lead efforts to improve IT and cybersecurity shared services.

U.S. Department of Homeland Security

The U.S. Department of Homeland Security (DHS) was formed in 2002 as a response to the September 11th attacks. DHS was intended to bring together all federal agencies with homeland security missions (which ended up being twenty-two agencies) under one umbrella. Because each of these twenty-two agencies had their own cultures, systems, and processes, it proved difficult to unite them under one DHS (England-Joseph & Heinzer, 2014, p. 18). Redundancies, miscommunications, and back-end misalignments were common, and in 2003 DHS was placed on the GAO's "High Risk List," which outlines federal agencies and processes that are particularly vulnerable to "fraud, waste, abuse, and mismanagement, or are most in need of transformation" ("High Risk List," 2017). As of 2017, according to the GAO, DHS has made progress on many of its vulnerabilities but remains on the High-Risk List due to issues remaining around acquisition management, IT management, and financial management (Gambler, 2017, p. 363). DHS has committed to addressing these problems through its Integrated Strategy for High Risk Management report, the latest version of which was published August 2016 and outlines

strategies for continued integration and strengthening of management functions (Deyo, 2016, p. i).

DHS is also subject to the Cybersecurity Workforce Assessment Act, which requires the DHS Secretary to assess the state of the agency's cybersecurity workforce every year through 2017 by collecting data on vacancies, workforce readiness, training, and types of workers (full-time, contractor, etc.). With this data, the Secretary must create a strategy (referenced above) to "enhance the readiness, capacity, training, recruitment, and retention of DHS's cybersecurity workforce" (Meehan, 2014). The Secretary must submit his or her findings to Congress as well as all plans for improvement.

Agency Characteristics

The Department of Homeland Security manages a total discretionary budget of $66,801,948 to complete its five main missions using 22 sub-agencies. These five main missions are as follows:

- *Prevent terrorism and enhance security.*
- *Secure and manage our borders.*
- *Enforce and administer our immigration laws.*
- *Safeguard and secure cyberspace.*
- *Strengthen national preparedness and resilience.*

(DHS, 2016, p. 1)

These missions are supported by a diverse workforce spread among 22 sub-agencies that include U.S. Customs and Border Patrol, the Transportation Security Administration, U.S. Coast Guard, FEMA, and many more. Total, DHS employs 226,030 full-time equivalent employees according to the 2017 Budget-in-Brief (DHS, 2016, p. 98).

DHS maintains a centralized cybersecurity office organized under the National Protections and Programs Directorate (NPPD). DHS also maintains and utilizes its National Cybersecurity and Communications Information Center to share critical cybersecurity information across all participating levels and agencies of government, consistent with recent directives from the President. The NPPD was established in 2007 and is comprised of 3,592 employees, and relies on a budget of $3,044,846,000 annually to conduct its operations (DHS, 2016, p. 26).

Information Responsibilities

With such a wide array of sub-agencies and services provided to the public, DHS is responsible for a variety of different types of information security. From classified documents of all levels within the U.S. Customs

and Border Patrol and the U.S. Coast Guard, to anti-terrorism efforts supported by the Countering Violent Extremism activities, there is no shortage to the variation amongst the types of data DHS must safeguard. A large amount of highly classified and sensitive information is contained within the records of the Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) office, and this is no less important than the private personal data accessed by the office of Immigration and Customs Enforcement. Because of this, the missions of DHS's cybersecurity professionals are extremely relevant and crucial to the protection of the information accessed on a daily basis across the Department.

Issues and Initiatives

DHS has conducted a significant amount of research into issues, best practices, and future plans for implementation concerning both cybersecurity practices as well as hiring, employment, and retention. DHS is continually developing programs and initiatives that are then copied and implemented into other agencies. Their Continuous Diagnostics and Mitigation Program, Einstein 3A, and Scholarships for Service programs have set the gold standard for other agencies to emulate.

The Continuous Mitigation and Diagnostics Program is a security enhancing, evaluative program that can be used to secure agency networks and the IT systems utilized within the Federal Government. It secures the users on government networks by allowing federal agencies increased operability to monitor and control user access and privileges, and better identified unauthorized users, activities, or other threats to the system in near-real-time. In its early phases, the system covered over 50 percent of the Federal Executive Branch civilian workers, and later iterations covered over 97 percent of the same. The CDM has since been passed on for implementation at over 60 Federal civilian agencies (Office of the Press Secretary, 2015). DHS has allocated $274.8 million of its FY-2017 budget to support the ongoing operation of CDM (DHS, 2016).

The revolutionary aspect of the CDM is its ability to be predictive: to sense early threats to the system to secure and neutralize the threat. By notifying agency cybersecurity professionals of a threat, they are better able to respond. Privacy issues can be a concern with this system, as it allows the agency full access to the activity of each user, but this is circumvented with user agreements.

Another system that works hand in hand with the CDM is the development of EINSTEIN 3A. This is an intrusion prevention system that detects and blocks cybersecurity threats before they have the ability to cause damage or infiltrate the networks. In 2015, the EINSTEIN 3A system

was implemented across fifteen executive branch departments, with growing numbers and government-wide implementation continuing (Office of the Press Secretary, 2015). DHS has allocated $471.1 million of its FY-2017 budget to maintain and continue to build the National Cybersecurity Protection System (EINSTEIN 3A) (DHS, 2016). These cutting-edge cybersecurity initiatives are being implemented for effective use across federal agencies, and are evidence of the benefits of institutional knowledge sharing.

Not only does DHS lead in the programming and application sector, but DHS has also implemented critical work stream improvements to address five of the main issues they feel pertain to building their workforce. The five work streams identified were as follows:

> *1 - How does DHS hire, train, and evaluate employees to the standards that are required to be successful in the position?*
>
> *2 - How does DHS open up a pipeline with academia and industry to create a flow through to the government of existing knowledge and expertise?*
>
> *3 - How does DHS strategically manage this higher skillset inherent with successful work as a cyber professional? Can this worker be shared amongst other agencies as needed?*
>
> *4 - How does DHS rewrite contracts for services that better identify the needs of the agency and the requirements of the workforce to better manage procurement and acquisition of top talent?*
>
> *5 - How does DHS strategically manage the workforce to meet the requirements of event management in a time of crisis? How does DHS swarm when a difficult problem arises?*
>
> *(J. Lute, telephone interview, April 28, 2017)*

As referenced in the fellowships and education portions of this report, DHS supports and funds a variety of initiatives to improve the cybersecurity talent pipeline. This is directly related to the first and fourth objectives identified in the work streams above, in which DHS focuses on employment and training as well as the acquisition of new talent. The National Science Foundation and DHS have both incorporated the Scholarship for Service Program. This program funds scholarships for undergraduate, graduate and doctoral students who are focusing on cybersecurity training, which are repaid by government service following graduation. These scholarships are both an incentive for the student, as well as guaranteed quality talent acquisition for the agency (DHS, 2017).

Additionally, DHS offers DHS Secretary's Honors Program, which is a competitive program offered to entry-level professionals. This program offers unique professional and mentoring opportunities to highly qualified candidates to train them for extended service within DHS. These opportunities include rotational assignments, professional development, and mentorship (DHS, 2017). The variety of unique opportunities and programs within DHS are significant steps towards meeting their strategic goals.

Compliance

DHS is in the unique position of being responsible for the implementation of many cybersecurity policies and regulations as well as also having to comply with these regulations internally. Despite the fact that DHS leads cybersecurity policy in many areas, it still has room for improvement in its own practices. For instance, in 2015 the Office of the Inspector General audited DHS' information security program against FISMA standards. This report found that, while DHS excelled in some areas of cybersecurity compliance, it was still lacking in many others such as "continuous monitoring, plans of action and milestones, security authorization, and configuration management" (Office of Inspector General, 2015).

Office of Personnel Management

The U.S. Office of Personnel Management (OPM) has a much longer history than DHS. The agency's precursor, the Civil Service Commission, was formed in 1883 and split into the Office of Personnel Management, the Merit Systems Protection Board, and the Federal Labor Relations Authority in 1978. OPM oversees civil service personnel information as well as many human resources functions, including attracting and retaining talent in government ("Our Mission, Role & History," n.d.).

In fact, OPM is responsible for oversight across the Federal Government concerning hiring practices, staffing, and recruiting plans. While each Federal agency sets their own strategic plans and workforce goals, OPM assists with the Human Resources (HR) component and oversees all policies created to address these workforce goals. OPM maintains and supports the application process for federal employment through their website USAjobs.com and sets the policies and requirements that each agency must follow when they would like to post a job for fulfillment.

Because it plays such a large role in bringing top talent into government, OPM is consistently a part of many major cybersecurity workforce initiatives alongside DHS and other agencies with a heavy focus on

cybersecurity. OPM is often tasked with collecting data on the cybersecurity workforce, identifying gaps, and developing and implementing strategies to meet agencies' talent needs. According to 2017 GAO testimony before the House Subcommittee on Information Technology, OPM has room for improvement in some of these areas. The report specifically suggested that OPM step up "its efforts to close government-wide skills gaps" and work with agencies to better utilize federal hiring authorities to attract and retain top candidates (Marinos, 2017).

Agency Characteristics

The Office of Personnel Management utilizes a total discretionary budget of $321,254,000 to complete its five main missions. These five main missions are as follows:

- *Directing human resources and employee management services*
- *Administering retirement benefits*
- *Managing healthcare and insurance programs*
- *Overseeing merit-based and inclusive hiring into the civil service*
- *Providing a secure employment process*

(OPM, February 2016, p. 1)

These missions are supported by a workforce of 6,192 full-time equivalent employees according to the 2017 Congressional Budget Justification (OPM, February 2016, p. 10). The total discretionary budget included a requested $21 million to "permanently sustain agency network upgrades and security software maintenance to enhance the strength, reliability, and protection of OPM's network architecture" (OPM, February 2016, p. 3).

Information Responsibilities

As OPM manages not only retirement information and workforce data, but also conducts and manages all federal employee security clearances, OPM is responsible for a very large amount of Personally Identifiable Information (PII). According to their internal Cybersecurity Action Report, "OPM stores more Personally Identifiable Information (PII) and other sensitive records than almost any other Federal agency. This is a tremendous trust placed in the agency by the millions of current and former Federal employees, and one that OPM must continually earn through constant vigilance" (OPM, June 2015, p. 7). Because of this, OPM is both critically reliant on the protection of cybersecurity professionals and initiatives, as well as particularly susceptible to cyber threats and information breaches.

Issues and Initiatives

In 2015, OPM experienced two different cybersecurity incidents that resulted in the substantial compromise of Federal employee data. In early 2015, 4.2 million employee records were hacked, including personal information such as addresses, Social Security numbers, full names, and dates of birth. In June 2015, the agency experienced a second data breach, this time including the background checks, Social Security numbers, and fingerprints of 21.5 million employees, contractors, and other personnel.

These incidents drew a large amount of public attention and criticism, and OPM worked to mitigate the problem in a number of ways. First, the agency developed their own Cybersecurity Action Report, in which they identified fifteen objectives and steps that would significantly improve the security of their systems. These key objectives included the following two work streams related to increasing the strength and knowledge of their cybersecurity workforce:

- *"Bringing in management and technology expertise by adding experts from around the Government to help manage its incident response, provide advice on further actions, and ensure that Congress and the public are kept fully up-to-date on ongoing efforts.*

- *Helping other agencies hire IT leaders to ensure they can acquire the personnel needed to combat evolving cyber threats. This includes leveraging tools and flexibilities such as direct hiring, excepted service hiring flexibilities and critical pay authority to bring IT and cyber experts from the private sector into the Federal Government quickly and efficiently."*
  (OPM, June 2015, p. 4)

In its report, OPM not only addressed issues related to the actual security of its network, but also issues related to building a strong talent pool and increasing institutional knowledge. The agency recognized the importance of attracting and retaining top cybersecurity talent to respond to (and ideally prevent) such incidents in the future.

To help close the identified cybersecurity skills gap, OPM built and nourished relationships with academia and higher education to focus on bringing in top talent at the entry-level positions. The Master of Science in Information Security Operations was one example of this: the degree would be offered at a discounted rate of 50% of the original cost and at an accelerated schedule to allow Federal employees to attain further knowledge and learning on the critical topic. This opportunity was key to helping build individual knowledge and the growth and development of

federal employees, while shoring up the gaps in institutional knowledge (Cobert, 2016).

OPM also responded to the threats to their network by hiring a new Chief Information Officer, as well as creating the specialized position of Chief Information Security Officer who was tasked with focusing exclusively on the protection of OPM's most sensitive data.

OPM took note of best practices identified in the Department of Homeland Security, and, in Fiscal Year 2016, implemented DHS's EINSTEIN I, II, and 3A programs, as well as the Continuous Diagnostics and Mitigation programs. It also established a consolidated Security Operations Center, much like DHS's National Cybersecurity Communications and Information Center; a 24-Hour manned space that is capable of responded to threats as they arise, ensure timely response and control of the situation (OPM, 2016).

Most recently, OPM launched the website CyberCareers.gov, an applicant website particularly dedicated to cybersecurity roles and careers. This website is still in its infancy, but is intended to be a separate avenue for entry-level employees to hone in on the available cyber positions in federal agencies (Cobert, 2016).

Compliance

OPM was most recently audited for FISMA compliance by the Office of the Inspector General (OIG) in 2016. OIG found both issues and opportunities in this audit. One key highlight was that OPM's "Information System Security Assessment and Authorization," which the agency uses to evaluate whether its security measures are adequate to protect its systems, had not been completed for "at least 18 major systems" within the agency. This has been a consistent problem in OPM's FISMA audits, and in 2016 OPM began an "Authorization Sprint" to address this problem and bring all its systems into compliance. OIG did recognize that OPM was working to install a continuous monitoring program that would someday replace its information security authorization program.

Additionally, OIG noted that in FY 2016, OPM had trouble meeting many FISMA requirements that it had easily met in years past regarding information security management. OIG attributed these issues to that fact that OPM has had high turnover of its cybersecurity management staff, and therefore, there has been limited personnel available to make sure OPM stays in compliance with FISMA ("Federal Information," 2016, p. i).

Other issues identified by OIG were a lack of definitions around IT roles and responsibilities and a lack of required training for "many individuals

with significant information security responsibility" ("Federal Information," 2016, p. ii). Additionally, most of OPM's Plans of Actions and Milestones were found to be at least 120 days overdue. Despite the fact that OPM specializes in workforce management and training, it is experiencing significant problems in these areas with regard to cybersecurity.

Case Study Conclusions

These case studies have exposed the variety of needs among agencies within the Federal Government to control and protect information. Even agencies such as DHS and OPM, which specialize in, develop, and often oversee many aspects of cybersecurity workforce improvement, struggle with securing their own systems and maintaining their own cyber workforces. These are clearly difficult problems that, no matter how big its staff or budget, one agency may not be able to solve on its own.

OPM's 2015 data breaches provided an illustrative example of the consequences of poor cybersecurity practices. It can be difficult to make cybersecurity a priority when all systems seem to be working. However, taking proper preventative measures and doing continuous monitoring, as advised by DHS, can help ensure events like this do not repeat themselves at OPM or other agencies. In fact, other agencies can learn from where DHS and OPM are still struggling with their cybersecurity efforts as well as mistakes made by OPM and DHS, to improve their own systems and improve their cybersecurity workforce management strategies.

Employment Models

Case studies provide a glimpse into how certain federal agencies are dealing with cybersecurity workforce challenges; in addition to the ideas mentioned in the case studies, there are many other options and opportunities that various agencies as well as nonprofits, universities, and private sector companies have used or considered to improve the recruitment and retention of cybersecurity professionals.

Below, the team has synthesized the main issues that have been consistently cited in the literature regarding cybersecurity workforce attraction and retention problems. These issues have been analyzed both in terms of steps the Federal Government is currently taking to make changes as well as possible future steps or employment models the government may consider, keeping in mind feasibility and implementation issues.

1: Pay, Benefits, and Opportunities for Advancement

Current Model: Pay

The General Schedule (GS) pay system is the predominant system of pay and salary utilized by federal employment and is based on the objective metrics of the difficulty of the job, education level required to perform the job, the responsibilities inherent in the job, and the qualifications that are required by the job. Currently, 71.39% of federal employees are hired under the General Schedule, 8.83% under federal wages systems, and 19.28% have been hired under other conditions, such as special hiring authorities and flexibilities. Recently, a number of special hiring authorities and flexibilities were implemented for the hiring of cybersecurity professionals, and cybersecurity professionals, when applicable, may also be hired under the special rate exceptions. These special rates allow employees to be hired at a higher rates of basic pay than normal rates, to assist with particular recruiting efforts or to assist in the retention of well-qualified employees (OPM, June 2016).

Salary and compensation differences can be stark between the Federal Government and the private sector for cybersecurity positions. Due to the special rates and hiring flexibilities used the by the government, it can be difficult to nail down exact numbers, however, in 2013, the Bureau of Labor Statistics identified that the public sector mean hourly wage for an Information Security Analyst (BLS position 15-1122) was $34.72, and the mean salary was $72,210, whereas the private sector numbers were $44.36 and $92,280, respectively. The most recent Bureau of Labor Statistics numbers place the 2016 private sector median pay of an Information Systems Analyst at $92,600 with a mean hourly wage of $44.52 (BLS, March 2017). However, corresponding numbers for the federal workforce are more difficult to find.

According to OPM's website, the GS-2210 Information Technology Management series of positions can range from a GS-5 position to a GS-11 position (OPM, n.d.). Although the pay scales for these positions can be augmented by the special pay rates (and even within each GS position there is flexibility for pay increases based on performance), the team selected the basic information for GS positions for ease of comparison. The 2017 annual base rate for a GS-5, at the highest within-grade step (the maximum salary available in that GS level) is $37,113, with an hourly rate of $17.78. The maximum 2017 GS-11 base rate is $68,025, with an hourly rate of $32.59 (OPM, January 2017). These numbers may be supplemented with the additional benefits and special pay rates, crucial to allowing the government to compete with the salaries found in the civilian sector. According to the self-reporting website, Glassdoor.com, total

benefits packages for an information technology specialist working in the Federal Government are $100,443, but this evidence is not necessarily reliable.

Current Model: Benefits

OPM is responsible for the government-wide administration of retirement benefits. These retirement benefits are an important characteristic of federal employment; 91.49% of federal employees are enrolled in the Federal Employees Retirement System (FERS). This system incorporates three complementary programs to assist Federal Employees in preparing for retirement: a basic benefits plan, social security benefits, and an employee-driven flexible savings plan, otherwise known as the Thrift Savings Plan (TSP). The Thrift Savings 401K Plan (TSP) is a form of 401K in which federal employees contribute money to the 401K via payroll deductions. The government will then match up to 5% of the employee's salary in contributions, based on the amount the employee is contributing. These contributions are tax-deferred and reduce the employee's taxable income. Both social security benefits and the TSP are transferrable benefits that an employee can take with them to employment in the private sector, whereas the basic benefits plan is built around a model of annuities that are determined by one's age and years of service to the Federal Government.

As modern workers prize flexibility and movement within the industry, the ability to transfer retirement savings and 401K benefits as the worker moves throughout the industry can be a critical asset in attracting and retaining talent. The benefit of the TSP and similar flexible 401K plans is that they allow employees to transfer their savings to a new company once they leave federal employment. This ensures continuity of retirement planning and savings, and allows employees in the modern, more mobile workforce, more freedom of movement. However, this plan can only be transferred provided the employee transfers to a company that offers a 401K as a retirement option. If one transfers to a company that does not offer this, he or she must make alternate arrangements: federal employees have the option to keep their savings in the TSP, transfer the funds to a traditional ROTH IRA, or cash out the balance (Thrift Savings Plan, 2017).

Federal benefits also differ in how they compare to private sector benefits based on education level. Once again, benefits were higher in the Federal Government for workers with a high school or bachelor's degrees, however, for those with advanced degrees, benefits were about equal to the private sector (Falk, 2017, p. 2). According to the CBO, the biggest contributing factor to the observed differences in benefits was the Federal

Government's pension plan, which very few private companies offer an equivalent for (Falk, 2017, p. 3). The Federal Government also subsidizes health insurance for retirees, which is also rare in the private sector. The subsidized health insurance plus the government pension means that much of a government worker's compensation is "deferred compensation," which "attract[s] workers who plan to stay with the same employer for many years, because the value of those benefits rises sharply" the longer an employee stays (Falk, 2017, p. 14). However, long-term employment with the government may not be the most attractive option for many cybersecurity experts, and hiring managers need to consider this when crafting pay and benefit options.

Federal employment also includes a wealth of other benefits such as group health care benefits, flexible spending accounts, various work/life balance programs, and a variety of other programs designed to enrich the lives of both federal employees and their families.

Current Model: Advancement

The General Schedule allows for advancement up through 15 levels of its pay scale. However, some federal employees report experiencing a ceiling in their advancement as many jobs are limited to a maximum GS number. As employees work to move up GS levels, this advancement can only occur in jobs labeled as "competitive." Currently, 69.52% of federal employees are employed in competitive positions, and 30.47% are employed in the Senior Executive Service (SES). The Senior Executive Service is reserved for federal leaders and was established by the Civil Service Reform Act of 1978 to "ensure that the executive management of the Government of the United States is responsive to the needs, policies, and goals of the Nation and otherwise is of the highest quality" (OPM 2016). Conversely, competitive employment jobs are open to all applicants, and are appointed based on the applicant's qualifications.

There are both pros and cons to the SES model. Limiting the mobility of top government managers maintains organizational and mission stability and continuity, which allows agencies to set and implement strong long-term policies and practices. Conversely, limitations on mobility may lead to senior leaders feeling trapped in their positions, causing them to either retire or move into the private sector. In this case, the SES member would take his or her expertise and agency knowledge out of the federal government, which currently desperately needs the wisdom of top managers.

Additionally, while SES positions are required to be posted on the USAJOBS website for at least 14 calendar days, they are often already

filled by prior SES employees, as appointment to the SES requires completion of a Candidate Development Program and approval by OPM. This exclusive selection process can be seen as a barrier to employment within the senior levels of management in the Federal Government.

Current Model: Reform Efforts

To assist with hiring a specialized workforce dedicated to cybersecurity, the Federal Government has implemented a government-wide special pay authority, allowing special rates (higher, more competitive salaries) to be authorized for Computer Engineers, Computer Science Specialists, and Information Technology Management Specialists (Reinhold, 2015). When combined with other special authorities, such as relocation allowances, recruitment incentives and retention incentives that have also been authorized for hard to fill positions, HR managers in federal agencies have more latitude in creating packages that can be competitive with the private sector.

Alternative Pay Model: Redistribute Wages

Pay and benefits in the public sector have a reputation for being much lower than the private sector. On the surface, this idea appears true. According to the Federal Salary Council, the gap between base Federal Government salaries and "non-Federal average salaries...was 61.10 percent" (Condrey, 2016, p. 1). However, data from the Congressional Budget Office (CBO) indicates that there is more complexity behind these pay discrepancies than is initially conveyed by the Federal Salary Council numbers. For instance, mitigating factors such as educational attainment affect how much the different sectors pay. Federal civilian workers actually earn more than their private sector counterparts if they have only a high school (34 percent more) or bachelor's degree (5 percent more). However, those with an advanced degree will make about 24 percent more in the private sector (Falk, 2017, p. 2). The CBO argues that if the higher wages being paid to employees with high school and bachelor's degrees were put toward increasing the wages of the most highly educated candidates, not only would the Federal Government be able to match the wages of the private sector, but it would actually "reduce its spending on wages by 3 percent" (Falk, 2017, p. 2). These findings are very important to managers considering how to attract better top cybersecurity employees, many of whom are entering the workforce with advanced degrees.

While fiscally sensible, this employment model of decreasing lower-skilled wages to increase higher-skilled wages is most likely not feasible for the federal government. Decreasing wages at any level of government is

notoriously unpopular, but decreasing lower wages to further increase higher wages seems a near-impossible sell.

Alternative Benefits Model: Increase Flexible Hours

Flexible work hours have been employed with great success in the private sector, being cited by a recent Forbes study as a top employee benefit leading to employee satisfaction. On a limited basis, the Federal Government has begun to employ this, however, the traditional model of employment still relies on eight-hour work days, for a total of forty hours per week. The implementation of flex-hours or an Alternate Work Schedule (AWS), is meant to enable employees to better manage the demands of personal responsibilities and improve work/life balance (OPM, 2017).

OPM identifies Alternate Work Schedules as being comprised of two components. The first, Flexible Work Schedules (FWS), revolves around the idea of core work hours and flexible hours. The core work hours are the specified hours per day that each employee must be at work. This is critical to ensure functionality of the agency and helps to maintain effective workforces with good communication among work teams and agencies. Flexible hours are built into the work schedule to give employees some freedom around their report time for work and their departure from work, thus allowing them to better manage family and personal commitments (OPM, 2017).

By increasing flexible hours options, the federal government could compete with the private sector on a benefit of key importance to employees. Challenges with the flexible work schedule arise in the Federal Government as agencies are often geographically diverse: a lack of overlap in working hours, which could lead to a breakdown in communication and degradation of the agency's ability to complete its mission. This concept would not work effectively for the military, for instance, as they are required to communicate cross-coast on a daily basis. The effectiveness and feasibility of implementation will depend heavily on the mission set of the agency, the geographic diversity of the agency, and the amount of external coordination the agency must balance.

2: Length and Complexity of the Hiring Process

Current Model: Posting a Job

OPM recommends and enforces an eight-step process for creating an opening for employment within the Federal Government. This process takes approximately 80 days, and the following steps must be completed

by the agency hoping to create the listing, in conjunction with OPM. Delays in communication both internally within-agency and externally with OPM, can significantly increase the time it takes for a job to be posted.

Step 1. Validate the Need

To post a job, a federal agency must first validate the need for the position against their agency's workforce and strategic plan. This creates a barrier to employment from the first step in the process, as the manager hoping to fill this vacancy must review the recruitment plans and the skills gap and verify that this cannot be completed by the current workforce.

Steps 2. Create an RPA

Once the need has been identified as valid, the manager then creates a Request for Personnel Action (RPA), which formally requests a job listing be made.

Step 3. Approve Internally

The manager must get the RPA approved internally before submission to OPM. OPM suggests that each of the above steps will take one day to complete.

Step 4. Forward RPA to HR

Once the RPA is submitted, it is forwarded on to the agency's Human Resources (HR) department, who must repeat the same step on a larger scale.

Step 5. Determine Sensitivity

HR is responsible for identifying the sensitivity level and clearance eligibility of the job. This process adds three days, according to OPM's Hiring Process Analysis Tool.

Step 6. Confirm Job Analysis

These steps are then repeated as the Human Resources Office works with the manager to "confirm the job analysis and assessment strategy." During this step, the involved entities identify the critical duties and responsibilities of the job posting as well as the skills a prospective employee must have to fulfill this role. This step adds eight days to the hiring process.

Step 7. Re-Approval

Prior to the job listing being posted on USAJOBS, the posting must again travel to all applicable entities for approval, adding an additional eighteen days to the procedure.

Step 8. Post the Job

The information is combined into a job posting, which will include the agency information, the job information, the skills and assessment tools that will be used to evaluate these skills, as well as a various other relevant information.

Current Model: Hiring a Candidate

In 2007, OPM reported an average length of 102 days to hire an employee, from identification of the need for a position to the filling of that position with a new hire. OPM's more recent numbers cite an 80-day time goal, but the team was unable to find a precise number for the actual current timeline. Comparatively, in 2015, the Society for Human Resource Management estimated that the time from application to hire in the private sector was an average of 22.9 days (Maurer, 2015). The large disparity between the two numbers could be responsible for a significant amount of attrition among applicants to the federal workforce.

The Partnership for Public Service conducted an analysis verifying these findings, showing, in one agency, "hiring a single employee involved 110 steps" ("Civil Service Reform," 2017). Because of factors such as this, the Partnership labeled the federal hiring process as "deeply broken" ("Federal Hiring," 2017). Former Deputy Secretary of Labor Seth Harris supported this assertion, explaining that the length of time between submitting an application to the Federal Government and actually starting a job can be excessive.

Current Model: Security Clearances

This hiring timeline becomes substantially longer for the federal government when the candidate must obtain a security clearance, as many cybersecurity employees who deal with sensitive data must do. To get security clearance for national security investigations, it takes an average of 123 days, for Secret clearance it takes on average 108 days, and for Top Secret clearance, candidates are facing an average of 220 days.

For those who identify as "ethical hackers," the process can be especially extensive because they are so distrusted in the government. One government employee who worked as an ethical hacker explained to the

Washington Post that it took him five years to receive his security clearance because he "had a huge target on [his] back" from his previous job (Peterson, 2015). Mr. Harris confirmed that this arduous process stood in the way of many top candidates being hired.

Current Model: Reform Efforts

In light of these critiques, the Federal Government has undertaken some measures to streamline the hiring process. In 2016, the Competitive Service Act was signed into law, which allows federal agencies to share their lists of top candidates with each other so that competitive candidates can be recruited into different agencies if one agency does not have enough available positions to hire all the top candidates ("Federal Hiring," 2017). Previously, if agencies identified a strong pool of candidates but could not hire all of them, they could not share this talent list with other agencies. Instead, other agencies would have to "go back into the marketplace and go through the whole process again" (Stier, 2014, p. 32), frustrating candidates and further drawing out the hiring timeline. In support of the Competitive Service Act, the Partnership for Public Service explained that, without this policy, agencies were not only competing with other sectors for top talent, but were competing rather than sharing resources ("Civil Service Reform," 2017).

Alternative Model: Interim Security Clearances

To shorten the hiring timeline, one solution is shorter security clearance checks that can be utilized to provide an interim clearance while the longer, more thorough background check is enacted. While waiting for the thorough background check to be completed, after the shortened clearance is done, employees could go through training and work on all but the most sensitive projects. When the full background check is finished, these employees would be prepared to get started immediately on the more sensitive work.

A modified, initial check that provides an interim security clearance could shorten the hiring and approval process, allow employees to begin work sooner, and also increase functionality for the departments. An obvious drawback of this proposal is finding a way to keep limited clearance employees from accessing extremely sensitive data while also having them work on meaningful projects.

The incorporation of this plan would not require the creation of additional programs or policies: the TSA Pre-Check run by the Department of Homeland Security could be used as an effective initial background check model. The TSA Pre-Check program includes a background check, 10-minute personal interview, and fingerprinting, which would allow for the

important initial steps to be completed. Fingerprints would be on file in the case of any emergencies or suspected breaches. A personal evaluation would be satisfied by qualified agents who can assess the external trustworthiness and characteristics of the subject. In addition, the simplified background check would have the opportunity to uncover any potentially disqualifying information.

One consideration with using the TSA model is overburdening the Pre-Check system with a large influx of new employees needing Pre-Screenings. The capacity of the Pre-Check program would need to be carefully evaluated before putting a program like this in place.

3: Negative Perceptions of Government Culture

A common view of the federal workforce is the 'poor image of the Federal Government as an employer' (US Merit, 2007, p. 12). This is based on a variety of concerns, ranging from bureaucracy and difficulty in creating an innovative workspace and solutions to issues, to concerns with the challenges of working in a stagnant workforce (Peterson, 2015). There are also concerns over how it can be difficult for managers to hold employees accountable. The idea that it is both difficult to get hired and difficult to get fired can create a stagnancy to the workforce and can deprive hard workers of their motivation. If a worker observers that poor performers are not held accountable, they may get frustrated and work satisfaction may suffer (Goldenkoff, 2014, p. 15).

In contrast, the private sector enjoys relative freedom in hiring practices, and also freedom in workforce design. This freedom allows workplaces such as Google to craft innovative, engaged work centers, individualized benefits packages, and unique branding that draws in the top echelon of the available labor market. Even though it is not thought of as overly innovative like the private sector, the government does have some strategies available to it to overcome its negative perception problem.

Current Model: "Doing Good"

One of the government's most powerful tools to combat these issues, which it utilizes with success, is its culture and the appeal of public service work and "doing good." Many employees pursue federal employment out of a sense of duty or service to their country. Company culture and commitment to social responsibility has been a topic of much discussion among academics and organizations alike. Young professionals especially seem to have taken an interest in this issue, with 71% citing an employer's "global or community social responsibility" as an important factor when selecting a job (ServiceCorps, n.d.). This is an area where the federal

government naturally shines, as its focus is on bettering the lives of citizens.

According to testimony in front of the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, given by the Honorable Katherine Archuleta, Director of the Office of Personnel Management, "Based on the conversations that I have had and I travel a lot around the country talking to university students—the first one is public service. And the second one, frankly, is the diversity of opportunities within the Federal Government" (A More Efficient, 2014, p. 21).

Alternative Model: Emphasis on Diversity

The incoming workforce is the most diverse in history and values seeing that diversity reflected in the workplace (Gallup, 2016, p. 10). The current cybersecurity workforce, however, is still relatively homogenous. The National Institute of Standards and Technology acknowledged this fact during a 2014 panel on diversity in cybersecurity, explaining that women compose only 8-13% of the cybersecurity workforce, African Americans make up 7%, and Hispanics account for only 5% (Siraj et al., 2014, p. 4). Diversifying, and thereby broadening, the cybersecurity talent pool may increase the supply of cybersecurity professionals and help alleviate the current high unmet demand in both the public and private sectors. Additionally, the government could show that it is a leader in attracting all types of talent by putting an emphasis on diversity initiatives.

The government has begun to craft some programs around increasing diversity in cybersecurity, however, they are limited in scale and scope. In fact, reflecting on the government's current cybersecurity diversity initiatives, a National Institute of Standards and Technology panel recommended more targeted recruitment efforts as well as the creation of mentorship programs (Siraj et al., 2014, p. 7). The Commission on Enhancing National Cybersecurity expanded upon this in its 2016 "Report on Securing and Growing the Digital Economy," advocating for "creat[ing] pathways into the field for underrepresented populations (e.g., women, minorities, and veterans) and older workers seeking career changes" (Commission on Enhancing National Cybersecurity, 2016, p. 33).

One program that may serve as a starting point as the federal government works to bring diversity into its cybersecurity recruitment efforts is President Obama's 2015 initiative "TechHire," which emphasized developing the technology talent pipeline by focusing on non-traditional and disadvantaged individuals. TechHire supports communities and the employers within those communities to train, connect, and hire local

people that may otherwise never be afforded the opportunity to develop technology skills. The initiative focuses on training people quickly (in months rather than years) and working with employers to focus on skills over degrees. The focus of the program is younger individuals (ages 17-29) as well as "disadvantaged groups with barriers to employment, including veterans, people with disabilities, people with limited English proficiency, and people with criminal records" ("TechHire Initiative," 2015). Since its founding, the program has grown substantially, with 4,000 participants finding tech jobs paying above the average median wage in the private-sector (Burke, 2016). The cybersecurity field may be able to use a similar model, pulling talent, as President Obama stated, "from the unlikeliest places" ("TechHire Initiative," 2015) to fill its many open positions.

4: Limited & Poorly Trained Talent

Current Model: Improving Education

One method the Federal Government has identified of increasing the pool of qualified cybersecurity talent is to invest in cybersecurity education. The Federal Government has created numerous programs and initiatives with this goal in mind. One such program is the National Initiative for Cybersecurity Education (NICE), which "focus[es] on cybersecurity workforce education, training, and career development" ("About NICE," 2015). Created in 2010 to address recommendations from President George W. Bush's Cyberspace Policy Review and Comprehensive National Cybersecurity Initiative, NICE is a public-private partnership that draws on the resources and ideas from the public, private, and academic sectors to train qualified cybersecurity talent and direct them toward careers in both the public and private sectors.

Another federal initiative, run by the Department of Homeland Security (DHS) and the National Security Agency (NSA), is the National Centers of Academic Excellence (CAE) program, which identifies universities with top cybersecurity programs based on how well they achieve "cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field" ("National Centers," 2017). By encouraging schools to meet the requirements of this prestigious designation, the Federal Government hopes that more students will have the opportunity to attend high-quality cybersecurity programs.

In 2013 DHS created the Secretary's Honors Program Cyber Student Volunteer Initiative, which allows both undergraduate and graduate students to volunteer in DHS field offices for ten weeks over the summer and gain valuable cybersecurity skills and connections. The students are

given training, mentoring, and professional development opportunities as a way to "expand the pipeline of future cyber talent" ("Cyber Student Volunteer Initiative," n.d.). According to DHS, the program is highly competitive and accepts only about fifty students per year ("Cyber Student Volunteer Initiative," n.d.).

In conjunction with NICE (as well as the National Centers of Academic Excellence (CAE) program and National Cybersecurity Workforce Framework), the Department of Homeland Security also created an educational resource entitled the National Initiative for Cybersecurity Careers and Studies (NICCS). NICCS is a cybersecurity training platform meant to "provide the nation with the tools and resources necessary to ensure the Nation's workforce has the appropriate training and education in the cybersecurity field" ("About NICCS," 2017). The website connects users to trainings and certifications offered by both the private and public sectors as well as scholarships and cybersecurity competitions.

In 2016, President Obama created an education initiative called Computer Science for All, which invests in a strong computer science curriculum, including cybersecurity, for students in kindergarten through high school. This initiative provides support to schools and teachers to develop their skills as well as develop coursework around computer science. It also engages state-level policy makers and experts in the private sector to provide additional support to schools (Smith, 2016).

Similarly, the National Security Agency and the National Science Foundation jointly fund a program called GenCyber, a cybersecurity camp for kids grade k-12 to develop their cybersecurity skills. According to the Commission on Enhancing National Cybersecurity, exposing children to cybersecurity early can help encourage them to pursue cybersecurity careers later in life (Commission on Enhancing National Cybersecurity, 2016, p. 35).

With the goal of attracting more young people to the cybersecurity field, the National Science Foundation also funds a program called CyberCorps: Scholarship For Service, which offers merit-based scholarships that often cover full tuition for students pursuing cybersecurity degrees ("CyberCorps," n.d., p. 2). This program has been so successful that some states have modeled similar programs after it (Commission on Enhancing National Cybersecurity, 2016, p. 34).

To support students in cybersecurity, the Federal Government has invested in student loan forgiveness for cybersecurity professionals (The White House, 2016). However, the Commission on Enhancing National Cybersecurity asserts that more can be done in this area. The Commission

suggests the government and private sector form a partnership to either cover the cost of students' cybersecurity education or reimburse or reduce their student debt. One option for crafting this model is to cover cybersecurity education costs if the student works for a short time in the government and then moves into the private sector; that way both sectors reap the benefit of their investment (Commission on Enhancing National Cybersecurity, 2016, p. 37).

Alternative Model: Increase Fellowship Offerings

In the team's conversation with former Deputy Secretary of Labor Seth Harris, Mr. Harris explained that the current government model is for employees to come into an agency and stay for years and even decades, moving up through the ranks steadily. He suggested that the cybersecurity workforce could do a better job of utilizing short-term fellowship programs or similar models to circulate top cybersecurity talent throughout the government. These fellowships would allow cybersecurity professionals to give back to their country through short-term public service as well as apply best practices from the private sector to the public sector and carry public sector knowledge into private sector jobs.

There has been some progress in creating this type of cybersecurity fellowship. In 2012 President Obama began the Presidential Innovation Fellows program with the goal of bringing top private sector technology talent into the Federal Government for "tours of duty" (The Obama White House, 2015). Throughout their twelve months of service, these "entrepreneurs-in-residence" ("Presidential Innovation Fellows," n.d.) work alongside federal employees to tackle difficult government technology issues using innovate ideas and practices from the private sector. Fellows are usually mid-career technology professionals and work on a broad variety of issues, including cybersecurity. A current project being spearheaded by a group of Presidential Innovation Fellows and a team at the FBI is "building a model [to help] both the FBI and the private sector more effectively manage risk…[shifting] how the FBI engages the private sector…[and] helping to drive culture change within the FBI" ("FBI Risk Management," n.d.).

Although this program is promising, it is limited, and there is more the Federal Government may be able to do to expand upon the fellowship model. One possibility is to "flip" the current fellowship model and allow public sector workers to spend time in the private sector to learn best practices and new ideas that they can then bring back to government. Betsy Cooper, executive director of the Center for Long-Term Cybersecurity at the University of California, Berkeley, proposes a model in which public and private sector cybersecurity employees switch jobs for

a year or two. During this time, she argues, public sector employees with gain an understanding of private sector culture and practices and private sector employees will gain an appreciation for "the importance of government problems and the importance of working on these issues in the public sector" (Naylor, 2016).

It is important to note that there are some barriers to rotational programs with the private sector. Companies may have non-disclosure agreements with their cybersecurity employees that prevent them from sharing best practices or ideas with their public sector counterparts. It can also take a very long time for security clearances to process, making quick rotations not very feasible. Additionally, if private companies are bidding on government contracts, possible conflicts of interest may emerge when they share employees or take in government employees (Commission on Enhancing National Cybersecurity, 2016, p. 36).

ServiceCorps, a New York City-based nonprofit, created another alternative fellowship model that utilizes private sector partnerships in a unique way. ServiceCorps “partner[s] with leading corporations to ‘secure and defer’ top undergraduate job offers so that emerging leaders can serve for one year at the finest nonprofit and public organizations” (ServiceCorps, n.d.). Participants receive a salary, living stipend, and ongoing professional development throughout their year of service, and after the year is up, participants begin their private sector jobs, which have been held for them by their employer.

ServiceCorps and its corporate partners note the many benefits of this model. Employers find the program helps overcome what they often term a “leadership gap,” in which young professionals, while very bright, often do not have enough experience leading in professional organizations to really “hit the ground running” when they begin their first job (ServiceCorps, n.d.). Because ServiceCorps participants are placed in high-impact roles in the public sector, these young professionals begin their private sector jobs with more experience, maturity, and transferable leadership skills than those that did not go through the program. This experience and maturity are incredibly valuable to employers as it decreases training time and creates competent leaders with experience solving difficult problems. Additionally, employers recognize that young professionals today are increasingly interested in giving back to their communities but do not want to forgo their careers to do it. By partnering with ServiceCorps, companies can demonstrate their commitment to public service, which is attractive to candidates, and participants have the opportunity to spend time serving their community without sacrificing their careers. Also, both ServiceCorps and its corporate partners recognize the need to strengthen the talent in the public sector and create linkages

between companies and nonprofits and government. ServiceCorps participants are top performers who the public sector would otherwise never have been able to attract due to their salary requirements. With the "secure and defer" model, these top performers are able to create lasting change in the public sector. Plus, when they are finished serving, these young leaders bring back their public sector knowledge to their companies and help facilitate continued interactions and partnerships between the sectors.

ServiceCorps stressed that the key to the successful creation and implementation of this model is to require corporations to nominate potential ServiceCorps participants, who must then apply to the program. By requiring a company nomination, it increases the prestige and honor of the program and ensures that truly the best talent will be coming into the nonprofit and government organizations ServiceCorps works with. Plus, if young professionals were allowed to apply without a company nomination, it may create a very self-selecting group that was already committed to public service. Through the nomination process, companies may encourage young leaders who had never given much thought to public service to work in and ideally become an advocate for the public sector.

ServiceCorps acknowledges that one challenge of this program is that, because the year of service is paid for by the sponsoring nonprofit or government agency, it can often be lower than participants would like, especially considering their comparative private sector salaries. However, because they choose top nonprofits and government institutions to work with who can often pay a fair wage, ServiceCorps says the salaries are still usually competitive enough to attract most candidates. This is a consideration the Federal Government would need to take into account when considering crafting a similar program.

Alterative Model: Apprenticeships

An area where the Federal Government could improve in education and training is in apprenticeship programs, according to Maine Senator Susan Collins (Duhigg, 2017). The Commission on Enhancing National Cybersecurity agreed with this recommendation, suggesting a national apprenticeship program "to train 50,000 new cybersecurity practitioners by 2020" (Commission on Enhancing National Cybersecurity, 2016, p. 35). The Commission recommended such an apprenticeship program be open to those both within and outside academia who have superb technical skills but little knowledge or skills in cybersecurity. Aimed at entry and mid-level professionals, this program would have participants shadow cybersecurity experts in both government and private companies so that

they gain broad expertise (Commission on Enhancing National Cybersecurity, 2016, p. 35).

Alternative Model: Training Managers

According to the Commission on Enhancing National Cybersecurity, another area of potential improvement regarding training is for current federal managers. Even if their role does not directly deal with cybersecurity, the Commission argues that they should be trained in the importance and basics of cybersecurity because cybersecurity is crucial to every agency. Just like finance, human resources, and operations, cybersecurity is a basic piece of knowledge every manager should be expected to have. Armed with this knowledge, they can make cybersecurity a priority and "create a culture of cybersecurity in their organizations" (Commission on Enhancing National Cybersecurity, 2016, p. 35). To make this training effective, the Commission recommends the Senior Executive Service (SES) be the first to undergo the training so that they can be brought on board and then communicate the importance of the training to the managers beneath them.

5: Workforce Structure and Flexibility

According to a 2014 GAO report, "Talent management tools lack two key ingredients for developing an agile workforce, namely the ability to (1) identify the skills available in existing workforces, and (2) move people with specific skills to address emerging, temporary, or permanent needs within and across agencies" (Goldenkoff, 2014, p. 24). By adapting its traditional workforce structure to more flexibly move or utilize employees, the Federal Government may be able to better meet its workforce needs.

Modern workers are not as interested in remaining with one company for their whole career: rather, they are looking to change companies and move around, while remaining in the same career field (J. Lute, telephone interview, April 28, 2017). This can prove difficult for the Federal Government, which is used to having employees join and stay for extended periods of time. However, the government is making efforts to expand its pipeline of talent by offering more short-term employment options. For example, as one of its work streams, DHS is focusing on opening up a pipeline of communication and employment within academia and the private sector industry to allow professionals the opportunity to include time and service to the Federal Government in their career pathways. Establishing this broader pipeline will allow workers the freedom to continue moving throughout the field of cybersecurity while allowing the federal government to partake of the

institutional knowledge available in the private sector. There is much more the Federal Government can do to adapt its workforce structure to changing models in being used in other sectors.

Alternative Model: Crowdsourcing

Crowdsourcing models are used extensively by the private sector, and may have applicability in the public sector as well. To understand crowdsourcing, it is helpful to provide a comparison with outsourcing, which the government utilizes heavily. Outsourcing involves procuring goods and services from an external source while crowdsourcing is merely a more extreme form of outsourcing, relying on a crowd or the public at large to solve problems or accomplish tasks.

The Federal Government currently outsources goods and services through government contracts, which are most commonly fulfilled by a bidding process. Outsourcing allows the government to accomplish tasks and acquire innovations in areas where it may not have expertise as well as experience cost savings when it does not need to develop many expensive talent or products in-house (Su et al., 2016, p. 81). While outsourcing is relatively common in government, crowdsourcing is a newer field and may provide opportunities for workforce innovation as well as efficiency gains in federal cybersecurity. Through crowdsourcing, hundreds of people may work on a problem but are only paid if they find a solution. This ends up being much cheaper than paying the same amount of people a salary to work on the same problem (Miller, 2017).

The Federal Government has begun to explore the crowdsourcing model in a small way very recently. The Pentagon has partnered with a private company that utilizes a remote workforce of highly vetted “ethical hackers” to crowd source the discovery of "security holes across the Federal Government” (Naylor, 2016). The Internal Revenue Service (IRS) began a similar program in 2016 after experiencing numerous cybersecurity incidents (Miller, 2016). Most recently, the General Services Administration’s (GSA) Technology Transformation Service (TTS) is creating a bug bounty program which offers compensation to trusted crowd-sourced individuals who can “find vulnerabilities in [the GSA’s] cloud-based applications” (Miller, 2017).

As the GSA has been learning, cybersecurity crowdsourcing in government is not without its challenges. For instance, there are very few companies that provide comprehensive bug bounty software and services, so vendor selection is limited (Miller, 2017). Additionally, it can be “uncomfortable” (Miller, 2017) to allow hackers into a government system. Agencies often reflect back to the bad press events such as the Snowden leak caused and

feel distrust toward hackers, whether ethical or not. One solution may be to bring vetted hackers in-house as employees, so the person doing the "hacking" is not a frightening, unknown entity.

As they move through the vendor selection and implementation process, it may be wise for the GSA and other federal agencies considering similar bug bounty crowdsourcing programs to consult with private sector companies such as "Google, Facebook, Microsoft, and Yahoo! [that] have found success with this approach" (Miller, 2017).

Alternative Model: Gig Economy

The gig economy refers to project-based work that is often flexible or freelanced. According to the Bureau of Labor Statistics, certain occupations lend themselves especially well to the gig model. Information technology is one of these occupations, as is computer technology (Torpey & Hogan, 2016). The gig economy also allows many workers who were previously "stuck on the margins," such as stay at home parents, the elderly, or people with disabilities, to enter the workforce (Mulcahy, 2016). As of October 2016, "162 million people in Europe and the United States—or 20 to 30 percent of the working-age population—engage[d] in some form of independent work" (Manyika et al., 2016).

An increasing number of companies are utilizing the gig economy through a "blended workforce" model in which "full-time permanent employees [work] side-by-side with freelancers" (Schawbel, 2016). The benefits for organizations include flexible teaming, the ability to bring on short-term talent to quickly solve problems, and the cost savings from not having to pay freelance workers a full salary or benefits (Schawbel, 2016). Freelance workers take advantage of this model to craft their own schedules and work only on the projects they are truly interested in. Centralized contracting companies also make use of the gig economy to contract out workers to jobs in a variety of organizations.

There are obvious drawbacks to the gig model, especially for the worker. Pay is not always steady, and benefits must usually be provided by the freelancer, which can become extremely burdensome. In its 2016 report on the gig economy, McKinsey highlighted these issues, suggesting the government modernize how alternative workers are supported and protected by the government through policies such as "a more portable system of benefits that is tied to workers themselves, not to a single employer" (Manyika et al., 2016, p. 15).

The Federal Government utilizes independent contractors for a variety of projects, but this process is not quick or flexible due to the time it takes to complete the bidding process as well as any additional time needed for

security measures such as clearances. Additionally, despite the fact that The Small Business Administration (SBA) has created online training materials to explain the process, the government contracting process is still very complex and difficult for many independent contractors to navigate ("SBA Learning Center," n.d.). Streamlining the contracting process may bring in a broader pool of talent that the cybersecurity field desperately needs. SBA is working to tackle the under representation of women in federal contracting through initiatives such as ChallengeHer, a conference "designed to educate, empower and provide opportunities for women in Federal Contracting" ("ChallengeHer," 2015). Because the field of cybersecurity is currently struggling to attract diverse talent, the federal government may consider broadening the audience for these types of contracting training to include other disadvantaged groups.

Alternative Model: Shared Services and a Centralized Workforce

Although all federal agencies have information to protect and unique cybersecurity concerns, it may not make sense for all agencies to employ their own cybersecurity workforce. Some agencies with similar cybersecurity processes and challenges may be able to share a cybersecurity team to cut down on the number of cybersecurity employees needed and to lower staff costs and increase efficiency, a stated goal of the Trump administration. Additionally, should they encounter a more sophisticated threat, smaller agencies with more limited budgets would have access to a more comprehensive cybersecurity team than they could otherwise employ. To this end, a shared services model may make sense for some agencies.

President Obama's 2016 Cybersecurity National Action Plan (CNAP) recognized this need, proposing the Department of Defense (DOD) create a Cyber Mission Force, which brings together both military and civilian employees from across military departments to address pressing military cybersecurity concerns. This Cyber Mission Force is expected to be fully functional by 2018 (The White House, 2016).

CNAP also proposed the Department of Homeland Security (DHS), the General Services Administration (GSA), and other Federal agencies "increase the availability" of cybersecurity shared services (The White House, 2016). However, this directive does not seem to have made much progress, as the GSA only lists human resources and payroll on its shared services website ("Shared Services," 2016). DHS' EINSTEIN system addresses the shared services goal to a small extent by providing centralized protection for federal civilian executive branch agencies ("EINSTEIN," 2015), however, the effective sharing of cybersecurity employees has still not been achieved.

There are a few models that may allow the Federal Government to effectively share cybersecurity staff among agencies. Former Deputy Secretary of Labor Seth Harris suggested what he termed a “flying squad,” housed in an agency with a high degree of cybersecurity expertise, such as DHS, that could move quickly from agency to agency as problems arose. The key to implementing such as strategy would be to either give the “flying squad” enough authority to quickly make changes or develop a system for holding agencies accountable for implementing what the shared services team recommended. He explained that in government this could be difficult due to such a strong hierarchical model where those at a higher GS level may not want to take orders from those at a lower GS level.

During her time at the Department of Homeland Security, former Deputy Secretary Jane Lute commissioned a blue ribbon panel to analyze the federal cybersecurity workforce. Based on their findings, Lute created “work streams,” one of which focused on dealing with cybersecurity crises. A recommendation that emerged was to create a standing team that could “swarm” when a large problem occurred. This idea is still being considered in spring 2017 by a number of lawmakers. For instance, Arizona Representative Ruben Gallego recently suggested a “cybersecurity reservist system, like a National Guard for digital security” (Larson, 2017). This Cyber National Guard could include individuals both from inside and outside the Federal Government that both address crises and work on more regular maintenance of the Federal Government’s cybersecurity systems.

One relatively recent instance where an institutionalized “swarming” model would have been useful is with the rollout of HealthCare.gov, the website meant to support the health insurance marketplace outlined in the Patient Protection and Affordable Care Act (ACA), which crashed throughout its launch, threatening the future of the ACA and confusing consumers and insurance companies alike. If the government had had an emergency team in place, the team could have quickly come together to troubleshoot and fix the website. Instead, the Obama administration scrambled to find a solution, during which time the website generated negative press and caused members of the public to lose faith in the ACA (Evans, 2014, p. 7). Finally, the administration reached out to six top private sector experts who formed an ad-hoc team, worked for six weeks straight, and fixed the website. Although not specifically a cybersecurity case, this example illustrates the need for teams to be in place to address IT emergencies when they occur. This case also points to some of the benefits of utilizing experts outside of government when creating swarming teams.

With the HealthCare.gov case, the implementation of a shared services model from the beginning of the project may have been useful to assist the agency charged with figuring out how to make the website a reality: the Centers for Medicare and Medicaid Services (CMS). CMS had no experience or expertise with digital projects of this size or complexity, and therefore made avoidable mistakes throughout the process of selecting a vendor and overseeing the project (Evans, 2014, p. 5). A shared services team with expertise in this area could have been tasked to run the project instead of CMS or could have been used as consultants throughout the process. In fact, CMS' lack of expertise in IT has made HealthCare.gov vulnerable to cybersecurity threats with "316 security-related incidents, between October 2013 and March 2015" (Wilshusen & Barkakati, 2016, p. 1). In the future, agencies like CMS without IT or cybersecurity expertise may benefit from a shared services model instead of attempting to develop such complex competencies in-house.

Although a shared services model initially seems like an easy solution to many of the government's workforce challenges, the logistics and implementation can be quite complex. At the most basic level, there must be an invested, visionary leader to move such a project forward. According to a 2015 report by the Partnership for Public Service and Deloitte, however, most top government leaders do not view shared services as a management priority (Rossmann et al., 2015, p. 7). Additionally, one the biggest issues around combining services is what exactly to do with the inevitable employees who are no longer needed in their current roles due to centralization. Although moving these employees to other positions is ideal, it is not always feasible, and often job cuts and low employee morale become synonymous with the implementation of shared services (Rossmann et al., 2015, p. 21). Other challenges agencies have encountered in the past when trying to create and utilize shared services include a hesitancy to give up control over familiar in-house systems as well as a lack of (or confusion around) agency governance and strategic planning.

To address these issues, the Partnership for Public Service recommends emphasizing transparency and feedback throughout the shared services creation and implementation processes, so agencies feel an element of control over how some of their most crucial functions will be run (Price, 2015, p. 4). The Partnership also recommends creating metrics to evaluate the success of any shared services model, both "in terms of efficiency and effectiveness, but also [its] ultimate contribution to enhancing mission delivery" (Price, 2015, p. 5). By evaluating the success of a shared services program, issues can quickly be identified and fixed, and successes can be shared and possibly reproduced in other agencies or areas. Other noted

best practices include making small changes as opposed to large, drastic ones and making sure there are early "wins" to get agencies on board (Rossmann et al., 2015, p. 1). Overall, to truly transform government through shared services, all participating agencies must be informed and involved throughout the entire process and leadership from the White House down to agency heads must make the successful implementation of shared services a priority (England-Joseph & Heinzer, 2014, p. 24).

The GAO also put together recommendations for shared service groups called integrated program teams (IPT). These teams, common across government, consist of individuals that come together from different departments and areas of expertise to work on a project and create a deliverable. Strong IPTs are defined by the team's makeup and processes as well as supportive and empowering leadership (Powner, 2016, p. 1). This means that the IPT has the resources and empowerment it needs to succeed as well as "cross-functional and multidisciplinary skill sets" (Powner, 2016, p. 1) across the team. Additionally, IPTs must establish strong processes and guidelines as well as involve stakeholders early in their process to make the teamwork process easier. These recommendations can be applied to many different types of shared services teams both inside and outside the government.

6: Lack of Workforce Planning, Definitions, & Strategy

Federal agencies have consistently struggled to coordinate and prioritize efforts around cybersecurity workforce planning. There is no comprehensive government-wide strategy for addressing cybersecurity workforce issues and often the issues and the workforce themselves are not well defined.

Alternative Model: Define the Jobs

Although this seems to be widely recognized by a number of agencies, defining the cybersecurity workforce in terms of job requirements and skillsets may help the federal government better decide how to move forward with recruitment and retention efforts. By focusing on writing and rewriting the contracts for each position to clearly identify the roles and responsibilities of the job, communication between the employer and employee can be clear, and the job positions can be filled by the appropriate applicant or existing worker. The requirements for the job must be outlined clearly for entry level positions, middle level, and career end positions. The metrics used to evaluate, test, and train these positions must also be clearly delineated if the workforce is to be scaled appropriately (J. Lute, telephone interview, April 28, 2017).

Alternative Model: Further Consult with the Private Sector

As the Federal Government considers crafting a comprehensive cybersecurity workforce strategy, it seems prudent to broaden this strategic planning to include other sectors, including the private sector. Both the private and public sectors seem to agree that there is ample space and need for the sharing of ideas and best practices between sectors. In fact, President Obama's Cybersecurity National Action Plan (CNAP) specifically called for the development of a National Cybersecurity Center of Excellence; a public-private partnership meant to address private sector cybersecurity challenges with input from government, academia, and a variety of business leaders (The White House, 2016).

Numerous private technology and consulting firms devote resources to enhancing technology and cybersecurity in government, which the government may use when creating a strategic plan. For example, IBM's Center for The Business of Government supports and facilitates research around how governments can be more effective in their "use of technology and social media, financial management, human capital, performance and results, risk management, innovation, collaboration, and transformation" ("About the Center for The Business of Government," n.d.). The incorporation of partnerships between the Federal Government and partnerships such as this could lead to a highly beneficial relationship. The sharing of best practices would increase institutional knowledge in the aggregate, and would enhance national security.

There are obvious concerns and issues with this, particularly as it relates to classified or sensitive information. However, with shortened security clearances, as was discussed previously, much of this collaboration could be a possibility. While it may not be possible for implementation in every agency and on every mission aspect, the increased knowledge, and alignment between sectors could benefit both sectors and the cybersecurity workforce as a whole.

Recommend-ations for Future Research

Much of the focus of this paper has been best practices, small and large improvements, and additional opportunities to create flexibility in and attract the cybersecurity labor force to Federal Service. This paper identified many pilot programs that agencies have adopted in the last five years, though many of these initiatives need improvements and updates.

The team recommends further research into the efficacy of these programs, and into the long term effects on the workforce.

In future research, the team suggests broadening the scope to include Information Technology and STEM careers, as those careers have also become vitally necessary to assist with the ever-changing missions of many of the government agencies. The end state research would include recommendations and implementation models that can be applied across the Federal workforce in the aggregate.

The employment models highlighted are not all applicable to each of the agencies within the Federal Government. A feasibility study particularly dedicated to the implementation of these models at each variant of the federal workforce is necessary to understand how models will affect the mission completion of the agency. For example, as was earlier discussed, the concept of flex time might not be applicable to incorporation into a military workforce, or a workforce that is geographically diverse.

Further research can be conducted into the actual structure of the workforce: particularly related to Information Technology and Cybersecurity is the truth that incoming employees who have received more recent training often have more in-depth, applicable information that can be applied to the effective completion of their mission. However, the leaders, who have often been in the position longer, are more removed from the actual technology or strategies. Those in leadership positions must be able to lead this more qualified, younger generation, which creates a significant amount of challenges, as the new employees may feel they are more qualified to lead. One solution to this may be the inclusion of programs designed to assist with accelerated career progression and leadership opportunities, or the incorporation of team leading, in which the more senior leader partners with the more relevant junior to lead a team combining the strengths of both. This concept of a reverse mentoring initiative could be very applicable to the cybersecurity workforces within the Federal Government.

The National Aeronautics and Space Administration has been identified as a highly effective, highly content workforce, which is employing a significant amount of new initiatives to revitalize and rejuvenate their administration. Further research or an in-depth case study centered on NASA could uncover models of employment that would be applicable to federal agencies and would have a proven track record of utilizing all resources available to craft a highly effective workforce. These opportunities for future research can further inform the problem and the many a multi-faceted solutions that the Federal Government would be able to incorporate.

Conclusion

The challenges facing the Federal workforce are many, and are hampered not only by current challenges such as hiring freezes and continuing resolutions, but are also hindered by longstanding biases and misconceptions. There are many options available to make adjustments, both large and small, to be able to build and strengthen the Federal workforce. This effort is key, particularly as it applies to cybersecurity: any efforts to build the cybersecurity workforce face their own set of challenges, such as the lack of uniformity in training and the difficulty in competing with the salaries and benefits packages offered in the private sector. This report endeavored to present these challenges and opportunities as they apply to the Federal workforce, and to assess the options for change and the feasibility of these changes.

Appendix I

Bureau of Labor Statistics - Occupational Employment and Wages, May 2016

Position Type: 15-1122 Information Security Analysts

Position Description: Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses. Excludes "Computer Network Architects" (15-1143).

Employment estimate and mean wage estimates for this occupation:

Employment	Employment RSE	Mean hourly wage	Mean annual wage	Wage RSE
96,870	2.4 %	$46.17	$96,040	0.6 %

Industry profile for this occupation: Industries with the highest published employment and wages for this occupation are provided.

Industry	Employment	Percent of industry employment	Hourly mean wage	Annual mean wage
Computer Systems Design and Related Services	27,300	1.39	$46.46	$96,650
Management of Companies and Enterprises	8,820	0.38	$43.73	$90,960
Depository Credit Intermediation	7,080	0.42	$46.18	$96,050
Management, Scientific, and Technical Consulting Services	4,650	0.35	$50.53	$105,100
Insurance Carriers	3,900	0.33	$44.66	$92,880

Retrieved from: Bureau of Labor Statistics 2017. Retrieved April 29, 2017, from https://www.bls.gov/oes/current/oes151122.htm#(3)

Appendix II

Office of Personnel Management - Fiscal Year 2016 Agency Financial Report

Average number of days to complete the fastest 90 percent of all initial national security investigations						
FY 2012 Results	FY 2013 Results	FY 2014 Results	FY 2015 Results	FY 2016 Results	FY 2016 Target	Met/ Not Met
36	35	35	67	123	≤40	Not Met

Explanation of Actual: Contract decisions made in 2014-Q4 have impacted timeliness of all initial national security investigations.

Average number of days to complete the fastest 90 percent of initial Secret national security investigations						
FY 2012 Results	FY 2013 Results	FY 2014 Results	FY 2015 Results	FY 2016 Results	FY 2016 Target	Met/ Not Met
N/A*	28	30	58	108	≤40	Not Met

Explanation of Actual: Contract decisions made in 2014-Q4 have impacted timeliness of initial Secret national security investigations.

*N/A - Not Available - no historical data available for this period.

Average number of days to complete the fastest 90 percent of initial Top Secret national security investigations						
FY 2012 Results	FY 2013 Results	FY 2014 Results	FY 2015 Results	FY 2016 Results	FY 2016 Target	Met/ Not Met
N/A*	80	75	147	220	≤80	Not Met

Explanation of Actual: Contract decisions made in 2014-Q4 have impacted timeliness of initial Top Secret national security investigations.

*N/A - Not Available - no historical data available for this period.

Retrieved from: Office of Personnel Management 2016. Retrieved April 29, 2017 from https://www.opm.gov/about-us/budget-performance/performance/2016-agency-financial-report.pdf

Appendix III

Bureau of Labor Statistics - Job Openings and Labor Turnover - February 2017

Table A. Job openings, hires, and total separations by industry, seasonally adjusted

Category	Job openings			Hires			Total separations		
	Feb. 2016	Jan. 2017	Feb. 2017[p]	Feb. 2016	Jan. 2017	Feb. 2017[p]	Feb. 2016	Jan. 2017	Feb. 2017[p]
LEVELS BY INDUSTRY (in thousands)									
Total	5,566	5,625	5,743	5,447	5,424	5,314	5,183	5,247	5,071
Total private	5,092	5,133	5,235	5,094	5,067	4,968	4,844	4,908	4,730
Mining and logging[1]	8	25	18	21	30	39	43	32	35
Construction[1]	193	142	169	347	387	369	334	361	334
Manufacturing	306	361	364	287	304	305	307	304	292
Durable goods[1]	158	206	209	170	165	156	189	163	155
Nondurable goods[1]	148	155	155	117	139	149	118	141	137
Trade, transportation, and utilities	988	959	910	1,160	1,023	1,089	1,047	1,012	1,035
Wholesale trade[1]	197	201	193	142	140	136	137	150	125
Retail trade	612	581	541	831	682	756	742	670	739
Transportation, warehousing, and utilities[1]	180	177	175	187	201	196	167	192	171
Information[1]	86	73	69	82	80	85	73	87	85
Financial activities	344	388	372	234	220	188	225	198	182
Finance and insurance	253	248	295	165	150	121	163	133	128
Real estate and rental and leasing[1]	90	140	77	70	70	67	61	65	54
Professional and business services	1,107	1,056	1,002	1,076	1,128	1,068	1,072	1,068	1,036
Education and health services	1,050	1,158	1,257	648	646	624	567	639	563
Educational services[1]	110	93	120	108	79	78	94	82	60
Health care and social assistance	940	1,065	1,138	540	567	546	473	557	503
Leisure and hospitality	775	729	808	1,051	1,015	989	1,018	987	974
Arts, entertainment, and recreation	68	83	96	151	146	151	128	135	139
Accommodation and food services	706	646	712	900	869	838	889	852	835
Other services[1]	235	241	267	188	233	211	160	219	194
Government	474	492	507	353	357	346	339	339	341
Federal[1]	87	82	78	44	46	33	39	38	32
State and local	387	410	430	309	312	313	300	301	309
State and local education	145	161	147	147	159	155	160	151	166
State and local, excluding education[1]	242	249	283	162	153	158	140	149	144

Retrieved from: Bureau of Labor Statistics News Release 11 April 2017. Retrieved 29 April 2017 from https://www.bls.gov/news.release/pdf/jolts.pdf

Appendix IV

Comparison of the issues and employment models across the public and private sectors

Issue/Employment Model	Federal Government	Private Sector
Pay	Bachelors and Associates degrees earn more	Advanced degrees earn more
Benefits (focus on retirement)	Federal Employees Retirement System	401k
Opportunities for Advancement	GS scale and Senior Executive Service (advancement in competitive positions only)	Not defined, but assumed less limited
Posting a job (timeline)	80 days, eight-step process	Unknown
Hiring (timeline)	80 day goal, 102 day average	22.9 days
Security clearances (timeline)	108-220 days	N/A
Perceptions of culture	Bureaucratic but public service is seen as "doing good"	Innovative
Improving the talent pipeline	Investment in education	Investment in education
Crowdsourcing	In its infancy - barely used	Used frequently
Gig economy	Government contractors used instead	Used frequently
Shared services	Slow adoption	N/A
Workforce planning	Better alignment needed	Better alignment needed

References

(2011). *Rightsizing the federal workforce: hearing before the Subcommittee on Federal Workforce, U.S. Postal Service, and Labor Policy of the Committee on Oversight and Government Reform, House of Representatives, One Hundred Twelfth Congress, first session, May 26, 2011.* Washington: U.S. G.P.O.

(2014). *Federal workforce: recent trends in federal civilian employment and compensation: report to the Ranking Member, Committee on the Budget, U.S. Senate.* [Washington, D.C.]: United States Government Accountability Office.

(2015). *Federal workforce: OPM and agencies need to strengthen efforts to identify and close mission-critical skills gaps: report to congressional requesters.* [Washington, D.C.]: United States Government Accountability Office.

Abdollah, Tami, & Superville, Darlene. (2016, December 3). Panel urges better cybersecurity to President-elect Trump. *Associated Press*. Retrieved from https://apnews.com/842aa26808a74397ab62b15096ea287b

About NICCS. (2017, March 31). U.S. Department of Homeland Security. Retrieved from https://niccs.us-cert.gov/about-niccs

About NICE. (2015, April). National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/nice/about.html

About the Center for The Business of Government: Connecting Research to Practice. (n.d.). Retrieved from http://www.businessofgovernment.org/content/about-center-business-government-connecting-research-practice

About Us. (n.d.). U.S. Office of Personnel Management. Retrieved from https://www.cybercareers.gov/about-us/

Bureau of Labor Statistics. (2016). Computer and Information Technology Occupations. Retrieved https://www.bls.gov/ooh/computer-and-information-technology/home.htm

Bureau of Labor Statistics. (2017, April 11). Job Openings and Labor Turnover - February 2017. Retrieved April 30, 2017, from https://www.bls.gov/news.release/pdf/jolts.pdf

Bureau of Labor Statistics. (2017, March 31). 15-1122 Information Security Analysts. Retrieved April 29, 2017, from https://www.bls.gov/oes/current/oes151122.htm#(3)

Burke, Ryan. (2016, December 2). What's Next for TechHire [The White House]. Retrieved from https://obamawhitehouse.archives.gov/blog/2016/12/02/whats-next-techhire

Callahan, R. M., Slayton, R., & Uenuma, M. (2016). The HR Professional's Guide to a Cyber-

Secure Workforce. Council on Cybersecurity, p. 1-7.

Carper, Thomas R. Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, S.2521 (2014). Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521

Cobert, B. (2016, January 20). Closing the Cybersecurity Skills Gap - The OPM Director's Blog. Retrieved May 01, 2017, from https://www.opm.gov/blogs/Director/2016/1/20/Closing-the-Cybersecurity-Skills-Gap/

Cobert, B. (2016, July 12). Strengthening the Federal Cybersecurity Workforce - The OPM Director's Blog. Retrieved April 30, 2017, from https://www.opm.gov/blogs/Director/2016/7/12/Strengthening-the-Federal-Cybersecurity-Workforce/

Commission on Enhancing National Cybersecurity. (2016). *Report on Securing and Growing the Digital Economy* (pp. 1–90). Retrieved from https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

Condrey, Stephen E. (2016, December 14). Level of Comparability Payments for January 2018 and Other Matters Pertaining to the Locality Pay Program. Memorandum. Retrieved from https://www.opm.gov/policy-data-oversight/pay-leave/pay-systems/general-schedule/federal-salary-council/recommendation16.pdf

Copeland, C. W. (2008). *The federal workforce: Characteristics and trends* (RL34685) [Electronic version]. Washington, DC: Congressional Research Service. http://digitalcommons.ilr.cornell.edu/key_workplace/551/

Cyber Student Volunteer Initiative. (n.d.). Department of Homeland Security. Retrieved from https://www.dhs.gov/homeland-security-careers/cyber-student-volunteer-initiative

CyberCorps: Scholarship For Service. (n.d.). U.S. Office of Personnel Management. Retrieved from https://www.sfs.opm.gov/StudFAQ.aspx?#num8

Cybersecurity Act of 2015, 754 S § (2015). Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/754

Department of Homeland Security. (2016). Budget in Brief: Fiscal Year 2017. Retrieved April 30, 2017, from https://www.dhs.gov/sites/default/files/publications/FY2017_BIB-MASTER.pdf

Department of Homeland Security. (n.d.). Homeland Security Careers. Retrieved April 30, 2017, from https://www.dhs.gov/homeland-security-careers/dhs-cybersecurity

Deyo, Russell C. (2016). *Strengthening Management Functions* (Integrated Strategy for High Risk Management) (p. i-130). Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20Integrated%20Strategy%20for%20High-Risk%20Management%20-%20August%202016_1.pdf

Duhigg, Charles. (2017, February 22). How Trump Might Become a Workplace Disrupter. *The New York Times*. Retrieved from https://www.nytimes.com/2017/02/22/business/how-trump-might-become-a-workplace-disrupter.html?_r=0

EINSTEIN. (2015, December 14). Department of Homeland Security. Retrieved from https://www.dhs.gov/einstein

England-Joseph, Judy, & Heinzer, Louis. (2014). *Helping Government Deliver: Transforming Mission and Support Services* (pp. 1–28). Partnership for Public Service & Deloitte.

Evans, Brad. (2014, March 18). The Obamacare Website. Ivey Publishing.

Executive Office of the President. (2015, June 12). FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity. Retrieved April 30, 2017, from https://obamawhitehouse.archives.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf

Falk, Justin. (2017). *Comparing the Compensation of Federal and Private-Sector Employees, 2011 to 2015* (No. 52637) (pp. 1–24). Congressional Budget Office. Retrieved from https://www.cbo.gov/system/files/115th-congress-2017-2018/reports/52637-federalprivatepay.pdf

FBI Risk Management: Defining an Ecosystem to Help the Private Sector Manage Risk and Mitigate Threats. (n.d.). General Services Administration. Retrieved from https://presidentialinnovationfellows.gov/projects/fbi-risk-management.html

Federal Employee Pay & Benefits. (2017, April 10). Retrieved April 30, 2017, from http://www.federaljobs.net/benefits.htm

Gallup, Inc. (2016). *How Millennials Want to Work and Live* (pp. 7–11).

Gambler, Rebecca. (2017). *Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* (High-Risk Series No. 17–317) (pp. 1–676). Government Accountability Office. Retrieved from http://www.gao.gov/assets/690/682765.pdf

Goldenkoff, R. (2014). *Federal workforce, human capital management challenges and the path to reform : testimony before the Subcommittee on Federal Workforce, U.S. Postal Service and the Census, Committee on Oversight and Government Reform, House of Representatives.* [Washington, District of Columbia]: United States Government

Accountability Office.

Goldenkoff, R. (2016). *Federal workforce, lessons learned for engaging millennials and other age groups: testimony before the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate.* [Washington, D.C.]: United States Government Accountability Office.

High Risk List. (2017). Government Accountability Office. Retrieved from http://www.gao.gov/highrisk/overview

Larson, Selena. (2017, March 12). Congressman: We need a National Guard for cybersecurity. *CNN*. Retrieved from http://money.cnn.com/2017/03/12/technology/national-guard-tech-cybersecurity-sxsw/

Lewis, C. R. (2009). *Federal workforce trends.* New York: Nova Science.

Mader, D. & Roth, D. T. (2015). *Scaling Implementation of Shared Services.* The White House of President Barack Obama. Retrieved from https://obamawhitehouse.archives.gov/blog/2015/10/22/scaling-implementation-shared-services

Manyika, James, Lund, Susan, Bughin, Jacques, Robinson, Kelsey, Mischke, Jan, & Mahajan, Deepa. (2016). *Independent work: Choice, necessity, and the gig economy* (pp. 1–136). McKinsey Global Institute. Retrieved from http://www.mckinsey.com/global-themes/employment-and-growth/independent-work-choice-necessity-and-the-gig-economy

Manyika, James, Lund, Susan, Bughin, Jacques, Woetzel, Jonathan, Stamenov, Kalin, & Dhingra, Dhruv. (2016). *Digital Globalization: The New Era of Global Flows* (pp. 1–21). McKinsey & Company.

Marinos, N. (2017). *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*. United States Government Accountability Office, pp. 1-16. Retrieved from https://www.gao.gov/assets/690/683923.pdf

Marschollek, Oliver, & Beck, Roman. (2012). Alignment of Divergent Organizational Cultures in IT Public-Private Partnerships. *Business & Information Systems Engineering*, *3*, 153–162.

Meehan, Patrick. Cybersecurity Workforce Assessment Act, Pub. L. No. 113–246, 2952 H.R. (2014). Retrieved from https://www.congress.gov/bill/113th-congress/house-bill/2952

Miller, Jason. (2016, November 28). IRS hires “white-hat” hackers to help protect IT systems. *Federal News Radio*. Retrieved from https://federalnewsradio.com/cybersecurity/2016/11/irs-hires-white-hat-hackers-help-

protect-systems/

Miller, Jason. (2017, February 6). GSA to join DoD in hiring ethical hackers to find cyber vulnerabilities. *Federal News Radio*. Retrieved from https://federalnewsradio.com/reporters-notebook-jason-miller/2017/02/gsa-join-dod-hiring-ethical-hackers-find-cyber-vulnerabilities/

Mulcahy, Diane. (2016). Who Wins in the Gig Economy, and Who Loses. *Harvard Business Review*. Retrieved from https://hbr.org/2016/10/who-wins-in-the-gig-economy-and-who-loses

National Centers of Academic Excellence (CAE). (2017, March 31). Department of Homeland Security. Retrieved from https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae

Naylor, Brian. (2016, December 26). Experts Hope Trump Makes Cybersecurity An Early Priority. *All Things Considered*. National Public Radio. Retrieved from http://www.npr.org/2016/12/26/506998645/experts-hope-trump-makes-cybersecurity-an-early-priority

Office of Inspector General. (2015). *Evaluation of DHS' Information Security Program for Fiscal Year 2015* (No. OIG-16-08). Retrieved from https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-08-Nov15.pdf

Office of Inspector General. (2016). *Federal Information Security Modernization Act: Audit Fiscal Year 2016* (No. 4A-CI-00-16-039). Retrieved from https://www.opm.gov/our-inspector-general/reports/2016/federal-information-security-modernization-act-audit-fiscal-year-2016-4a-ci-00-16-039.pdf

Office of Personnel Management. (2016). *2017 Assessment Preparation Guide* (pp. 1-19). Retrieved from https://sipa.columbia.edu/system/files/PMF%202017%20Assessment%20Preparation%20Guide.pdf

Office of Personnel Management. (2015, June). Actions to Strengthen Cybersecurity and Protect Critical IT Systems. Retrieved April 30, 2017, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/opm-cybersecurity-action-report.pdf

Office of Personnel Management. (2016). *Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals* (pp. 1–25). Retrieved from https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf

Office of Personnel Management. (2016). Cybersecurity Resource Center Cybersecurity Incidents. Retrieved May 01, 2017, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Office of Personnel Management. (2016, June). Common Characteristics of the Government. Retrieved April 29, 2017, from https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/common-characteristics-of-the-government/ccog2015.pdf

Office of Personnel Management. (n.d). Our Mission, Role & History. Retrieved from https://www.opm.gov/about-us/our-mission-role-history/

Office of Personnel Management. (2016, November 20). PMF - Presidential Management Fellows. Retrieved April 30, 2017, from https://www.pmf.gov/the-opportunity/pmf-stem.aspx

Office of Personnel Management. (2016, November). Fiscal Year 2016 Agency Financial Report. Retrieved April 29, 2017, from https://www.opm.gov/about-us/budget-performance/performance/2016-agency-financial-report.pdf

Office of Personnel Management. (2016, September 30). Data, Analysis & Documentation Federal Employment Reports. Retrieved April 29, 2017, from https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/profile-of-federal-civilian-non-postal-employees/

Office of Personnel Management. (2017, February). Congressional Budget Justification - Fiscal Year 2017. Retrieved April 30, 2017, from https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2017.pdf

Office of Personnel Management. (2017, January). Salary Table 2017-GS. Retrieved April 30, 2017, from https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2017/GS.pdf

Office of Personnel Management. (n.d.). Classification & Qualifications General Schedule Qualification Standards. Retrieved April 30, 2017, from https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/0300/gs-2210-information-technology-management-series/

Office of Personnel Management. (n.d.). Federal Employees - Flexible Work Schedules. Retrieved April 30, 2017, from https://www.opm.gov/policy-data-oversight/pay-leave/work-schedules/fact-sheets/alternative-flexible-work-schedules/

Office of Personnel Management. (n.d.). Human Capital Management Hiring Reform. Retrieved April 29, 2017, from https://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/hiring-process-analysis-tool/close-job-opportunity-announcement/

Office of the Press Secretary. (2015, July 09). FACT SHEET: Administration Cybersecurity Efforts 2015. Retrieved April 30, 2017, from https://obamawhitehouse.archives.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015

Partnership for Public Service, & Booz Allen Hamilton. (2015). *Cyber In-security II: Closing the Federal Talent Gap* (pp. 1–31).

Partnership for Public Service. (2017a). Civil Service Reform. Retrieved from https://ourpublicservice.org/research/civil-service-reform.php

Partnership for Public Service. (2017b). Federal Hiring. Retrieved from https://ourpublicservice.org/issues/federal-hiring/index.php

Peterson, Andrea. (2015, October 24). How the government tries to recruit hackers on their own turf. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/10/24/how-the-government-tries-to-recruit-hackers-on-their-own-turf/?utm_term=.70dc283f825f

Powner, David A. (2016). *Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps* (IT Workforce) (pp. 1–86). Government Accountability Office. Retrieved from https://www.gao.gov/assets/690/681309.pdf

Presidential Innovation Fellows. (n.d.). General Services Administration. Retrieved from https://presidentialinnovationfellows.gov/

Price, Austin. (2015). *Building a Shared Services Marketplace: Recommendations from the Shared Services Roundtable* (pp. 1–28). Partnership for Public Service.

Powner, D. A. (2016). *Digital Service Programs: Assessing Results and Coordinating with Chief Information Officers Can Improve Delivery of Federal Projects*. United States Government Accountability Office (pp. 1-39). Retrieved from http://www.gao.gov/assets/680/677794.pdf

Rainey, Hal G., & Chun, Young Han. (2005). Public and Private Management Compared. In *The Oxford Handbook of Public Management* (pp. 72–102). Oxford University Press.

Reinhold, M. (2015, November 23). Cybersecurity Hiring, Pay, and Leave Flexibilities. Retrieved April 29, 2017, from https://www.chcoc.gov/content/cybersecurity-hiring-pay-and-leave-flexibilities

Rossmann, Nick, Beyer, Bill, & Heinzer, Louis. (2015). *Helping Government Deliver II: The Obstacles and Opportunities Surrounding Shared Services* (pp. 1–28). Partnership for Public Service & Deloitte. Retrieved from

https://ourpublicservice.org/issues/government-reform/shared-services.php

Schawbel, Dan. (2016, November 1). 10 Workplace Trends You'll See In 2017. *Forbes*. Retrieved from https://www.forbes.com/sites/danschawbel/2016/11/01/workplace-trends-2017/#37e37f1556bd

Scott, T. (2015, July 31). Strengthening & Enhancing Federal Cybersecurity for the 21st Century. Retrieved April 30, 2017, from https://obamawhitehouse.archives.gov/blog/2015/07/31/strengthening-enhancing-federal-cybersecurity-21st-century

ServiceCorps. (n.d.). Corporate Partners. Retrieved from http://www.servicecorps.org/corporate-partners-overview/

Shared Services. (2016, June 14). General Services Administration. Retrieved from https://www.gsa.gov/portal/category/25608

Siraj, Ambareen, McGrew, Wesley, Pruitt-Mentle, Davina, & Shumba, Rose. (2014). *Panel: Diversity in Cybersecurity Workforce*. Retrieved from http://csrc.nist.gov/nice/2013workshop/presentations/day2/d2_trk1_sirja_diversity_cybersecurity_workforce.pdf

Smith, Megan. (2016, January 30). Computer Science For All [The White House]. Retrieved from https://obamawhitehouse.archives.gov/blog/2016/01/30/computer-science-all

Stier, Max. A More Efficient and Effective Government: Cultivating the Federal Workforce, Pub. L. No. 113–507, § Committee on Homeland Security and Governmental Affairs, 1 (2014). Washington, D.C. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-113shrg89529/pdf/CHRG-113shrg89529.pdf

Su, Ning, Levina, Natalia, & Ross, Jeanne W. (2016). The Long-Tail Strategy for IT Outsourcing. *MIT Sloan Management Review*, *57*(2), 81–89.

TechHire Initiative. (2015). The White House: President Barack Obama. Retrieved from https://obamawhitehouse.archives.gov/node/325231

The Obama White House. (2015). *President Obama Makes the Presidential Innovation Fellows Program Permanent*. Retrieved from https://medium.com/@ObamaWhiteHouse/meet-the-presidential-innovation-fellows-194dec20442b

The President's Budget: Fiscal Year 2016. (2016) (pp. 1–3). Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity.pdf

The White House Office of the Press Secretary. (2016). *FACT SHEET: Cybersecurity National Action Plan*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Thrift Savings Plan. (n.d.). Maximize Your Retirement Savings: The Thrift Savings Plan. Retrieved April 30, 2017, from https://www.tsp.gov/PlanningTools/InvestmentStrategy/retirementsavings/powerOfCompounding.html

Torpey, Elka, & Hogan, Andrew. (2016, May). Working in a gig economy. U.S. Bureau of Labor Statistics. Retrieved from https://www.bls.gov/careeroutlook/2016/article/what-is-the-gig-economy.htm

Triplett, C. (2017, February 12). Investing in Cybersecurity - The OPM Director's Blog. Retrieved April 30, 2017, from https://www.opm.gov/blogs/Director/2016/2/12/Investing-in-Cybersecurity/

U.S. Merit Systems Protection Board. (2004, September). Managing Federal Recruitment: Issues, Insights, and Illustrations. Retrieved April 29, 2017, from https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=253626&version=253913

U.S. Small Business Administration. (2015). ChallengeHER. Retrieved from https://www.sba.gov/about-sba/sba-newsroom/press-releases-media-advisories/challengeher

U.S. Small Business Administration. (n.d.). SBA Learning Center. Retrieved from https://www.sba.gov/tools/sba-learning-center/training/government-contracting-101

Uhler, Andy. (2017, April 12). Trump to call for slashes to the federal workforce. *Marketplace*. Retrieved from https://www.marketplace.org/2017/04/12/economy/federal-freeze-hiring

Wilshusen, Gregory C. Cybersecurity: Actions Needed to Strengthen U.S. Capabilities, § Subcommittee on Research and Technology, Committee on Science, Space, and Technology (2017). Retrieved from https://www.gao.gov/assets/690/682756.pdf

Wilshusen, Gregory C., & Barkakati, Nabajyoti. (2016). *HEALTHCARE.GOV: Actions Needed to Enhance Information Security and Privacy Controls* (No. 16–265) (p. 1). U.S. Government Accountability Office. Retrieved from http://www.gao.gov/products/GAO-16-265

Work, R. O. (2017, February 1). MEMORANDUM: Implementation of Civilian Hiring Workforce Freeze. Retrieved April 24, 2017, from https://www.defense.gov/Portals/1/Documents/pubs/OSD000999-17-RES-Final.pdf