CYBER IN-SECURITY II

Closing the Federal Talent Gap

APRIL 2015

PARTNERSHIP FOR PUBLIC SERVICE

Booz | Allen | Hamilton

The Partnership for Public Service is a nonpartisan, nonprofit organization that works to revitalize the federal government by inspiring a new generation to serve and by transforming the way government works. The Partnership teams up with federal agencies and other stakeholders to make our government more effective and efficient. We pursue this goal by:

- Providing assistance to federal agencies to improve their management and operations, and to strengthen their leadership capacity
- Conducting outreach to college campuses and job seekers to promote public service
- Identifying and celebrating government's successes so they can be replicated across government
- Advocating for needed legislative and regulatory reforms to strengthen the civil service
- Generating research on, and effective responses to, the workforce challenges facing our federal government
- Enhancing public understanding of the valuable work civil servants perform

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for a century. Today, the firm provides services primarily to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

Booz Allen is headquartered in McLean, Virginia, employs approximately 25,000 people, and had revenue of $5.86 billion for the 12 months ended March 31, 2012. To learn more, visit www.boozallen.com. (NYSE: BAH)

INTRODUCTION

Technology has changed our lives. Individuals can email, text and talk to each other, take pictures, get directions, watch television, control their home appliances, read the news, play games and manage their schedules using a device that fits in their pockets. The government uses computers and the Internet for every aspect of its work, from handling crucial information about our national and economic security to managing the air traffic control system, interacting with citizens and processing benefits. The financial system, the electric grid, our nation's commerce and communications systems are dependent on computer networks.

While these innovations have transformed society, the technology has exposed us to new vulnerabilities, and these dangers continue to grow and evolve. According to James Clapper, the director of national intelligence: "Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact."[1]

In 2014 alone, there were tens of thousands of cyber break-ins adversely affecting the private and public sectors, including 67,168 intrusions into federal systems alone, a 1,121 percent increase from 2006.[2] In one instance, intruders from China broke into the U.S. weather system and satellite network, potentially comprising disaster planning, aviation, shipping and other critical uses; while in another case, the top security clearance application files of thousands of federal employees were breached.

At JP Morgan Chase, the nation's largest bank, hackers from overseas gained access to the names, addresses, phone numbers and emails of 76 million customers and seven million small businesses, while the Obama administration blamed North Korea for the crippling computer attack against Sony Pictures Entertainment.

Mike McConnell, formerly director of national intelligence and the National Security Agency (NSA), noted: "There are two kinds of organizations: those that have been penetrated and are aware, and those that have been penetrated and are unaware."

Protecting communication and information networks is the responsibility of public- and private-sector organizations, but as President Obama recently stated, "The cyber world is the wild, wild west and to some degree [the federal government] is asked to be the sheriff."

All sectors rely on sophisticated technology and software to defend their data and networks, but more importantly they depend on highly skilled workers capable of dealing with complex and emerging cyber threats. Without these individuals, even state-of-the-art security controls will be of limited value.

There is a nationwide shortage of highly qualified cybersecurity experts, and the federal government in particular has fallen behind in the race for this talent—individuals who are essential to protecting our nation's critical public and private information technology infrastructure.

The Partnership for Public Service and Booz Allen Hamilton first examined this problem in a 2009 report entitled "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," finding that agencies were having a difficult time recruiting, hiring, retaining and properly training skilled workers in the cybersecurity field. We found that the government did not even know

1 Statements from James R. Clapper, Director of National Intelligence to the Senate Armed Services Committee, Thursday, Feb. 26, 2015.

2 GAO, High-Risk Series: An Update, GAO-15-290, Washington, D.C.: Feb.11, 2015.

the size and competencies of the workforce let alone what would be needed in the future, and it had no plan to address this problem.

During the past five years, the federal government has taken some positive steps, but the same basic problems outlined in our 2009 report have grown more acute as the threat has multiplied. In short, the government still lacks the cyber workforce it needs and still does not have a comprehensive, enterprise-wide strategy to recruit and retain that workforce.

Today, just as in 2009, federal agencies are left to fend for themselves in the hypercompetitive market for top cyber talent. Some agencies—like the NSA and FBI—fare better than others, partly because of their mission and partly because they have more personnel flexibilities than their sister agencies. That agency-centric, "have versus have-not" approach has resulted in a federal cyber workforce that in 2015 is uneven at best, especially when compared with top-tier private sector organizations.

This stovepipe approach to cyber talent has another, even more serious problem. Our interconnected world requires a seamless team of cyber defenders to protect our networks. Those defenders must be able to operate quickly and collaboratively in ways that cut across both private and public organizations.

The cyber talent crisis has persisted long enough. Our nation is at risk as the number and sophistication of cyber-attacks continue to grow, but the government has failed to act with urgency.

WHAT HAS CHANGED SINCE 2009?

In our 2009 report "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," we found a number of shortcomings regarding the federal government's cybersecurity workforce. The following outlines some of what we found in 2009, and the status today.

2009

There was no government-wide strategy to build a vibrant, highly trained and dedicated federal cybersecurity workforce.

The government lacked a clear definition of cybersecurity jobs.

2015

There still isn't one.

The lack of a coordinated strategy to help agencies get the high level talent they need continues to be a major problem. The Department of Defense and the Department of Homeland Security have been able to get legislative authority that will enable them to become more competitive for top cyber talent, but other agencies remain wanting.

Those definitions exist, but they still haven't been fully implemented.

In an attempt to address this problem, the Bush administration established the National Initiative for Cybersecurity Education. First led by the National Institute for Standards and Technology (now led by the Department of Homeland Security), this effort resulted in a Cybersecurity Workforce Framework that defines cyber work and identifies related competencies and KSAs (knowledge, skills and abilities). With seven categories and thirty-two specialty[3] areas, this framework provides a common understanding of cybersecurity work, and the Office of Personnel Management has asked agencies to use it to begin to inventory the employees who are actually engaged in cybersecurity work. However, there are no public plans to undertake a government-wide competency assessment of the cybersecurity workforce based on that framework.

3 The National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework,* http://1.usa.gov/1N8oJI5 (accessed 12 March 2015).

Many of the personnel issues confronting the cybersecurity workforce are endemic in the federal system that makes recruiting and retaining the best and brightest talent in any career field a formidable challenge.

The Partnership and Booz Allen have argued that the best way to deal with this government-wide challenge is to reform the entire civil service system through market-sensitive, performance-based pay that accounts for occupational differences; a new, modern job classification system; expectations and rewards for excellence; more flexibility to hire talented candidates and hold them accountable; and a new enterprise-focused leadership structure that engages its employees, all without comprising the core principles that have always anchored our civil service.

While such a government-wide overhaul may take time, cybersecurity is one area that simply cannot wait. The current federal personnel system is more than 60 years old, created decades before the Internet was a reality. With our national and economic security at stake, the cyber workforce is an ideal place to launch a comprehensive strategy that will address current and future cybersecurity workforce needs.

In the pages that follow, we outline the challenges faced by the federal government in building an enterprise-wide, first-class cybersecurity workforce and offer recommendations for a total workforce solution. Many of these recommendations are actions that the administration can take right now with existing authorities. Other recommendations may require legislation, but are worth the effort to address our vulnerabilities.

The pipeline of potential new cyber talent was inadequate.

The cumbersome hiring process hampered the government's ability to secure top talent.

Some tools have been added to increase the talent pool, but demand still outstrips supply.

This problem continues to plague both public and private sector organizations, due to a continuing nationwide shortage of skilled IT and related professionals. However, in the federal government's case, that shortage has been exacerbated by stringent security clearance requirements and antiquated personnel rules that have made its ability to compete for that limited talent pool even more difficult. The administration has continued efforts to encourage more Americans to develop science, technology, engineering and mathematics (STEM) skills, but this will take time to bear fruit, even as the demand for those skills—for cyber-related work and otherwise—is projected to rise at an ever faster pace.

This problem still exists.

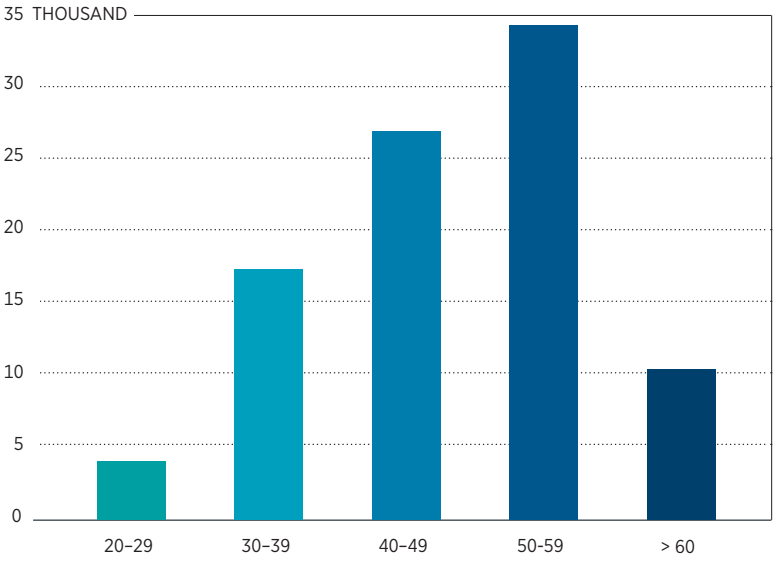
Some agencies have unique flexibilities, but these flexibilities are too limited to help most agencies compete for talent. The length of time that it takes agencies to offer positions to top talent can result in these individuals taking other positions. As a result, critical positions in the federal government can remain vacant for long periods of time.

SPOTLIGHT

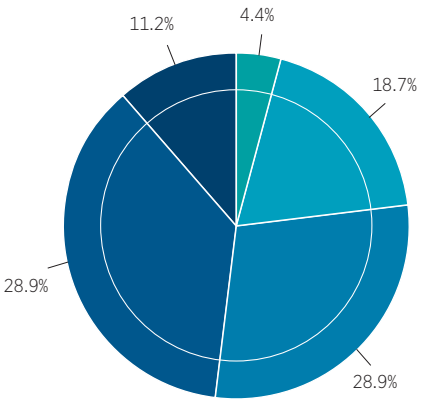
Federal Civilian Cyber Employees

For the purposes of this analysis, "Cyber Occupations" is defined as federal employees within occupational series 0854, 1550 and 2210 as of the end of September 2014. This analysis is based on information from OPM's Fedscope database, which includes records for federal civilian employees at most executive branch agencies. This analysis does not include records for uniformed military personnel or employees of the intelligence community, because these records are not included in this dataset.

AGE GROUPS FOR EMPLOYEES IN CIVILIAN CYBER OCCUPATIONS



PERCENTAGE BREAKDOWN

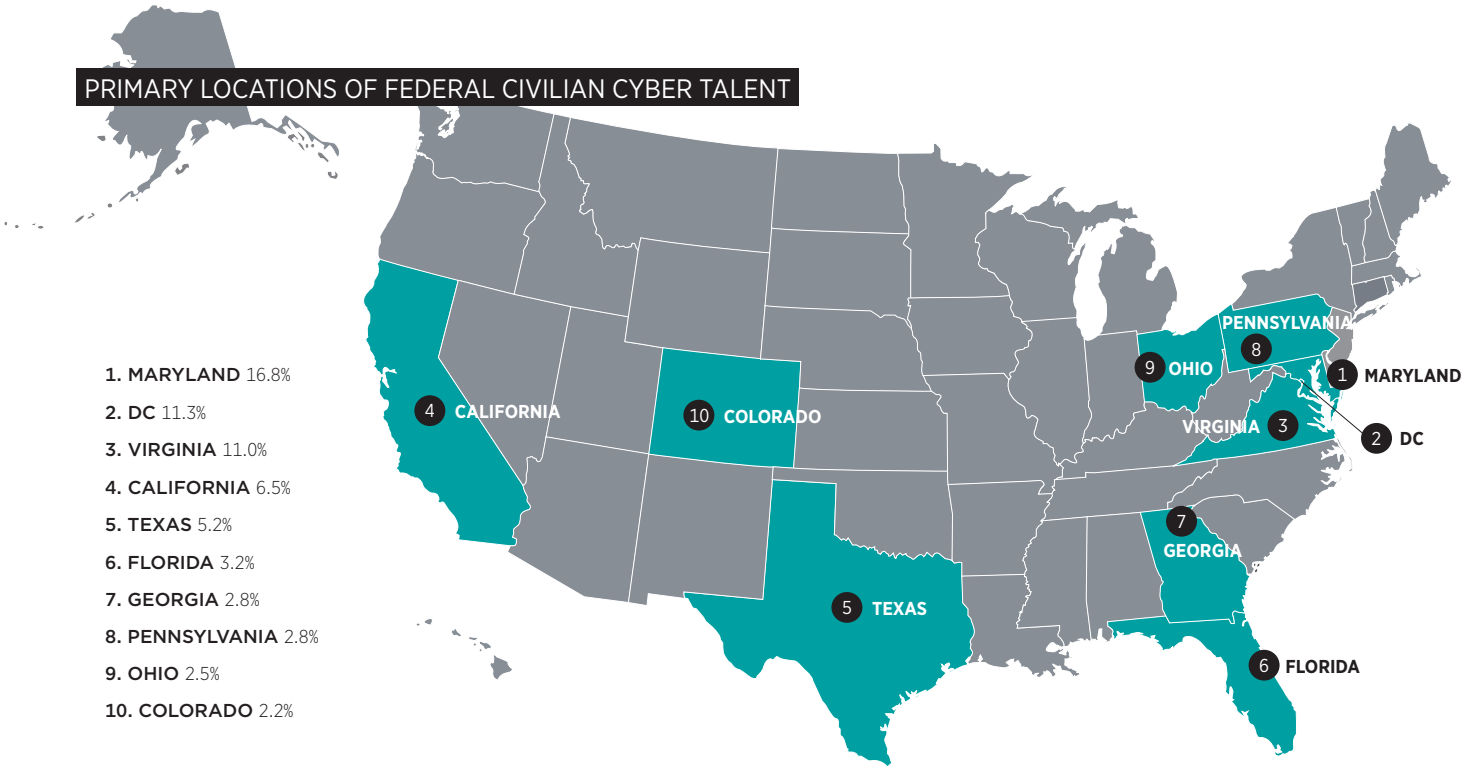


92,863

CIVILIAN CYBER EMPLOYEES GOVERNMENT-WIDE

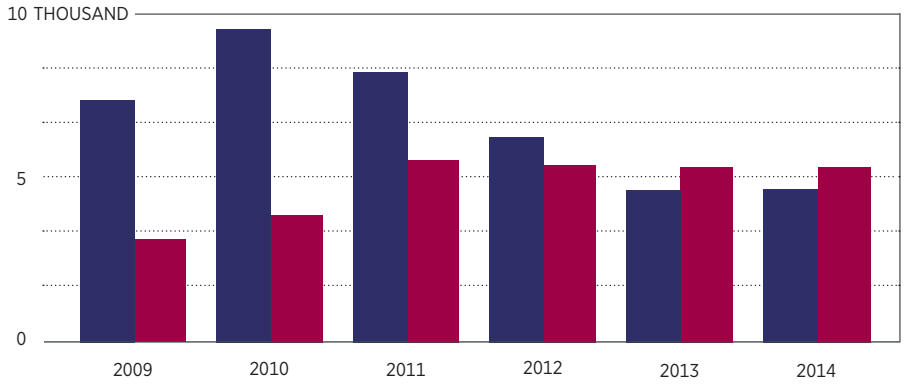
ABOUT 1 OF EVERY 22 GOVERNMENT EMPLOYEES

PRIMARY LOCATIONS OF FEDERAL CIVILIAN CYBER TALENT



SEPARATIONS AND NEW HIRES FOR CIVILIAN CYBER EMPLOYEES

New hires in this chart are defined as the total number of individual hires that are new to federal service. Employee transfers from a previous civil service position are not included as new hires in this analysis. Total separations in these charts are defined as the total number of "separations from federal service." Employee transfers to civil service positions within government are not included as separations in this analysis.



New hires Separations

2014 SEPARATIONS
(FY14)
5,335

2014 NEW HIRES
(FY14)
4,709

SEPARATIONS FOR CIVILIAN CYBER EMPLOYEES BY LENGTH OF SERVICE

FINDING ONE

The Government Lacks a Master Cyber Workforce Strategy to Attract and Retain Top Cyber Talent

In the six years since our last report, the government has taken some important steps to close the cybersecurity workforce gap, but still has not developed a government-wide master cybersecurity workforce strategy. Such a strategy would include an understanding of the size and skills of the current cybersecurity workforce, using the National Cybersecurity Workforce Framework developed by the National Initiative for Cybersecurity Education as a basis for the inventory; a projection of the government's future cybersecurity human capital needs; an assessment of quantitative and qualitative gaps between the current workforce and the workforce that the government needs to address future challenges; and a set of strategies, as well as program and policy goals, designed to close those gaps.

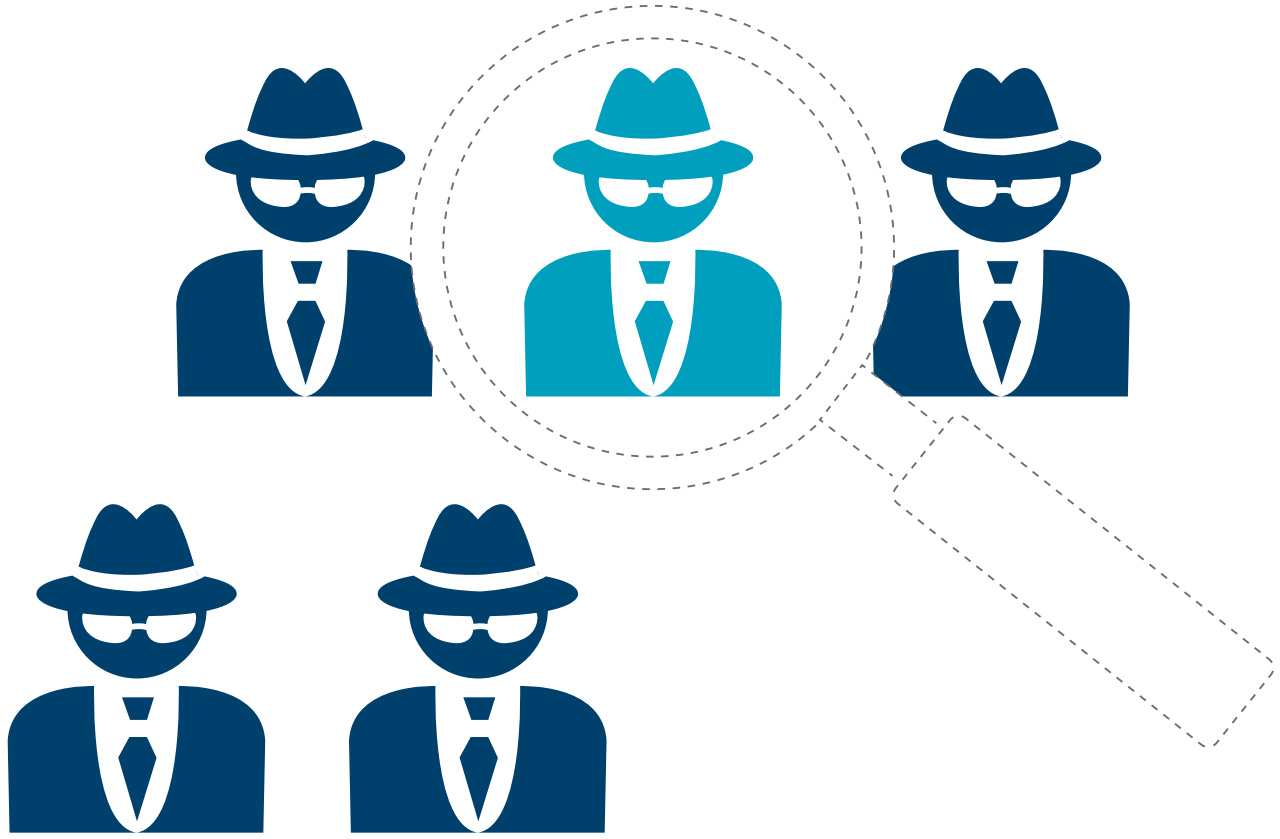
Without this master strategy in place, agencies are operating largely on their own under a haphazard system. Some agencies in the intelligence and defense communities have more success than others, leaving the playing field for cybersecurity talent uneven at best. And since the emerging talent needs remain undefined, supervisors and employees experience frustration in understanding who in the current workforce needs to be retrained to meet future requirements.

The lack of a cohesive, enterprise-wide plan creates other problems. Some college graduates, for example, find it hard to enter the federal cyber workforce because they don't know where the good jobs are located. At the same time, the status quo leaves cybersecurity employees without clear career paths that would enable them to grow and progress through the ranks.

Currently, the government still does not know exactly how many cyber workers it employs, what skills they have, where they work and what skills they need. Understanding this number needs to be the first step in creating a master cyber workforce strategy.

Put more simply, if you do not know how many cyber professionals you have, where they sit and what their specialties are, you can't create a strategy to recruit, develop, deploy and retain them, nor can you effectively predict future needs.

The reason for this dilemma is due in part to the antiquated way jobs are classified. The federal job classification system was established under a 1949 law and



is called the General Schedule (GS). Job classification is important since it is used to determine the qualifications required to fill positions and the pay levels.

Today, many cyber workers under the GS are classified in the "2210 Information Technology Management Series," but because it is insufficient to capture the full range of cyber work, agencies began to hire cyber workers under many additional occupational categories. The 2210 occupational series itself has been split into at least 11 specialties, but only one is clearly focused on cybersecurity. Furthermore, descriptions of the work performed by these many occupations have not been updated in years or in some cases decades.

The National Initiative for Cybersecurity Education, a project initially begun under the Bush administration's Comprehensive National Cybersecurity Initiative, has made some promising strides in seeking to address this issue. Originally led by the National Institute of Standards and Technology, NICE is now the responsibility of the Department of Homeland Security, and the effort includes stakeholders from across government, academia and industry.

One of the most significant contributions of the NICE effort has been its Cybersecurity Workforce Framework, which categorizes, organizes and describes all cybersecurity work in an effort to have a common taxonomy of the jobs that encompass the field, the critical tasks that are performed and the knowledge, skills and abilities that are needed (see chart on page 8).

In its initial release, the authors of the framework noted: "The absence of common language to discuss and understand the cyber work and skill requirements of information technology specialists, computer engineers, computer scientists, law enforcement, and intelligence professionals hinders our nation's ability to baseline capabilities, identify skill gaps, develop cybersecurity talent in the current workforce, and prepare the pipeline for future talent."

Unlike the GS-2210 classification standard, the NICE framework recognizes the wide and widening range of cyber work. In that regard, it takes far more than a small group of cyber experts to defend the government's networks. Network defense requires a concerted and continual effort by everyone who touches a terminal, from

system administrators and architects and designers to help-desk technicians and those with highly specialized cyber skills. Even psychologists, law enforcement and language experts, sociologists and others with social science skill sets are needed to protect the security of our computer networks.

DHS and NIST have made iterative improvements to the structure and scope of the framework during the past several years.

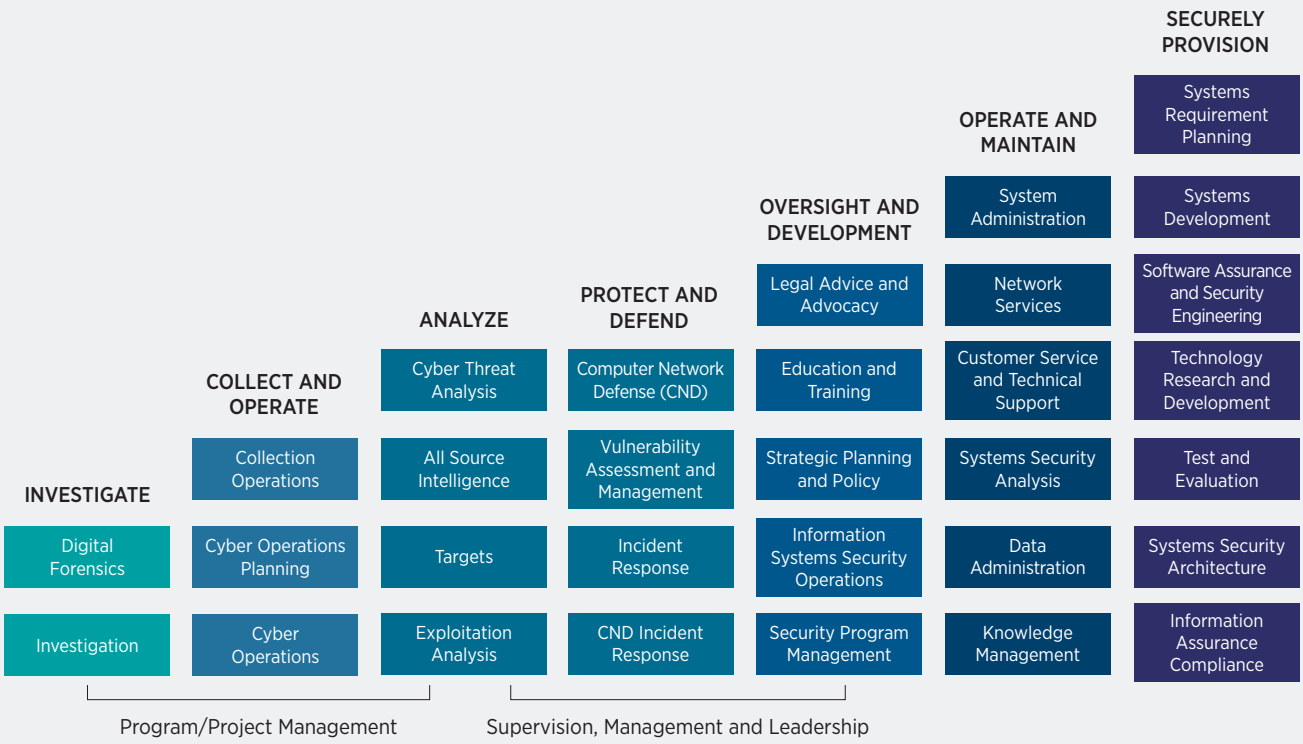
The Office of Personnel Management is currently engaged in a process of having federal agencies identify employees whose duties align at least in part with the seven job categories and 32 specialty areas outlined in the Cybersecurity Workforce Framework. The analysis, however, does not include contractors and other talent segments such as uniformed military members, leaving a gap in understanding the government's total cybersecurity workforce.

The Office of Management and Budget reported in February 2015 that preliminary OPM estimates show that cybersecurity is "a multidisciplinary work function existing as a significant work assignment in positions spanning more than 100 federal occupation series." OPM officials said they plan to continue gathering data and verifying the accuracy of the data throughout 2015, eventually making the information publicly available about all federal jobs that have some cybersecurity responsibilities. They said the goal is for agencies to have a better understanding of the actual cybersecurity duties of their workforce, and to engage in more informed decision-making regarding recruitment, hiring and retention of employees with cybersecurity responsibilities.

To date, however, OPM has not announced plans to undertake a thorough government-wide assessment of the current cybersecurity workforce or to develop a comprehensive cybersecurity human capital strategy to meet current and emerging needs. Additionally, there are no public plans to create a distinct occupational series for cybersecurity professionals.

THE CYBERSECURITY WORKFORCE FRAMEWORK

The National Initiative for Cybersecurity Education developed the Cybersecurity Workforce Framework in 2013 that provides definitions to help classify and categorize cybersecurity workers. Created by the National Institute of Standards and Technology, the Department of Homeland Security and other federal agencies, the framework includes seven categories and 32 distinct specialty areas covering a broad range of jobs. This is the version of the framework that OPM is using to code jobs. Federal organizations define the cyber workforce in different ways, but for the purpose of this report, we are relying on this framework. The categories, including the specialty areas, are:



Source: This framework was developed by the joint efforts of NIST, DHS and OPM through the NICE project.

RECOMMENDATIONS

Develop a comprehensive cybersecurity workforce strategy

In our 2009 report, we recommended that the White House cybersecurity coordinator, a special assistant to the president, develop a government-wide strategy to hire, train and retain the cyber talent that the government needs. This need still exists.

OPM's effort to identify cyber-related work within many different federal job series will be helpful in building that strategy, but it is just the first step of what is needed for agencies to more effectively recruit, hire and retain cybersecurity talent.

The cybersecurity coordinator, or another goal leader with staff and authority, such as an individual within the Office of Science and Technology Policy, should undertake a comprehensive, enterprise-wide examination of the cybersecurity workforce to better understand current capabilities and to develop a strategy to meet future needs. This strategy should contain clear steps to attract and retain cybersecurity talent, and include metrics for evaluating its success and shortfalls.

Create a new occupational job series for cybersecurity employees

Following the development of the cyber workforce strategy, OPM should establish a separate occupational series for the cyber workforce, or even a framework for an occupational group. The Cybersecurity Workforce Framework should serve as the basis for defining the new occupation.

WHAT DO WE MEAN BY A GOAL LEADER?

The GPRA Modernization Act established the position of goal leaders to be in charge of and drive the president's cross-agency priority goals. This is a useful construct for leading other government-wide efforts. Such individuals must have the skills and savvy—as well as the gravitas—to lead multi-agency initiatives or missions and coordinate interagency teams. This leadership needs to be focused and full time, with staff to support the effort. We recommended that goal leaders heading the cross-agency efforts be appointed by the president to ensure their independence and provide authority, and this should be the case for developing the cybersecurity workforce strategic plan as well.

FINDING TWO

Skilled Cyber Workers Are in High Demand and the Federal Government Struggles to Compete

At its root, the cyber talent gap represents a mismatch between supply and demand. With the demand for cybersecurity specialists increasing exponentially, one tactic for the federal government is to concentrate its efforts on the supply side of the equation by increasing the quality and quantity of candidates earning degrees in cybersecurity and related disciplines.

One of the big challenges cited by agency officials was finding employees with experience identifying and analyzing sophisticated cybersecurity threats as well as individuals who can combine technical capabilities with the soft skills of leadership, communication and team building. The demand for such talent is outstripping the supply, and that demand is expected to grow and evolve in the years ahead as cyber threats increase in number and complexity.

A study by the RAND Corporation corroborated this point, noting that there is "general agreement that jobs for cybersecurity professionals are going unfilled within the United States (and the world), particularly within the federal government, notably those working on national and homeland security as well as intelligence." RAND found that the shortage is most acute at the upper end of the workforce for employees with such skills as forensics, code-writing and those capable of thinking like an attacker to figure out a system's vulnerabilities.[4]

RAND and others have acknowledged that the skill gap may correct itself over time "as the supply of cyber professionals in the educational pipeline increases, and the labor market reaches a stable, long-run equilibrium," according to RAND. However, the problem remains acute today and will for the foreseeable future.

The citizenship requirements for federal positions further limits the talent pool. In 2012, there were more than 500,000 graduate students in science and engineering attending doctorate-granting institutions, according to the National Science Foundation. Of these students, about a third were temporary visa holders, which means they are ineligible for classified federal employment.

Many federal organizations readily admit they do not have the personnel needed to address the risks inherent in the flurry of technology advancements, especially the high-end experts. However, a mix of cyber experience in many cases is optimal, and hiring young professionals is usually more affordable than experienced senior experts.

Scholarships can increase the supply and caliber of cybersecurity employees

One way agencies can increase the supply of cyber talent is through the use of undergraduate and graduate scholarships to promising cybersecurity and science, technology, engineering and mathematics (STEM) students.

There are a number of advantages associated with scholarships and recruiting of students while they are still in college. First, scholarships typically require a post-graduation service commitment or reimbursement if the recruit defaults on that commitment. This allows agency officials to know they have talented individuals in the pipeline. Many federal scholarships also allow agencies to use excepted service appointing authority when

4 Martin C. Libicki and David Senty and Julia Pollak, "Hackers Wanted," The RAND Corporation, 2014, http://bit.ly/1pnuZmI (accessed 21 August 2014).

hiring the student,[5] which avoids the hiring delays that are a major source of frustration to cyber candidates and hiring managers alike, an issue we discuss in more detail later in this report. This authority exists for positions where there is a limited applicant pool. When agencies use this authority, the appointments cannot exceed four years, but individuals serving under these appointments can apply for permanent position any time. If agencies invest in scholarships, they are investing in making it easier to hire the entry-level talent that they need.

Once a student receives a scholarship—if the student has a job offer contingent upon graduation—agencies can begin the time-consuming security clearance process. This allows the agency to ensure that the scholarship recipient is able to begin work immediately upon graduation, instead of waiting months for a security clearance.

One successful initiative is the CyberCorps Scholarship for Service program, run through the National Science Foundation, that supports the education, recruitment and retention of undergraduate and graduate students entering the cybersecurity workforce. The scholarships cover the cost of books, tuition and room and board, as well as money for a stipend in return for entering government service when the student's academic work is completed. Students who receive a scholarship for more than one year are required to complete a 10-week summer internship with a federal, state, local or tribal government agency or a federally funded research and development center. Following graduation, students are required to work for a government agency for the same length of time as their scholarship or one year, whichever is longer.

As of April 2014, there were 51 participating academic institutions with more than 460 active scholarships awarded to undergraduate and graduate students. The first SFS graduates entered the federal workforce in 2002 and since then more than 2,000 students have been in the program, with 1,536 completing their degrees. SFS scholarship recipients have been placed in internships and full-time positions in more than 120 federal agencies and departments, with an overall placement rate of 93 percent, according to a June 2014 report by the National Science and Technology Council.[6]

Congress recognized the importance of this scholarship program in the Cybersecurity Enhancement Act of 2014, which directs NSF to continue the program and highlights the existing provision, which gives agencies excepted appointing authority to hire scholarship recipients and noncompetitively convert the students to term, career-conditional or career appointments. The law also requires NSF to evaluate and report periodically to Congress on the success of recruiting individuals for such scholarships and hiring and retaining those individuals in the public-sector workforce.

Agency officials have praised the quality of students from the SFS program, but note that there are not enough students. Additionally, agency officials said that when they identify top talent on campus, they would like to offer them scholarships in exchange for a commitment to work with their agency. Agency officials said they do not

5 5 CFR 213.3102(r).

6 This report was distributed by the Networking and Information Technology Research and Development Program, a subgroup of the National Science and Technology Council. According to the NITRD supplement to the President's FY 2016 budget: "NITRD is the nation's primary source of federally funded work on advanced information technologies in computing, networking, and software. Through its interagency coordination and collaboration activities, the NITRD program seeks to provide the research and development foundations for the advanced information technologies that sustain U.S. technological leadership and meet the needs of the federal government."

have a chance to recruit SFS graduates until these students are ready to graduate. Under the current design, NSF allows the colleges and universities to award the scholarships, not the agencies that will ultimately hire these students.

Other, more limited scholarship programs such as the Information Assurance Scholarship Program, run by the Department of Defense, and the Pat Roberts Intelligence Scholars Program put the scholarship decision in the hands of the agency and, in many cases, the managers who will actually employ the students. However, the IASP has not received funding for new scholarships for the past two years and, as a result, DOD has not been able to offer these scholarships.

Another interesting variation on traditional scholarship programs is the intelligence community's civilian reserve officer training program. Patterned after its military namesake, the program operates just like it. Students in intelligence-related academic disciplines (including cyber) can receive two-year scholarships as well as a stipend for books and room and board in exchange for a two-year service commitment. And as part of their obligation, the students are required to complete an agreed-upon undergraduate or graduate degree program and attend summer sessions with the employing agency. The program was included in the fiscal year 2010 Intelligence Authorization Act and is centrally funded, with agencies applying and competing for blocks of scholarship funding.

Higher academic standards improve the supply of cyber talent

Another tactic to address the supply of cyber talent is enhancing the quality of undergraduate and graduate-level cybersecurity education.

The Department of Homeland Security and the NSA jointly established the Centers for Academic Excellence program, which sets undergraduate curriculum and faculty standards for educational institutions that offer degrees in information assurance, and more recently, cybersecurity. The goal is to "reduce vulnerability in our national information infrastructure by promoting higher education and research in Information Assurance and producing a growing number of professionals with IA expertise in various disciplines."[7]

There are four CAE programs, based in large part on the type of institution that CAE is accrediting: the original information assurance/cyber defense program; the CAE research program, which is geared toward graduate-level studies; the two-year program, which is focused on community colleges; and a CAE operations program.

Colleges and universities can apply to become a CAE school by submitting evidence that the school meets a set of curriculum standards, which are linked to the Cybersecurity Workforce Framework. The Department of Homeland Security and NSA review the applications and certify the institutions that pass the test. While the CAE designation doesn't entitle the school to any federal resources, it has become the gold standard for degree programs in cyber disciplines, and a real differentiator in the competition for STEM undergraduates.

While there is rigor in that process—DHS and NSA take certification very seriously—it is relative. For example, the CAE information assurance/cyber defense program office is jointly staffed by employees from both sponsoring agencies, but doesn't have the resources to conduct a more thorough review that would parallel the far more intensive type of process that leads to full academic accreditation for other disciplines, such as business or engineering. In addition, a thorough accreditation program looks at results—for example, the quality of students matriculated and graduated by the school—and thereby has a measure of true educational outcomes. According to one cyber expert, of the four programs only the newest, the CAE operations program, focuses on the actual outcomes generated by the educational programs.

Internships remain the best way to assess talent, but are still too limited

One of the best means of assessing talent is through the use of student internships, where an employer can witness firsthand an applicant's relationship-building skills, work product and other skills required for the job. If an agency uses the Pathways programs, it is able to noncompetitively convert an intern into a full-time position. However, agencies historically have not made full use of federal internships and only have converted a limited number of interns into full-time service.

And while students are interested in internships, the demand currently exceeds the supply, creating a wasted opportunity on the part of federal agencies.

DHS, for example, created the Secretary's Honors Program Cyber Student Volunteer Initiative, an unpaid program for current college-level cybersecurity students in DHS's field offices and fusion centers. In a news release, the agency's deputy secretary said: "The DHS mission in cybersecurity offers opportunities for the best and brightest of our nation's cybersecurity talent. Through the Department's Cyber Student Volunteer Initiative, students gain firsthand experience in applying their skills directly to our wide-ranging efforts—from helping to defend the nation's cyber networks against attacks

7 National Security Agency, "National Centers of Academic Excellence in Information Assurance / Cyber Defense," http://1.usa.gov/1G1AOQrf (accessed 11 March 2015).

to going after criminals who exploit innocent members of the public." DHS expanded the program from 30 students in 2013 to 70 students in 2014, but officials said they received almost 1,500 applications. Further, DHS officials said they did not have the authority to easily convert high-performing student volunteers into full-time employees. In some cases, these students were quickly hired by federal contractors after their assignments. Even if the department had been able to convert a large portion of the students to employees, such a strategy would only help address a portion of the cyber talent gap.

RECOMMENDATIONS

Expand cybersecurity internships and scholarships

Agencies should make greater use of internship programs in the cybersecurity arena as a way to assess potential talent. If agencies use Pathways internship programs, agency officials can convert top talent to full-time positions following completion of the internship.

Congress should increase the funding to expand successful programs like the NSF's Scholarship for Service and DOD's Information Assurance Scholarship that provide graduate and undergraduate scholarships in the cybersecurity field to help meet the government's need for entry-level talent. Congress also should allow agencies to use Scholarship for Service authority to offer high-performing students scholarships directly in order to build a pipeline of talent that they want.

Create a cybersecurity reserve corps for college students

To encourage more students to consider government service, we propose a civilian Cyber Reserve Training Corps, similar to the military's ROTC and modeled after the intelligence community's program, that would offer third and fourth-year college students tuition assistance and perhaps a stipend if they supplement their regular academic coursework by completing a common curriculum of cyber courses and labs, game-based challenges and intramural and intercollegiate cybersecurity competitions. Members of the corps could begin the process of receiving security clearances when they receive the scholarship, so that immediately upon graduation they would be available to begin their federal jobs. During their college career, corps members would complete at least one cybersecurity-related internship with a government agency. Entry into this corps would come with a multi-year commitment to serve in a cybersecurity position in the government. Under this model, corps members could be hired non-competitively following their graduation by any federal agency as new federal employees.

> **WHAT IS ROTC?**
>
> The Reserve Officers' Training Corps—commonly known as ROTC—is a college-based program for training commissioned officers of the U.S. Armed Forces. Participants receive college scholarships and leadership training during college. After participants graduate from college, they agree to serve in the U.S. military reserves for up to eight years, which may include periods of active duty.

Make academic cybersecurity certification more rigorous

Another way to increase the number of skilled cyber workers is to invest in the CAE program. This would require additional resources for the DHS-NSA program office. It also would require additional investment on the part of educational institutions in order to become CAE-certified.

FINDING THREE

Government Loses Top Candidates to a Slow and Ineffective Hiring Process

It is an all-too-common refrain from federal cybersecurity leaders that because the hiring process is too slow and inflexible, and lacks the ability to adequately assess the talent that is needed, they are unable to hire many top candidates. However, their human resources counterparts often assert that agencies and hiring managers have all the flexibilities required to identify and retain top-tier candidates. They are both right, to a point.

When it comes to identifying and bringing on cybersecurity talent, the hiring processes and flexibilities currently exist that can at times lead to successfully hiring and retaining skilled professionals, but they are too limited, too centralized and too traditional to help most agencies compete for talent.

The overall slowness of the federal hiring process places the government at a competitive disadvantage. The length of time it takes to receive a job offer can result in talented individuals getting frustrated and taking positions in the private sector. A number of federal leaders interviewed said that as a result, critical positions have remained vacant for long periods of time.

The Government Accountability Office reported in 2011 that the average length of the hiring process for cybersecurity positions ranged from about 50 days at the Department of Health and Human Services to almost 130 days at the Treasury Department[8] This was before the individuals went through the similarly lengthy security clearance process. There is little indication that much has changed since that time. In comparison, the hiring cycle in the private sector can often take days or a few weeks for cybersecurity professionals, according to a senior private sector information technology official.

Direct-hire authority is too limited and based on the wrong metric

One way agencies can begin to address the lengthy hiring process is to use existing direct-hire authority, although the practice is only available to select cybersecurity subspecialties.

Designed to grant agencies the authority to expedite "hiring by eliminating competitive rating and ranking, veterans' preference and 'rule of three' procedures,"[9] the Office of Personnel Management grants such authority when "there is either a severe shortage of candidates or a critical hiring need for a position or group of positions."[10] It can also approve direct-hire authority for any or all grade levels within a position, which allows agencies to target a specific caliber of talent.

In 2003, OPM granted agencies direct-hire authority for information technology information security professionals, just one subsection of the broader 2210 IT Series.

8 GAO, Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination, GAO-12-8 Washington, D.C., Nov. 29, 2011–.

9 Office of Personnel Management, "Hiring Authorities: Direct Hire Authority," http://1.usa.gov/1OwWt5p (accessed 12 March 2015).

10 Ibid.

Under current law, OPM can approve direct-hire authority when it determines that there is a critical need for candidates in a particular occupation or occupations, and it can approve that authority for hiring the GS-15 grade level (or equivalent) and below. OPM's rules state that critical need can be declared by an administration to meet a particular mission priority, so potentially it could be sufficient to have a statement by the White House's cybersecurity coordinator, vetted in advance with key lawmakers, to support the extension of the authority to a new cybersecurity job classification series. OPM has discretion to grant direct-hire authority on a year-by-year basis or for a longer period of time.

OPM can also approve direct-hire authority when agencies show a shortage of minimally qualified individuals (i.e., individuals with the competencies or the knowledge, skills and abilities required to perform the job). The Partnership and Booz Allen have previously recommended that OPM amend the criteria that must be met before it grants direct-hire authority. Specifically, the more appropriate standard for direct-hire authority is a shortage of highly qualified individuals because our nation should not have "minimally qualified candidates" meeting our most pressing needs.

Schedule A, another set of special hiring authorities, is also available to hire cybersecurity experts under special circumstances outlined in federal regulations. While this flexibility offers a measure of relief from regular civil service hiring rules, agency personnel offices are cautious and tend to default to existing human capital processes rather than fully leveraging this flexibility.

The National Initiative for Cybersecurity Education Workforce Framework, painstakingly developed and rigorously validated over the last several years, provides empirical evidence that the cyber workforce is far broader than the positions delineated in the 2210 job series. As a result, many critical cybersecurity jobs cannot be filled using the current direct-hire authority. As we discussed earlier, if OPM created a new job series for cybersecurity, it could grant broad direct-hire authority to all the jobs in the series.

One way to ensure that the cyber hiring flexibilities are exercised responsibly would be for the Office of Management and Budget and OPM to make the expanded use of the direct-hire authority contingent on the rigor and quality of the agency's cybersecurity workforce planning, the successful execution of that workforce plan and a post-audit of the agency's use of those expanded flexibilities to ensure that the agency meets all legal and regulatory requirements.

The government's acquisition workforce offers a case study when it comes to expedited hiring. This workforce atrophied as a result of significant downsizing in the late 1990s, a situation that resulted in problems for the Pentagon and other agencies when there was sudden growth in federal acquisition spending. The acquisition workforce only now is recovering, and one of the most effective tools in the rebuilding effort has been specific statutory direct-hire authority for all acquisition occupational categories.

While further investment in the acquisition workforce is needed, the measures taken have helped sustain a more strategic and comprehensive approach to acquisition talent that has included a positive education re-

quirement, acquisition intern programs and an unrivaled professional education system that includes acquisition universities. The statutory direct-hire authority Congress provided for acquisition professionals has allowed that community to more rapidly replenish its ranks.

There are too many self-inflicted process delays

While expanded direct-hire and Schedule A authorities can accelerate cybersecurity hiring, we know from examination of the federal hiring process that many of the delays routinely described by agencies and candidates are self-inflicted, the result of cumbersome and bureaucratic internal processes that the agencies themselves have imposed.

Cyber leaders expressed frustration in this regard, noting that it is sometimes hard to distinguish direct hiring authority processes from the regular and agonizingly slow civil service hiring procedures. They said many agency human resources offices—careful to adhere to well-intentioned merit principles—end up following time-consuming and often rigid procedures.

One OPM official said it is possible that some human resources staff do not fully understand the flexibilities granted to them under the direct-hire authority, prompting unnecessary delays. Nonetheless, the official said problems can arise even with direct-hire authority because of poor recruiting, poorly written job announcements and inadequate assessment procedures.

And even when used properly, the official said, direct hire authority is not necessarily a "silver bullet."

"Everyone thinks they can go make on-the-spot hires. Direct-hire authority is a timesaver, but not as much as people think it's going to be," said the OPM official. "It shaves a couple of weeks off the hiring process, maybe 20 to 24 days. But hiring managers still need to put the job out, post it, pick who's qualified and then deal with the background security process."

Additionally, cyber hiring managers know cyber talent when they see it, and they know the skills they most need to fill their cyber talent gaps. Yet, most of the time, cyber hiring is delegated to agency personnel offices. If cyber hiring managers are engaged in the process of developing job descriptions and are held accountable for recruiting talent—with the human resource offices support—they will be better positioned to recruit the talent they want.

Outdated assessment methods inhibit the identification of qualified cybersecurity talent

One critical but fixable problem centers on the outdated methods used by agencies to screen applicants.

From an agency and hiring manager standpoint, there is a lack effective tools to screen all the applicants to find those who are truly qualified and warrant more extensive examination. The current screening methods frequently do not provide the best insights into a candidates' capabilities.

To be sure, most agencies use staffing software, some of it quite sophisticated, but that software typically has some fundamental shortcomings. First, candidate resumes are usually filtered against a set of key words or phrases that purport to represent the various competencies that are required by the job—that is, their basic qualifications. The problem is that those key words and phrases cannot tell a hiring manager much about how proficient a particular candidate may be with respect to the competencies they represent. And that leads to the second major shortcoming. Most staffing software uses length of experience as a surrogate for proficiency—in other words, the more experienced a candidate is, the more proficient he or she is presumed to be. We know that's simply not the case, especially in cybersecurity, where time on a job may not be the best indicator of ability.

One senior federal official said that creating strict requirements for cybersecurity positions restricts the diversity of people who are hired. "I've seen so many job descriptions with strict certification requirements that exclude highly qualified people," he said. In another instance, senior Department of Defense officials complained that many qualified cybersecurity candidates leave the Armed Forces, but then are not considered qualified for equivalent positions in the federal civil service due to strict certification requirements.

Several federal cybersecurity officials said they know that certification requirements are not always the best way to assess cybersecurity talent, but that they struggle to implement an alternative process that meets the merit requirements for federal hiring. Several government chief information officers said a college degree demonstrates an aptitude for critical thought, and in the absence of an alternative screening process, it remains a reasonable proxy.

Many private-sector cyber experts we interviewed during focus groups said they began their forays into cybersecurity by tinkering, coding and in some cases even hacking as a hobby. These experiences are not usually reflected in formal education or resumes, so government often overlooks promising candidates with nontraditional backgrounds or experiences.

Cyber competitions hold promise, but are not validated and are rarely used to source and recruit top talent

One option that holds promise, but is used sparingly to recruit and assess candidates, involves cybersecurity competitions. The Department of Homeland Security hosts the National Collegiate Cybersecurity Defense Competition. But even though hundreds of students participated in the competition in 2014, DHS did

not recruit these individuals. During competitions, participants often work together to secure and defend networks or identify vulnerabilities in network defenses. Teams or individuals receive points for each success, and the team with the most points wins. For job seekers, these competitions offer a safe space to practice hacking and defense without crossing into potentially illegal activity. For organizations, the competitions offer a way to assess the practical skills and capabilities of candidates. While these games provide real-life cyber challenges, they are frequently held as team activities, which limits the abilities of the hiring manager to assess the skills of individuals. Additionally, OPM has not yet validated these competitions in order to identify the specific skills that the competitions can assess in potential talent. If validated, these challenges can be a unique way to assess top talent.

According to the National Institute of Cybersecurity Careers and Studies, competitions "foster talent in potential cybersecurity professionals that might otherwise be unidentifiable through traditional academic means."[11]

Richard Danzig, who serves on the President's Intelligence Advisory Board, proposed creating a competition as a screening tool where potential applicants could attempt to hack into various systems. Danzig noted that this would be challenging to implement for the federal government as a whole, but could be used for an elite group that could be deployed to address top cybersecurity issues.

Use of these competitions as an assessment tool is starting to draw some attention.

For example, the Defense Department's Cyberspace Workforce Strategy states: "The department seeks to attract highly skilled individuals who might otherwise be uninterested in regular government service. This may include world-class experts identified from competitions and games, as well as security conferences."

The Homeland Security Advisory Council's CyberSkills Task Force report of 2012[12] also proposed that DHS create a certification program for every mission-critical cybersecurity job using "simulation-based proficiency evaluation combined with written examinations to verify competency."

Additionally, the council recommended that once hired, employees undergo regular "scenario-based training and evaluation" to ensure they have the skills needed to perform their jobs. In response to this proposal, DHS has drafted testing materials for assessing mission-critical task proficiency in cyber skills and created proposals for possible future use of a hands-on, scenario-based testing, but has not disclosed plans to use such assessments.

In another example, the US Cyber Challenge, run by the not-for-profit Council on Cybersecurity, was launched in 2010 with the mission to significantly reduce the shortage in today's cybersecurity workforce by "serving as the premier program to identify, attract, recruit and place the next generation of cybersecurity professionals."

The Cyber Challenge hosts online competitions and camps with elite training and hands-on exercises for high school, college and post-graduate students to help them develop their skills, gain access to advanced training and achieve recognition with scholarships, internships and jobs. The goal of the Cyber Challenge is to "find 10,000 of America's best and brightest to fill the ranks of cybersecurity professionals where their skills can be of greatest value to the nation." In 2013, the Cyber Challenge had more than 1,200 applicants, 350 of whom were accepted to one of four training camps where they interacted with industry and government expert. The Cyber Challenge recently announced a partnership with monster.com to develop a central repository for resumes and profiles of cyber talent to increase the ease with which private- and public-sector employers can hire Cyber Challenge participants.

The drawn-out security clearance process is an impediment to hiring cybersecurity professionals

Even when agencies are able to use direct-hire authority to make quick job offers, the candidates still must obtain security clearances, resulting in delays. In some cases, recruits opt to seek employment opportunities with private industry rather than wait for the long process to be completed.

According to a 2011 Government Accountability Office study, some agencies "reported that it can take about a year for a new employee to start working because of both the lengthy hiring process and the time required to obtain a security clearance."[13] A RAND study found that "the long recruitment, vetting, background checks and security clearance can add months to the recruitment cycle."[14]

Federal chief information officers said this timeline is not shortened when they hire talent from other agencies because many security clearances are not transferable between agencies.

11 National Initiative for Cybersecurity Careers and Studies, "Cyber Competitions," Department of Homeland Security, http://1.usa.gov/1y1WF25 (accessed 12 March 2015).

12 Homeland Security Advisory Council, CyberSkills Task Force Report, Department of Homeland Security, Fall 2012, http://1.usa.gov/1BKU2lG (accessed 12 March 2015).

13 U.S. Government Accountability Office, Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination, 2011, http://1.usa.gov/19i0Tw5 (accessed 12 March 2015).

14 Martin C. Libicki and David Senty and Julia Pollak, "Hackers Wanted," The RAND Corporation, 2014, http://bit.ly/1CVvTQz (accessed 12 March 2015).

Although Section 3001(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 requires that equivalent security background investigations completed by an authorized agency be accepted by other agencies, subject to some exceptions, a 2014 report by the Office of the Director of National Intelligence said implementation has been inconsistent across the government.

Due to this lapse, the Intelligence Authorization Act of 2013 included a provision requiring the director of national intelligence to develop a strategy and a schedule to implement the security clearance reciprocity provision of the 2004 law. That policy is scheduled to be issued sometime in fiscal year 2015.

As part of the administration's Insider Threat and Security Clearance cross-agency priority goal, federal officials also are working to ensure that the security clearance process has the necessary rigor, as well as consistent standards across the government. It also calls for a shift to a continuous evaluation model where employees with clearances are subjected to automatic credit checks and review of their social media, personnel records and other relevant information. The purpose of this approach is to enable agencies to spot trends, determine if there are risk factors warranting further inquiry and expedite security clearance re-certifications.

RECOMMENDATIONS

Expand direct-hire authority

The talent pool is already thin, and it is critical that OPM make it is as easy as possible for agency officials to hire qualified individuals that they have identified. To this end, the administration needs to declare that there is a "critical need for cyber talent." Following this declaration, OPM should expand direct-hire authority to cover all the jobs described in the Cybersecurity Workforce Framework, where cyber work is a considerable percentage of the individual's time. As discussed above, if OPM creates one job series for the positions covered by the Cybersecurity Workforce Framework, it could then grant direct-hire authority to the full series.

Put all cyber positions in the excepted service

OPM also should place all cyber work in the excepted service. The Border Patrol Agency Pay Reform Act of 2014 recently authorized DHS to transition select cyber positions to the excepted service. This move will make it easier for DHS to hire the talent it needs, but this is a flexibility that should be granted to all agencies. OPM has the administrative authority to place jobs in the excepted service when it determines that it is administratively difficult to evaluate candidates by traditional means.

Validate cybersecurity competitions and scenario-based testing to identify and assess talent

The Cybersecurity Enhancement Act of 2014 directs the Department of Commerce, DHS, the National Science Foundation and OPM to "support competitions and challenges" that will help "identify, develop and recruit talented individuals to perform duties relating to the security of information technology in federal, state, local and tribal government agencies." It also directs that these competitions and challenges be used to identify talented individuals relating to such cyber skills as ethical hacking, penetration testing, vulnerability assessment, continuity of system operations, security in design, cyber forensics and offensive and defensive operations.

Working with the federal CIO Council, competition sponsors and other game developers, OPM should use this congressional authority as a basis to immediately begin designing, developing and validating a prototype game-based assessment battery that is linked directly to the Cybersecurity Workforce Framework, and that can effectively and efficiently evaluate candidates' proficiency for cybersecurity jobs.

Allow agencies to share best qualified candidate lists

Employment flexibilities should be expanded by Congress to permit agencies to share their best qualified candidate lists for those cybersecurity candidates qualified under the same hiring authorities. This will speed up the process by freeing hiring managers from a lengthy review needed to identify talented cybersecurity professionals by providing them with candidates who have already been screened and vetted by an agency, but not chosen for the available opening. Creating cross-agency lists will reduce the number of times a qualified applicant has to apply for and undergo assessment for similar jobs, and it will save agencies time and money in their search for cybersecurity employees. This would be particularly feasible if OPM validates a common skills-based assessment, as described above.

In "Building the Enterprise: A New Civil Service Framework," the Partnership and Booz Allen Hamilton previously recommended that the federal government create a national best-qualified applicant pool for major occupations or specialties. The cyber workforce would be an ideal place to begin building this asset.

Reform the security clearance process

The administration has been reassessing government security clearance processes, including the standards to be used, the nature of the investigations and the methods to be employed for recertification. It also has been examining the length of the inquiries, the reciprocity that exists between agencies for accepting clearance credentials and the number of people who need security clearances.

These efforts should be sustained and thoughtfully implemented, ensuring that the investigations are rigorous while being done in a timely manner to ensure the government can hire the cybersecurity talent it needs.

We also encourage agencies to begin the lengthy security clearance process as early as possible. As discussed above, agency officials can begin the process once a student receives a scholarship or begins an internship, if the student has a job offer contingent upon graduation.

Develop recruitment expectations of managers

Agency leaders should clearly communicate to program managers that they are expected to identify and recruit their cyber teams. Agencies can hold program managers accountable for this expectation through their performance plans. Agencies' human resource offices should be made available to support these managers.

COMPETITIVE VS. EXCEPTED SERVICE

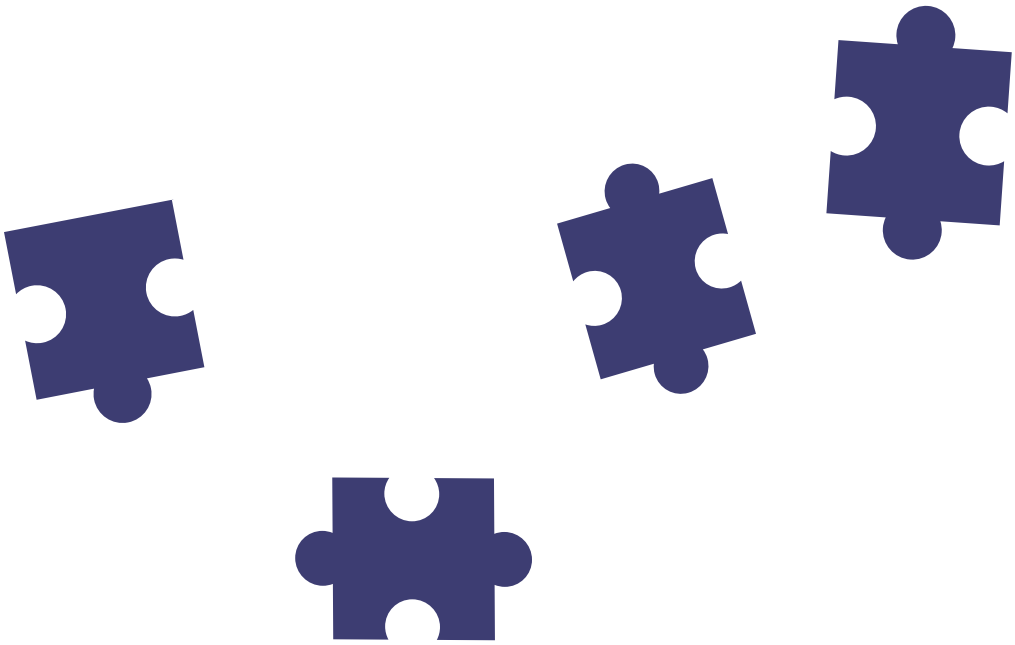
Federal jobs are typically in either the excepted service or competitive service. Jobs in the excepted service are exempt from some of the procedural requirements in law and regulation that apply to the competitive service. The chart below highlights some of the key differences.

COMPETITIVE SERVICE	EXCEPTED SERVICE
Recruitment: All vacant competitive service positions must be posted and advertised on USAJOBS, and all eligible/qualified candidates must be considered. Note that in some cases, applications can be limited to candidates who have already earned "competitive" status.	**Recruitment:** No requirement to post and advertise vacant positions on USAJOBS or elsewhere; applicant search (the area of consideration) may also be targeted to a geographical area or other specifications.
Applicant Assessment: Applicants for competitive service positions must be examined against the qualifications requirements of the job; in most cases, the examination consists of an assessment of the applicant's qualifications against the requirements of the position. By law, OPM establishes the qualification requirements for competitive service positions.	**Applicant Assessment:** Applicants may be examined by alternative means, including written examinations, skills tests, personality tests and psychological evaluation. These alternative assessment methods must still meet federal validation requirements.
Appointment: Requires application of veterans preference, using either the rule of three (that is, appointment is restricted to the top three candidates, after application of veterans preference) or category rating (in which highly qualified veterans must be hired). Veterans can only be passed over in the most limited of circumstances. Under certain limited circumstances, OPM can grant direct-hire authority, which allows hiring without regard to veterans preference, or "excepted" hiring authority (for example, Schedule A).	**Appointment:** Because (by definition) it is not feasible or practical to use standard competitive civil service procedures, highly qualified applicants can be appointed quickly and from a variety of sources, and while veterans preference must still be applied, it is not formulaic. Specifically, veterans must be considered before other candidates, but with no requirement to select them if they are not the most qualified.

In addition to the differences outlined in the table above between the competitive and excepted service, some organizations or jobs in the excepted service also have considerable difference in regard to pay, classification and promotion.

FINDING FOUR

Agency Cyber Training and Development Is Uneven



Even with broad, delegated scholarship authority to prepare cyber-skilled graduates, almost all new federal cybersecurity recruits will need additional training before they are ready for the front lines of network defense—everything from information security policies and incident reporting protocols to analytic tradecraft and tactics, techniques and procedures.

Colleges and universities, and the Center for Academic Excellence schools certified by the Department of Homeland Security and the National Security Agency, do not, as a general proposition, seem to be producing a finished graduate who can walk out of the classroom and right into a seat in a network threat operations center.

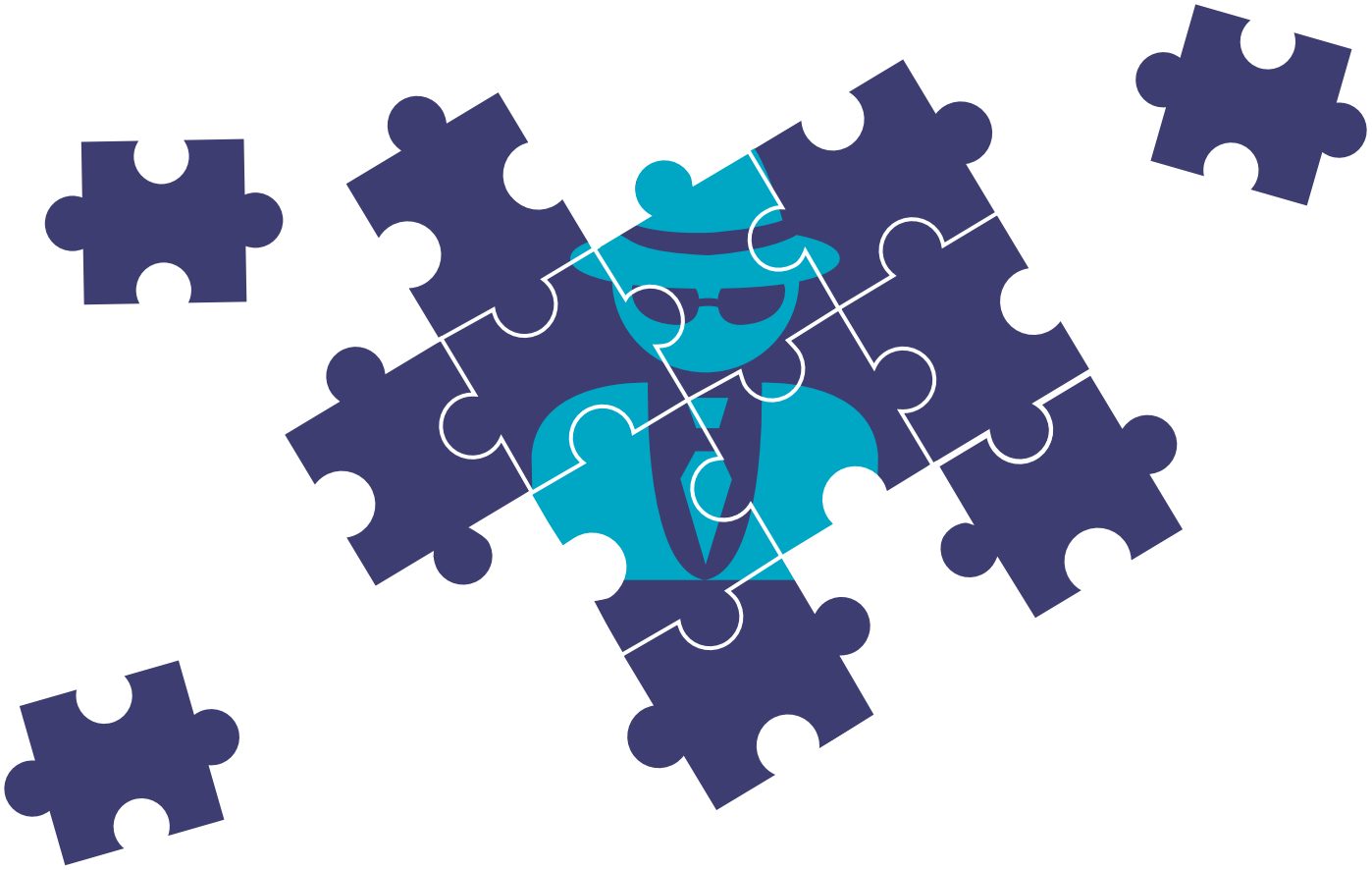
As a result, officials we spoke with at virtually every agency reported that they invested in entry-level training for new cybersecurity specialists regardless of a recruit's pre-entry preparation, and almost every agency did so on its own.

Much of that training has not been agency-specific, but rather geared toward any one of the standard cybersecurity certifications or the various government-wide policies, regulations and reporting protocols that are common to all federal agencies.

At the same time, agencies have faced budget constraints, often making it more difficult to free up funding to give new recruits all the help they need and to keep the skills of more experienced employees up-to-date.

While there are a variety of options available to agencies, the current approach has created a cybersecurity training regimen that is ad hoc and uneven at best, with every agency and IT staff on its own to find suitable training. As a result, there is no unified program across government to instill a set of professional values and behavior, and no common thread to create a shared mission and sense of community across government.

One available option used by some agencies is the Federal Virtual Training Environment, an initiative created by DHS, the Department of Defense and the Department of State. This online training center provides federal cybersecurity and IT professionals with hands-on labs and training courses, and is free to users and their organizations. According to DHS, the Federal Vir-



tual Training Environment delivered 22,761 completed courses in fiscal year 2014.

DHS and the State Department also have developed an initiative known as the Federal Cybersecurity Training Events program, which delivers training, labs and competitions for federal cybersecurity and IT professionals. One- to three-day classes on a variety of cybersecurity topics provide training, hands-on experiences, knowledge of best practices and network opportunities at no cost to participants.

Years ago, the federal law enforcement community confronted a similar problem regarding ad hoc training programs. The federal government has more than two dozen different types of law enforcement officers in the GS-1811 occupational series, including employees who work for the U.S. Park Police, the Secret Service, Customs and Border Protection, Drug Enforcement Administration and many others. Some of these law enforcement officers are in uniform and some are not, but all of them have the power to arrest and even use deadly force.

These are awesome responsibilities, and to ensure that all of them know all they need to know as federal officers, the agencies involved banded together to create the Federal Law Enforcement Training Centers. Operated by DHS, FLETC is supported by tuition and fees paid by participating agencies for all of the recruits they send, as well as agency-provided instructors who teach both common and agency-specific courses on everything from investigatory techniques to marksmanship and combat driving.

Perhaps more importantly, FLETC instills a sense of common mission and community—in effect, a law enforcement philosophy, complete with values and rules of professional behavior among these newest members of the federal law enforcement community regardless of their agency affiliation.

In another model, the Defense Acquisition University provides targeted training for DOD civilian and military acquisition professionals throughout all career stages. It also provides continuous learning and knowledge sharing to help ensure the acquisition workforce is able to fulfill evolving training and certification requirements.

Similarly, the Defense Cyber Crimes Center provides intensive basic and intermediate computer forensics training for all DOD components, as well as a number of agencies outside the department, and the military also delivers a number of joint courses for all uniformed services.

These examples prove the concept of combining agencies in a unified training program is viable.

Another training option, according to some experts we interviewed, has been the use of job rotation programs to give employees new challenges and opportunities to learn how components within their own departments or other agencies handle cybersecurity issues.

The Office of Personnel Management is currently exploring a worker exchange program known as GovConnect, an online platform where agencies can advertise rotational opportunities and employees can find challenging assignments that match their skills in a variety of fields, including cybersecurity. Some agencies, such as the State Department, have already implemented these types of programs.

OPM Director Katherine Archuleta told a Senate appropriations subcommittee on May 7, 2014, that GovConnect would "seek to create a more mobile and agile workforce." As this project advances, she said agencies could utilize GovConnect to secure expertise they need on selected projects and provide their cybersecurity staff with new opportunities.

RECOMMENDATIONS

Create a cybersecurity training academy focused on both technical and leadership skills

The federal government's cybersecurity workforce deserves its own version of FLETC. A common, enterprise approach to cyber training would help equip the cyber workforce with the knowledge, skills and ability to do their jobs. An academy will help ensure that the government's cybersecurity professionals meet the most rigorous technical standards, but perhaps even more importantly, it could be leveraged to instill a common ethos among members of that corps. It also would allow cyber talent to build relationships with each other that could enhance protection of our networks. An academy would also provide significant economies of scale and substantial savings since agencies would no longer have to develop and deliver or buy their own standalone cybersecurity training, and instead could pool funds, course work and instructors to support its operation.

WHERE COULD WE HOUSE THE TRAINING ACADEMY?

Recently, the General Services Administration received a $35 million appropriation—as part of the Consolidated and Further Continuing Appropriation Act of 2015—from Congress to design a "Civilian Cyber Campus" that would co-locate incident response teams from multiple civilian agencies, including the DHS and the Department of Justice. It is also intended to develop a working environment to support the recruitment, development and retention of the best-in-class cyber professionals. This campus could be an ideal site to create and house a cyber-training facility that could serve federal agencies.

Create a cyber reserve for experienced talent

Upon graduation from the cybersecurity training academy, top candidates would be considered for the Cybersecurity Reserve Corps, an entity that provides cyber experts during emergencies and at other times when technical help is needed.

The DOD has already experimented with reserve units that specialize in the department's cybersecurity mission—people who do cybersecurity when they are not in uniform. Like any military unit, reservists initially complete basic training, where among other things they learn the values of military service, and during their terms of service the DOD invests heavily in their training, from weekend drills to the same formal technical schools as active-duty service members. When there is a conflict or disaster, reservists can be mobilized quickly; when there isn't they return to civilian life, but they are still bound together just like a network.

We envision a civilian Cybersecurity Reserve Corps that would operate in a similar way. In September 2012, the Homeland Security Advisory Council Task Force on CyberSkills recommended that DHS establish a pilot "CyberReserve program that ensures DHS cyber alumni and other talented cybersecurity experts outside of government are known and available to DHS in times of need."

The Cybersecurity Reserve Corps as we envision it could include graduates of the training academy who agree to assist agencies with specific projects over time. Since we know that many of government's top talent leave federal service for the private sector, we need to create opportunities to re-engage them as needed. This will allow the government to expand the size of its network of experts that can be relied upon to help on special projects and emergencies, and supplement the work of the United States Computer Emergency Readiness Team (US-CERT).

Members of the Cybersecurity Reserve Corps would take part in annual continuing education programs, receive compensation for their participation and be subject to recall by DHS if there is a declared national cybersecurity incident. In some cases, that may mean a cyber-reservist would report for duty to an affected government agency. Others could be recalled "in place" if their company or industry has experienced an attack.

In suggesting creation of a reserve corps, we envision an organization that captures the intellectual rigor and standards of conduct of the medical and legal professions; and the ethos of the Public Health Service and the military reserves, as well as their agility, continuous learning and ability to provide assistance in times of need.

Further, as the size of the reserve grows, the network of skilled cyber workers—in all sectors—will grow. Borrowing from the emergency management field, establishing opportunities for individuals to train together and work together will improve their ability to work together and leverage each other's areas of expertise when needed.

WHAT IS US-CERT?

Part of DHS, US-CERT responds to select incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities.

FINDING FIVE

Government Compensation Isn't Competitive, Especially for Experienced Talent

After several years of pay freezes, exacerbated by increased retirement and health benefit contributions, the federal government is simply falling behind when it comes to cyber compensation, particularly among elite talent. Some of this difference can be offset by the compelling nature of the federal government's cybersecurity mission and the opportunity for individuals to gain valuable experience. But as the compensation gap continues to widen, especially for the most talented professionals, the federal government will continue to fall further behind.

On the other hand, agency officials without those special authorities told us that they have challenges competing for entry level talent, because they are not only competing with the private sector, they are also competing with other government agencies such as the Defense Department and the intelligence community. These officials said they are often left "scraping the bottom of the barrel," because they have very little flexibility. They often cannot match entry-level pay scales of the private sector or other federal agencies, cannot show pay progression in technical fields because of the way jobs are defined, and are impeded by pay scales that make it impossible to compete for the high-end talent.

Alan Paller of the SANS Institute, an information security research and educational institution, said he sees the problem as a "crisis of quality, not quantity."[15] He said what is most needed are people who can excel at both technical as well as critical thinking and communication skills.

Several agency officials said that their agencies have been able to attract entry-level talent, noting that the opportunity to learn from the federal government and gain the experience serves as a reasonable recruitment tool. Additionally, as noted in the figure, for entry-level talent, the compensation gap is not as large compared to more seasoned experts.

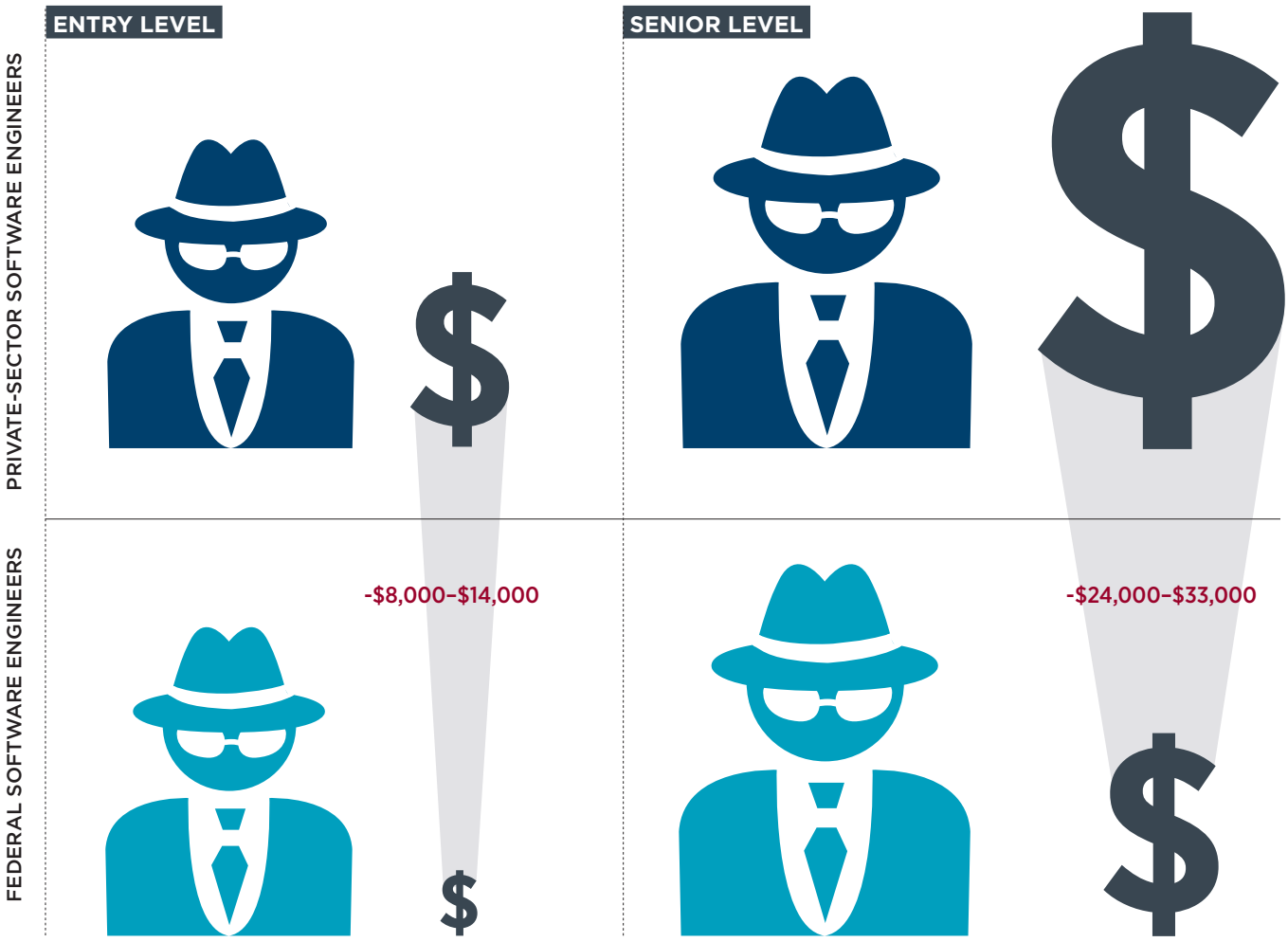
Regardless of their ability to hire the entry-level talent, many agency officials said that once these individuals gain experience in the federal government, they are very desirable to private companies. At this point, they can command much higher salaries outside of government, and after five or six years, many choose to leave.

The Corporate Executive Board analyzed compensation data from hundreds of private-sector security professionals. In this study, the median total compensation of individuals across occupations ranged from $74,000 to $122,000, but in many instances, particularly for those with experience and expertise, the salaries are far above the median. The top earners in the Corporate Executive Board's study made about $225,000 annually. By comparison, without special authorities, federal salaries top out around $130,000, before accounting for locality pay. As noted in the figure, the gap between public- and private-sector salaries becomes magnified in the senior ranks.

To illustrate this point, we selected one position and location—software engineers in Washington D.C.—and compared salary data between the public- and private-sectors. For software engineers, the federal government has special salary rates for entry-level talent, but this does not close the salary gap.

There are some tools currently available to fed-

15 "'There's No Pipeline' of Deep-Knowledge Pros," Careers Info Security, March 18, 2013, http://bit.ly/1Ge6kcX (accessed 3 March 2015).



Notes: The federal government has special salary rates for entry-level software engineers in the Washington Capital Area, which is GS-9 and below. While the actual difference between senior level software engineers is greater than entry-level talent, the actual difference as a percentage of total salary is similar.

eral agencies. The Office of Personnel Management can authorize special salary rates and retention bonuses.[16] These special rates and bonuses can be used by any agency to "address existing or likely significant handicaps in recruiting and retaining well-qualified employees...caused by significantly higher non-federal pay rates than those payable by the federal government within the area, location, or occupational group involved," among other factors. However, special salary rates are a blunt tool, meaning that once approved, everybody within the area, location or occupational group gets a salary increase. This can make use of special salary rates cost-prohibitive for agencies. As a result, OPM may allow any agency to veto a special salary rate.

Congress addressed this pay gap issue for the government's financial agencies under the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA). This law has helped the financial regulatory agencies recruit and retain personnel with critical skills by offering higher pay than the rest of the federal government to better compete with the private sector. There has been no similar effort with regard to the government-wide cybersecurity workforce. A more complete solution would be wholescale civil service reform so that all occupations are market sensitive.

Government additionally competes with its own contractors—both private-sector companies and federally funded research and development centers—which can offer far more generous compensation packages. Contractors are not limited to the General Schedule when it comes to salaries. They can simply hire away the best cybersecurity talent and rent it back to the government at a higher hourly rate. They also can offer performance-based pay and progression, as well as career paths that

16 Retention bonuses cannot exceed 25 percent of an employee's rate of basic pay, if authorized for a specific employee, or 10 percent if offered for a group or category of employees. But the retention bonuses can be increased to 50 percent in certain circumstances with approval from OPM.

can span both government and private-sector work, so it's understandable that the federal government is losing highly sought talent to its own contractors.

Furthermore, as RAND and others have noted, the way that many cyber jobs are currently defined makes it difficult to ensure that individuals will be promoted based on their technical skills without requiring that they take on more supervisory responsibilities.

The Partnership and Booz Allen have reported that this is a challenge for many STEM positions. Specifically, we have said that agencies and STEM talent both benefit when STEM practitioners have the choice of moving into either managerial positions or becoming subject-matter experts in their field. Creating dual tracks for STEM talent is a standard practice in many private-sector companies and provides flexibility for top talent.

One chief information security officer at a large federal agency said that the lack of a career path for cybersecurity employees is a serious detriment for the government. "Right now, the only way to move up is to leave your job, and we need to fix that," he said

Other interviewees pointed out that the current General Schedule system offers a potential for advancement for some employees who want to move into the managerial ranks, but stymies those who want a career path and higher earning capacity while remaining in the technical arena.

RECOMMENDATIONS

Conduct a pay study

The first step in closing the gap should be to examine in depth the nature and extent of the differences between federal and private-sector IT and cybersecurity salaries for various specialty areas and localities.

While this should eventually be done for all occupations across government, OPM and the federal CIO Council should start by commissioning a biannual total compensation comparison between federal and private-sector cybersecurity jobs to more precisely measure differences in pay and benefits that may impact recruiting, hiring and retention. The comparison should be built off of the cyber professions that have been identified in the Cybersecurity Workforce Framework.

Track cyber attrition

OPM and the CIO Council should develop and administer a common web-based exit survey to track and understand the reasons behind cybersecurity attrition. An exit survey would further our understanding of why top talent is leaving across the government so we can learn how better to retain it.

OPM also could track the Federal Employee Viewpoint Survey data by occupation, which could point to warning signs before talent leaves government.

Develop a market-sensitive pay system for the cyber workforce

Once OPM completes the compensation comparison, the President's Pay Agent should immediately begin the design and development of a special occupational pay system for jobs covered by the Cybersecurity Workforce Framework.

The executive branch already has the administrative authority to implement pay reforms with respect to its mission-critical cybersecurity occupations.

This authority exists in an obscure, never-before-exercised provision of U.S. Code Title 5—Government Organization and Employees. Specifically, Section 5392 of Title 5 gives the President's Pay Agent—collectively, the directors of OPM and the Office of Management and Budget, and the secretary of labor—the authority to establish "special occupational pay systems" that supersede the limitations of the General Schedule. To do so, they must determine that for reasons of "good administration," those limitations "do not function adequately" for the jobs in question.

Under the law, the Pay Agent is authorized to "consider alternative approaches for determining the pay for employees" in the occupations in question. This could include broad pay bands that are adjusted according to the labor market for cybersecurity work, and progression within those bands would be based on competence, contribution and performance.

The law requires a number of procedural hurdles before such authority can be exercised. For example, the Pay Agent must consult with relevant agencies and labor organizations, publish its proposals in the Federal Register, conduct public hearings to collect input with regard to those proposals, and give Congress 90 days' notice before implementation. As long as these procedural requirements are met, the executive branch is free to move forward.

What might a special occupational pay system for cybersecurity look like? The Partnership and Booz Allen Hamilton released a broad blueprint in, "Building the Enterprise: A New Civil Service Framework," but there are a number of successful models already in existence. For example, DOD has operated such a system for thousands of acquisition professionals, as well as a variation for thousands of scientists and engineers in its vast complex of research laboratories, for more than two decades. These examples, which started as demonstration projects but were later permanently authorized, cover occupations that are as critical and complex as cybersecurity.

CONCLUSION

As society continues to enjoy new innovations from technology, it must be prepared for new threats. Because government is the means through which we address common societal needs, government has a critical leadership role to play in protecting the nation against cyber threats.

Taking a page from the nation's approach to counterterrorism, we believe it will take a network to defeat—or at least defend against—all the cyber threats against our network. And that network cannot just be one of terminals and fiber optic cables, it must be about the people. This process needs to begin with a comprehensive understanding of our existing federal workforce and the resources that we have available. We also need to anticipate the types of skills that we will need in the future.

There is no time to lose. The government is dependent on communication and information systems in all aspects of its operations and mission, from business transactions and national security, defense and law enforcement matters to processing, maintaining and transmitting sensitive and proprietary information.

Without the skilled workforce in place to protect the integrity of these systems, the nation will be highly vulnerable.

Currently, federal agencies are scrambling to attract and retain elite professionals to strengthen their defenses, but as outlined in this report, they often are impeded in getting some of the highly skilled employees by the absence of a government-wide strategy, and because of factors such as weak talent pipelines, insufficient applicant assessments, a cumbersome and inflexible hiring process, a lack of consistent and targeted training, non-competitive pay, and ill-defined job classifications and career paths.

In our 2014 report "Building the Enterprise: A New Civil Service Framework," we called for modernizing the decades-old federal personnel system to improve the way the government recruits, hires, classifies, pays and promotes federal employees. While these and other government-wide changes in the federal personnel system will take time to implement, they can serve as a framework for helping to build a world class cybersecurity workforce.

The cyber workforce is an ideal place to test the vision of a comprehensive workforce solution to meet a critical need.

The administrative changes that the Office of Personnel Management can take include the creation of a new cybersecurity occupational series and career paths; new candidate assessment tools that include cybersecurity competitions; and expanded direct hiring authority. The Office of Personnel Management also has the authority in the mid-term to put cyber work in the excepted service and create a special occupational pay system. Some of the longer term solutions include Congress expanding scholarship opportunities and allowing agencies to share their lists of top candidates. Additionally we have proposed agencies pooling training resources into a government-wide cybersecurity training academy and creating and coordinating a cyber reserve program.

Many of the personnel issues confronting the cybersecurity workforce are endemic in the federal system. Comprehensive civil service reform is needed in the long-term for the health of the entire federal government. However, in the short-term, the bottom line is that federal agencies need immediate help to deal with the escalating and increasingly sophisticated cyber threat.

APPENDIX ONE
METHODOLOGY

The Partnership for Public Service, with Booz Allen Hamilton, conducted interviews for this study from April through September 2014.

Our findings and recommendations come from interviews with more than 40 current and former cybersecurity officials, including chief information officers and chief information security officers representing more than 20 agencies, as well as cybersecurity workforce experts in academia and private-sector firms. In addition, we spoke to staff members of congressional committees with jurisdiction over cybersecurity and workforce issues.

To supplement our interviews, we conducted an extensive literature review and held two focus groups in August 2014 for junior or mid-career personnel who actively work in the area of cybersecurity at both federal and non-federal organizations.

We also held a dialogue in June 2014 with 20 senior executives from across government as well as representatives of cybersecurity certification organizations to outline emerging threats the government faces in the realm of cybersecurity.

APPENDIX TWO
CONTRIBUTORS

CONGRESSIONAL RESEARCH SERVICE

Eric Fischer, Ph.D.
Senior Specialist in Science and Technology

Wendy Ginsberg, Ph.D.
Analyst in American National Government

DEPARTMENT OF AGRICULTURE

Cheryl L. Cook
Former Chief Information Officer

Christopher Lowe
Chief Information Security Officer

Charles McClam
Former Deputy Chief Information Officer

DEPARTMENT OF DEFENSE

Gary Evans
Director, Information Management and IT/IM Workforce
Office of the Chief Information Officer

Stephanie P. Keith
Chief, Cyberspace Workforce Strategy & Policy Division
Office of the Chief Information Officer

Daniel Prieto
Former Director of Cybersecurity and Technology
Office of the Chief information Officer

DEPARTMENT OF EDUCATION

Steve Grewal
Chief Information Security Officer

DEPARTMENT OF ENERGY

Rodney Turk
Associate Chief Information Officer for Cybersecurity
Chief Information Security Officer

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Frank Baitman
Deputy Assistant Secretary for Information Technology
Chief Information Officer

Jennifer Duncan
Continual Service Improvement Lead
OS Office of Information Security

DEPARTMENT OF HOMELAND SECURITY

Luke Berndt
Program Manager, Science and Technology Directorate

Kristina Dorville
Branch Chief, Cyber Education and Awareness
Office of Cyber Security and Communications
National Protection and Programs Directorate

Renee Forney
Executive Director
CyberSkills Management Support Initiative

Travis Hoadley
Chief of Staff, CyberSkills Management Support Initiative

Richard Johnson
Branch Chief, Technology Implementation

Douglas Maughan, Ph.D.
Director, Cyber Security Division
Homeland Security Advanced Research Projects Agency
Science and Technology Directorate

Phyllis Schneck, Ph.D.
Deputy Undersecretary for Cybersecurity and Communications, National Protection and Programs Directorate

Benjamin Scribner
Program Director, National Cyber Professionalization and Workforce Development

Robin “Montana” Williams
Branch Chief, Cybersecurity Education and Awareness

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Melanie P. Cohen, D.M.
IT Strategic Planning and Communications
Office of the Chief Information Officer

Kevin Cooke
Deputy Chief Information Officer

DEPARTMENT OF THE NAVY

Chris Kelsall
Branch Head, Cyberspace Workforce
Office of the Chief Information Officer

Tony Martin
Navy Information Dominance Forces
Domain Cybersecurity Workforce Lead

DEPARTMENT OF TRANSPORTATION

Richard McKinney
Chief Information Officer

DEPARTMENT OF VETERANS AFFAIRS

Terri Cinnamon
Director, Information Technology Workforce Development
Office of Information Technology

Stephen Warren
Chief Information Officer

FEDERAL BUREAU OF INVESTIGATION

Chris Stangl
Acting Section Chief, Cyber Division

GOVERNMENT ACCOUNTABILITY OFFICE

Edward R. Alexander, Jr.
Assistant Director, IT Security

Gregory C. Wilshusen
Director, Information Security Issues

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY

Susan Alexander
Director, Safe and Secure Operations Office

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Lenora Gant, Ph.D.
Senior Executive for Academic Outreach and STEM

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ann Quigley
Deputy Chief, Workforce Planning and Competencies
Intelligence Community Human Capital Office

Daniel Scott
Deputy Assistant Director of National Intelligence
Human Capital

OFFICE OF MANAGEMENT AND BUDGET

Lisa Schlosser
Chief Deputy Administrator
Office of E-Government and Information Technology

OFFICE OF PERSONNEL MANAGEMENT

Lucy Antone
Human Resources Specialist, Strategic Workforce Planning, Talent Management Group

Angela Bailey
Chief Operating Officer

Jeanne Friedrich
Human Resources Specialist, Strategic Workforce Planning, Talent Management Group

Mike Mahoney
Manager for Hiring Policy, Center for Recruitment and Hiring, Employee Services

Sydney Smith-Heimbrock
Deputy Associate Director, Employee Services, Strategic Workforce Planning
Chief Learning Officer

Michael Torres
Program Manager, Human Resources Information Technology Transformation

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Tim Polk
Assistant Director for Cybersecurity

OFFICE OF THE CHAIRMAN JOINT CHIEFS OF STAFF

Rebecca Coleman
Public Affairs Officer

OFFICE OF THE PRESIDENT

Michael Daniel
Special Assistant to the President
Cybersecurity Coordinator

NATIONAL SCIENCE FOUNDATION

Victor Piotrowski
Lead Program Director, CyberCorps®: Scholarship for Service

NATIONAL SECURITY AGENCY

Christopher Dobyns
Manager, Human Resources Strategy Office

Daniel Christopher "Chris" Olexia
Deputy Manager, Office of Recruitment

NUCLEAR REGULATORY COMMISSION

Darren Ash
Deputy Executive Director for Corporate Management

U.S. CENSUS BUREAU

Josh De La Rosa
Project Management Team Lead

UNITED STATES MARINE CORPS

Master Gunnery Sergeant Leroy Hall
C4 Cyber Security Chief

Dr. Ray A. Letteer
Chief, Cybersecurity Division
Senior Information Security Official

113TH AND 114TH CONGRESS

Staff from the Senate Homeland Security and Government Affairs Committee

PRIVATE-SECTOR AND NONPROFIT CONTRIBUTORS

William "Joe" Adams, Ph.D.
Vice President, Research and Cybersecurity, Director of Michigan Cyber Range, Merit Network
Former Chief Information Officer, National Defense University

Robert Brese
Vice President, Executive Partners, Gartner, Inc.
Former Chief Information Officer, Department of Energy

Diana L. Burley, Ph.D.
Professor, George Washington University

General James Cartwright (Ret.)
Harold Brown Chair, Defense Policy Studies, Center for Strategic and International Studies
Former Vice Chairman of the Joint Chiefs of Staff

Michel Cukier, Ph.D.
Director, Advanced Cybersecurity Experience for Students
University of Maryland, College Park

Angel Diaz
President, Technical Services Corporation

Richard Danzig
Vice Chair of the Board of Trustees, RAND Corporation

Terry Erdle
Executive Vice President, CompTIA

John Felker
Director, Cyber and Intelligence Strategy, Enterprise Services, Hewlett-Packard
Former Deputy Commander, U.S. Coast Guard Cyber Command

Gary Gagnon
Senior Vice President and Chief Security Officer
The MITRE Corporation

John Gilligan
President and Chief Operating Officer, Schafer Corporation
Former Chief Information Officer, Departments of Energy and Air Force

Lee Holcomb
Former Chief Technology Officer
Department of Homeland Security

Lt. Col. Sean C.G. Kern
Adjunct Fellow for Cyber Leadership Policy, Pell Center for International Relations and Public Policy
Former Assistant Professor for Cybersecurity, National Defense University

Eric Loui
Cyber Threat Analyst
EWA-IIT

Admiral Mike "John" McConnell (Ret.)
Senior Executive Advisor, Booz Allen Hamilton
Former Director, National Security Agency

Ernest McDuffie, Ph.D.
Founder and Chief Executive Officer, The Global McDuffie Group
Former Program Lead for the National Initiative for Cybersecurity Education, National Institutes of Standards and Technology

Daniel Mintz
Program Chair, Information Systems Management
Collegiate Associate Professor
University of Maryland, University College
Former Chief Information Officer, Department of Transportation

Cliff Neve
Chief Operating Officer, MAD Security
Former Chief of Operations, Coast Guard Cyber Command

Alan Paller
Founder and Director of Research, SANS Institute

Marcus Richardson
Application Security Consultant, nVisium

Mark Silis
Director, IS&T Operations and Infrastructure
Massachusetts Institute of Technology

Richard Spires
Chief Executive Officer, Resilient Network Systems, Inc.
Former Chief Information Officer, Department of Homeland Security

Maurice Uenuma
Chief Operating Officer, Council on CyberSecurity

Dan Waddell
Director, Government Affairs, (ISC)2

Justin Wilder
Member, Technical Staff, In-Q-Tel

APPENDIX THREE
PROJECT TEAM

PARTNERSHIP FOR PUBLIC SERVICE

Mallory Barg Bulman, Managing Editor of Research
Beth Schill, Manager
Patrick Moniz, Associate Manager

Madeline Christian, Research Fellow
Bob Cohen, Writer and Editor
Max Ingraham-Rakatansky, Research Fellow
Sally Jaggar, Senior Strategic Advisor
Bevin Johnston, Creative Director
Jessica Law, Research Fellow
Audrey Pfund, Associate Design Manager
Lara Shane, Vice President of Research and Communications
Max Stier, President and CEO

BOOZ ALLEN HAMILTON

Ron Sanders, Vice President (Principal Contributor)
Andrew Smallwood, Lead Associate (Principal Contributor)

Lisa Dorr, Lead Associate
Judi Dotson, Executive Vice President
Mary Purdy, Lead Associate
Stephanie Shively, Associate
Erin Weiss, Lead Associate

PARTNERSHIP
FOR **PUBLIC SERVICE**

1100 New York Avenue NW
Suite 200 East
Washington DC 20005

(202) 775-9111
ourpublicservice.org
CFC# 12110

Booz | Allen | Hamilton

13200 Woodland Park Road
Herndon VA 20171

(703) 984-1000
boozallen.com