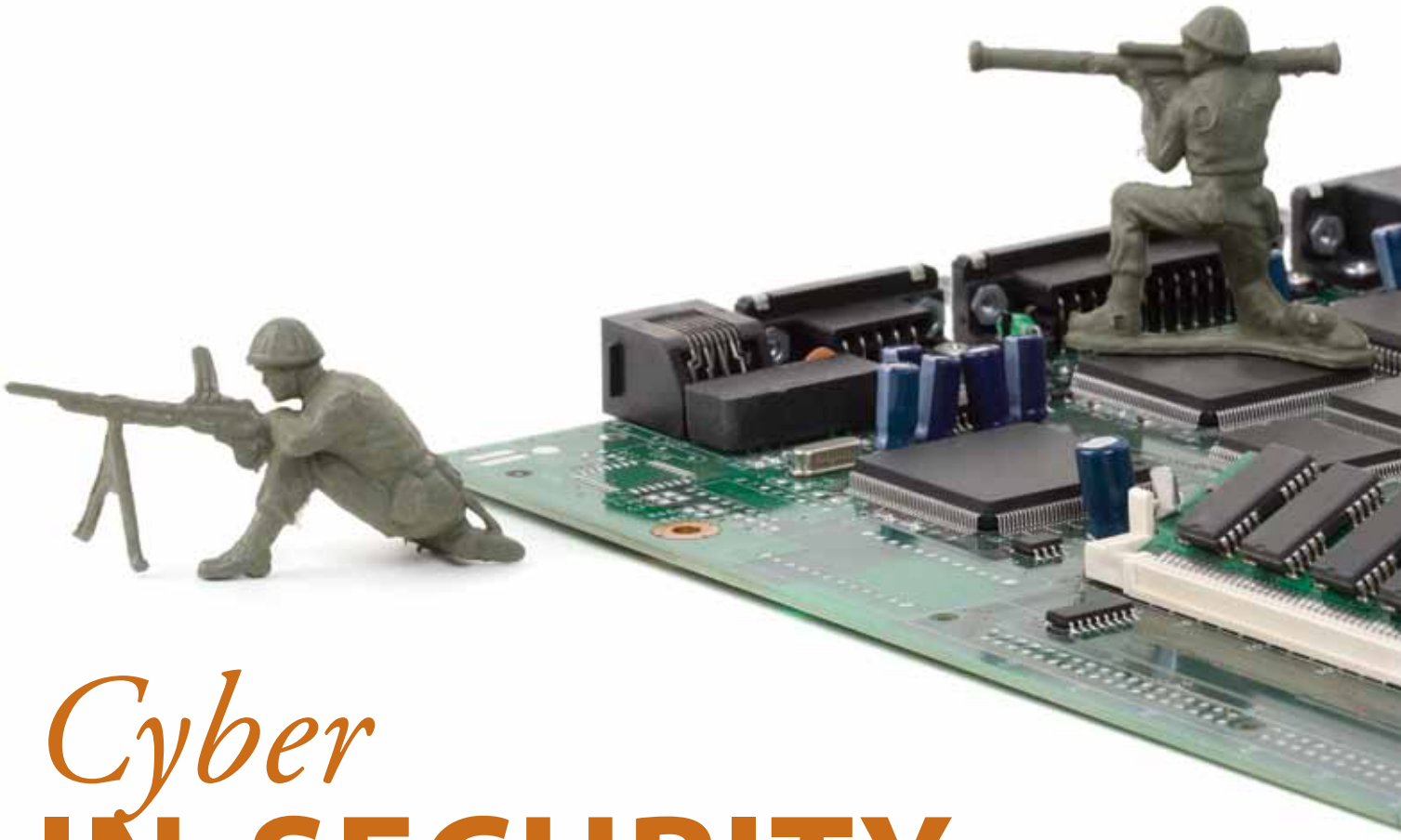

Cyber IN-SECURITY

Strengthening the Federal Cybersecurity Workforce

JULY 2009

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.

Booz Allen Hamilton has been at the forefront of management consulting for businesses and governments for more than 90 years. Providing consulting services in strategy, operations, organization and change, and information technology, Booz Allen is the one firm that helps clients solve their toughest problems, working by their side to help them achieve their missions. Booz Allen is committed to delivering results that endure.

EXECUTIVE SUMMARY

President Obama has declared cybersecurity to be "one of the most serious economic and national security challenges we face as a nation."[1] Critical government and private-sector computer networks are under constant attack from foreign nations, criminal groups, hackers, virus writers and terrorist organizations.

The president's success in combating these threats and the safety of the nation will depend on implementing a comprehensive and coordinated strategy—a goal that must include building a vibrant, highly trained and dedicated cybersecurity workforce in this country.

While the responsibility for securing our nation's computer networks is shared by the public and private sector, our federal government must take a leadership role. That is why the Partnership for Public Service and Booz Allen Hamilton examined the state of the federal cybersecurity workforce by interviewing experts inside and outside of government, and examining public testimony, reports and documents. The Partnership and Booz Allen held focus groups and surveyed federal chief information officers (CIOs), chief information security officers (CISOs) and human resource (HR) officials at 18 federal agencies.

Our federal government will be unable to combat these threats without a more coordinated, sustained effort to increase cybersecurity expertise in the federal workforce.

The results of this research are troubling and, in many ways, familiar.

With most Americans, it would hardly set off alarms to hear that our federal workforce faces significant challenges, such as difficulty in recruiting and retaining highly skilled workers, a reliance on contractors to fill talent gaps, poor management and arcane processes that undermine employee performance, and a lack of coordination that leaves some agencies competing against one another for talent.

What should get people's attention is the fact that these government-wide problems are particularly acute within the federal cybersecurity workforce, creating potential for major vulnerabilities for our national security.

The overriding finding of our analysis is that our federal government will be unable to combat these threats without a more coordinated, sustained effort to increase cybersecurity expertise in the federal workforce.

Defense Secretary Robert Gates has stated that the Pentagon is "desperately short of people who have capabilities (defensive and offensive cybersecurity war skills) in all the services and we have to address it." Our interviews confirm that this view is shared across government. Three-fourths of CIOs, CISOs, IT hiring managers and HR professionals surveyed for this report said attracting skilled cybersecurity talent would be a "high" or "top" priority through the next two fiscal years.

To fill current gaps, agencies look outside government for information technology (IT) talent. For example, an official at the Department of Homeland Security estimates that 83 percent of the staff in the office of its CIO are private contractors. Government not only needs to recruit and train more people with cybersecurity expertise, it needs more people who can effectively manage the blended cybersecurity workforce.

The other key finding of our research is that numerous factors hamper government's ability to build a top-notch cybersecurity workforce, making it difficult to fill critical talent gaps.

1 *Securing Our Nation's Cyber Infrastructure*, Speech by President Obama, May 29, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

"It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."

President Barack Obama, May 29, 2009

Our analysis revealed four primary challenges that threaten the quality and quantity of our federal cybersecurity workforce.

1. **The pipeline of potential new talent is inadequate.** According to our survey, only 40 percent of CIOs, CISOs and IT hiring managers are satisfied or very satisfied with the quality of applicants applying for federal cybersecurity jobs, and only 30 percent are satisfied or very satisfied with the number of qualified candidates who are applying. Our government runs a successful scholarship program to fill about 120 entry-level cybersecurity jobs with recent graduates, but officials say the need is much greater—closer to 1,000 graduates a year. For mid- and senior-level positions, no government-wide feeder program exists at all. More broadly, there are concerns that America is not developing enough IT experts, creating labor shortages in both the public and private sector.

2. **Fragmented governance and uncoordinated leadership hinders the ability to meet federal cybersecurity workforce needs.** Human capital management in the federal government is decentralized. Like other sectors of our federal workforce, there is no one in government in charge of cybersecurity workforce planning or decision making. No one interviewed for this report could provide an official count of the number of people in our government's cybersecurity workforce. In this fragmented climate, departments and agencies are on their own and sometimes working at cross-purposes or in competition with one another.

3. **Complicated processes and rules hamper recruiting and retention efforts.** Our federal government has a notoriously cumbersome hiring process, which deters talent of all types from entering government service, and there are many other systemic problems that raise challenges for our cybersecurity workforce.[2] How jobs are classified impacts managers' ability to bring in people with the right skills, but government is operating with an outdated and often vague job classification scheme for information security. One of government's computer science job categories was last updated in 1988, before the Internet was even invented.[3] In addition, there are no uniform government-wide certification standards for specific jobs categories, no federal career path for cybersecurity specialists, insufficient specialized training for workers to upgrade skills and salary caps that lag the private sector.

4. **There is a disconnect between front-line hiring managers and government's HR specialists.** Within agencies, hiring managers and human resources offices are often not on the same page. Our surveys reveal that front-line managers are consistently less satisfied with the effort to hire new cybersecurity talent than their peers in HR. In addition, 41 percent of the CIOs/CISOs and 38 percent of HR managers reported being either dissatisfied or very dissatisfied at the level of collaboration with the Office of Personnel Management (OPM), which should provide vital support for agencies looking to acquire skilled cybersecurity workers.

Although our research revealed a number of problems with the state of our federal cybersecurity workforce, it also uncovered many successful strategies to hire and retain top IT talent at individual agencies.

Based on these best practices, this report contains advice for what agencies can do right now to attract and retain critical cybersecurity talent. These recommendations cover ways to recruit candidates, market jobs, select talent and bring new talent on board.

In addition to these tips, this report also includes recommendations for the White House, OPM and Congress to address the more systemic problems which undermine the health of our federal cybersecurity workforce. In particular:

- **The White House cybersecurity coordinator, when designated by President Obama, should develop a government-wide strategic blueprint for meeting current and future cybersecurity employment needs, working closely with OPM**

2 *Memorandum for the Heads of Departments and Agencies*, Peter R. Orszag, Director of Office of Management and Budget, June 11, 2009.

3 *Position Classification Flysheet for Computer Science Series, GS-1550*, January 1988.

and agency leaders to develop and implement this plan. It should include the development of tools to measure the health of our cybersecurity workforce and provide guidance on the appropriate or desired roles for civil servants and for private contractors.

- **Much like our government did during the space race, the White House should lead a nationwide effort to encourage more Americans to develop technology, math and science skills. In conjunction with this effort, Congress should fund expansion of the successful programs that provide graduate and undergraduate scholarships in computer science and cybersecurity fields, such as the Scholarship for Service program, in return for a commitment to government service.**
- **Key government principals in the defense, intelligence and civilian information security fields, brought together under the direction of the White House cybersecurity coordinator and the Office of Personnel Management, should reach agreement on new, up-to-date job classifications for cybersecurity functions in government and establish certification requirements for each job category.**
- **These new job classifications should be the basis for OPM to map a cybersecurity career path starting at the entry-level.**
- **Congress should provide significant funding to train federal cybersecurity workers to meet the new standards and to provide employees with continual opportunities to upgrade and improve their skills to stay at the top of their game.**
- **Invest in management skills, too. It's not enough to recruit and retain individuals with technical cybersecurity expertise. Agencies also need to focus on developing a cadre of managers with the skills to effectively lead a multi-sector cybersecurity workforce.**
- **In addition to enhancing current efforts to streamline the federal hiring process, OPM should give agencies greater hiring flexibilities.**

The president has pledged that government computer networks will be "secure, trustworthy, and resilient," and that his administration will do everything possible to "deter, prevent, detect, and defend against attacks."

Achieving these goals requires a dedicated, highly trained and well-managed government workforce. Failure to address the government's critical cybersecurity workforce needs will undermine the president's commitment, and could result in increased vulnerability of systems and the data they house.

"We cannot afford to discover successful cyber intrusions after-the-fact, accept disastrous losses, and then seek merely to contain them. It requires a broad alliance of departments, agencies, and industry leaders to focus on countering the threat, mitigating vulnerabilities, and enhancing resiliency in order to preserve our national security, national economy, and public welfare."

Dennis Blair, Director of National Intelligence

Hearing on "Annual Threat Assessment of the Intelligence Community" for the Senate Select Committee on Intelligence, February 12, 2009

INTRODUCTION

The United States is facing threatening and unrelenting attacks against critical government computer systems that hold military and national security secrets, confidential federal documents and personal data including Social Security numbers, medical and tax records.

Some call it a cyber war, and in fact foreign powers have infiltrated the e-mail of Defense Secretary Robert Gates, stolen data from the Pentagon's most technologically advanced fighter aircraft, and hacked State Department computers and the electrical grid. There were millions of attempts to penetrate defense digital networks in 2008 and there have been thousands upon thousands of intrusions a year into civilian agency computers.

Director of National Intelligence Dennis Blair sounded an alarm in February 2009, telling Congress that government computer systems are being targeted for espionage by foreign nations such as China and Russia, as well as by criminal groups and individuals who may want to disrupt power, communication or financial systems. The Government Accountability Office (GAO) earlier this year reported weaknesses in the ability of 23 of 24 major agencies to detect or prevent cyber attacks, and investigators said that unless those flaws are corrected a "broad array of federal assets and operations will remain at unnecessary risk of fraud, misuse, and disruption."[4]

President Obama in May 2009 announced a new strategy led from the White House that includes appointment of a cybersecurity coordinator who will be "responsible for orchestrating and integrating all cybersecurity policies for the government."[5]

The White House plan is designed to overcome a system of bureaucratic conflicts, frequent turf battles and confusing lines of authority that have undercut the government's effectiveness in protecting the nation's digital networks.

The new presidential commitment follows previous efforts to deal with the cybersecurity challenge by both the Clinton and Bush administrations and Congress. This has included three major White House directives, billions of dollars in funding and congressional enactment of a variety of laws.

The previous initiatives and debates, however, have given scant attention to a crucial element in the cyber war—building the capability and caliber of the government's cybersecurity workforce.

The examination of the cybersecurity workforce by the Partnership for Public Service and Booz Allen Hamilton found several clear themes, including serious shortages of highly skilled cybersecurity specialists in government, and an absence of coordinated leadership on cybersecurity workforce issues, despite ongoing efforts by the CIO Council, individual agencies and others.

This study looks at the obstacles that have worked against building a top-notch workforce and examines the current approaches used by agencies to overcome hurdles to finding, hiring and retaining cybersecurity talent. We give voice to concerns and problems faced by hiring and information security managers, highlight some of their successes and make recommendations for systemic changes to enable agencies to find and keep the talent they need.

The heightened concern from the White House about cybersecurity offers a path for greater consideration of these critical workforce issues. Bringing about needed reforms and meeting the growing and ever-more sophisticated cybersecurity workforce requirements will not be easy, but it must be a national priority.

4 *High Risk Series: An Update* (GAO-09-271), Government Accountability Office, January 2009.

5 Securing Our Nation's Cyber Infrastructure, Speech by President Obama, May 29, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

FINDINGS

GOVERNMENT NEEDS MORE SKILLED CYBERSECURITY PROFESSIONALS

We discovered broad agreement that our government faces a serious shortage of highly skilled cybersecurity professionals, a personnel deficit that exists amid ominous daily reports of digital intrusions that threaten classified and military networks, personal and confidential data, and the country's critical electronic backbone, including our financial, aviation and electrical power systems.

Defense Secretary Robert Gates has stated that the Pentagon is "desperately short of people who have [defensive and offensive cyber war skills] in all the services and we have to address it."

Our research confirmed this high level assessment.

In a survey conducted at 18 federal agencies and subcomponents that hire cybersecurity talent, 76 percent of respondents ranked recruiting skilled cybersecurity talent a "high" or "top" priority through the next two fiscal years. "The need for more work on cybersecurity is growing. The pace of change and tasks in the cyber area is not going to stop," a deputy chief human capital officer (CHCO) from a major department told us.

A CIO at another large federal department noted, "A high level of talent is needed to be effective. The role played by cybersecurity in the department has changed from overseer to doer and real-time monitoring of security. There is a need for more detailed skills and policy, and understanding of concepts and issues. The role has changed and the need is very high."

An intelligence agency official has described a critical hiring need for cybersecurity specialists at nine major federal departments to support two important 2008 presidential national security directives, while Vance Hitch, the CIO at the Justice Department and co-chair of the CIO Council's Information Security subcommittee, said people with "cybersecurity skills are among the most difficult to find—if not the most difficult—especially the good ones."

Alan Paller, director of research at the Sans Institute, an organization that provides high-level information security training and certification, said the lack of high-caliber cybersecurity personnel is a critical problem for the government. "There is a radical shortage of people who can fight in cyber space—penetration testers, aggressors and vulnerability analysts," said Paller. "My sense is it is an order of magnitude short, a factor of 10 short."

An annual survey of federal CIOs reported in February 2009 by the industry trade association TechAmerica found that IT security was the top CIO challenge, including "critical skill shortages, especially for technical staff with certifications." The CIOs also reported concerns about retirement-eligible employees, and recruiting, retention and training.[6]

Turning to Contractors

The response at most agencies has been to turn to contractors to perform sensitive government information technology work, including computer and network security, vulnerability analysis, intrusion detection, digital forensics and protocol analysis.

The number of contractors doing cybersecurity work in federal agencies is not available, and the contractor-to-government employee ratio varies by agency. But information technology experts inside and outside government uniformly report that contractors account for a majority of the cybersecurity workforce at federal departments, including the Departments of Energy, Defense and Homeland Security.

A CISO at one major government department reported that "we have 18 full-time employees and probably 70 contractors."

Margaret Graves, the acting CIO at the Department of Homeland Security, told a House Oversight and Government Reform subcommittee on May 19, 2009, that one-third of approximately 600 major systems in use in the department reside in contractor facilities.

The inspector general of DHS reported in September 2008 that contactors accounted for 83 percent of the total staff of the department's office of the CIO.[7]

6 TechAmerica CIO Survey 2009 – 19th Annual Edition

7 *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), Department of Homeland Security, Office of the Inspector General, September 2008

"My sense generally in the IT world is that the contractor workforce dwarfs people on the federal payroll. In the classified world, a person with high-level clearances works for whatever contractor is serving that agency at the moment and they stay in place while bosses move around."

Frank Reeder, former government IT official and chairman of the nonprofit Center for Internet Security

There are good reasons that CIOs rely on contractors. Some information technology departments need specific cybersecurity skills immediately, and they can get this talent most readily through a contractor rather than through the laborious and time-consuming government hiring process. In other cases, CIOs may have a short-term need, making it better to hire a contractor rather than add a full-time government employee to the payroll. "Contractors provide flexibility," said one government IT official.

Budgetary limits on the number of full-time equivalent (FTE) employees also make contracting an attractive option. In addition, CIOs who need experienced cybersecurity specialists may not be able to hire this talent because federal pay rates are too low in comparison to the private sector rates for the same skills. A contractor may more likely meet salary demands and be able to provide experienced talent.

"Contractors can afford to pay the workers more, they have their finger on the pulse of innovation a little more than government and they tend to get the best and brightest people who are highly skilled," said Greg Garcia, a former DHS assistant secretary for Cyber Security and Communications. "And when the task is finished or the need for the specialized skills goes away, contractor requirements can be decreased."

Garcia said another reason for the large contractor workforce centers largely on the "broken hiring process" that takes too long, is bureaucratic and makes it hard to get the right talent. He said it sometimes takes as long as a year for new hires to get security clearances. "Contractors hire really fast and put people on site," said Garcia. "As a business model, having a contractor is good for a surge and good for downsizing."

Managing the Multi-Sector Workforce is Complicated

Despite the demand and some clear benefits, using contractors is not risk-free. One government information security specialist noted that a key to successful contracting is having the right talent inside an agency to monitor and manage the work. Without the skills to successfully manage and review the work of contractors, he said, serious problems can occur, including delays, cost overruns and technical problems.

David Powner, the GAO director of IT management issues, told a Senate Homeland Security and Governmental Affairs subcommittee in April 2009 that agencies do not manage risk well or do not always have a complete understanding of what they buy when they award a contract. "Sometimes the government is flying blind. We don't realize we have cost, schedule and performance problems until someone says we have a 30 percent variance. Why didn't we know when it was at 15 percent or 20 percent? Because we weren't watching and didn't know what was going on."

Our interviews did not specifically examine the quality of the management of both our civilian and contractor cybersecurity workforces, but there is evidence suggesting room for improvement. For example, a September 2008 report by the Department of Homeland Security's inspector general found that "the DHS CIO remains hindered in his ability to fully integrate IT management practices to ensure IT investments fulfill mission goals."

Further, the Partnership's *Best Places to Work in the Federal Government* rankings have consistently found that the greatest driver of employee satisfaction—by far—is effective leadership.

THE PIPELINE OF NEW CYBERSECURITY TALENT IS INADEQUATE TO MEET AGENCY NEEDS

Solving government's cybersecurity problems requires having enough of the right people with the right skills to carry out critical missions—professionals with experience and know-how in computer network engineering, forensics, software development, defense, vulnerability

and protocol analysis, intrusion detection, and in the case of the military and intelligence communities, digital exploitation and attack.

Our survey of CIOs, CISOs and hiring managers found 41 percent were dissatisfied or very dissatisfied with the number of qualified applicants for information security openings, and one-third were dissatisfied or very dissatisfied with the quality of the candidates HR referred to them. The survey also found that 33 percent were dissatisfied or very dissatisfied with the number of candidates who accept job offers.

A July 2008 GAO report, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, cited difficulties hiring and retaining adequately trained cybersecurity analysts in DHS's Office of Cybersecurity and Communications' (CS&C) Computer Emergency Readiness Team (US-CERT). US-CERT is the focal point for the government's interaction with federal and nonfederal entities for cyber-related analysis, warning, information sharing, major incident response and national-level recovery efforts. It is also charged with disseminating cybersecurity information to improve warnings and respond to attacks.

"Obtaining and retaining adequately trained cyber analysts and acquiring up-to-date technological tools to implement the analysis capability attributes is an ongoing challenge to US-CERT and other analysis and warning centers, hindering their ability to respond to increasingly fast, nimble, and sophisticated cyber attacks," said the GAO.

The problem with the amount of available cybersecurity talent extends beyond government.

Lt. General William Shelton, the CIO of the Office of the Secretary of the Air Force, told a House Oversight and Government Reform subcommittee in May 2009 that "in terms of technical expertise, we have, certainly, a concern along with everyone else in the nation that there's just not that many people coming out of our schools that are prepared for the technical type of work."

"They don't have the educational background, haven't studied math, engineering science, those sorts of things," he said.

Successful Scholarship Programs are Too Small

By far the most important sources of entry-level hiring are scholarship programs, specifically the Scholarship for Service Program (SFS)—run by DHS—OPM and the National Science Foundation (NSF), and the smaller Department of Defense (DOD) Information Assurance Scholarship Program.

SFS is the federal government's most successful, but still limited, pipeline for young cybersecurity talent. Commonly known as the "Cyber Corps," the program now has about 225 students enrolled at several dozen colleges and universities designated as Centers for Academic Excellence in Information Assurance Education. Approximately 80 percent are in master's degree programs; the rest are working toward doctorates and bachelor's degrees. About 1,080 students have taken part in SFS since it was created in 2000; more than 870 have graduated and entered government service to complete their one-year service commitment for each year of scholarship support. The hiring process is streamlined for most SFS candidates, since agencies can use direct hire authority for the 2210 job series at GS-9 or above, or use student programs, such as the Federal Career Intern Program (FCIP) or the Student Career Experience Program (SCEP).

While about 120 SFS students currently graduate each year and then move into federal cybersecurity jobs, officials say the need is much greater. Victor Piotrowski, head of the SFS program, said a 2008 presidential cybersecurity directive estimated that between 500 and 1,000 such graduates are needed every year.

SFS funding has averaged about $12 million a year. The "Cyber Security Act of 2009," introduced by Sen. Jay Rockefeller (D-W.Va.) to overhaul the government's computer security apparatus, would dramatically increase SFS spending to $300 million over five years to fund up to 1,000 cybersecurity scholarships per year.

In the past several years, government agencies have competed with each other for Cyber Corps graduates. The National Security Agency (NSA) and DOD have hired the most SFS graduates, causing some to feel like these two agencies snatch up the best candidates in some instances because of offers of higher pay. One agency made 10 job offers to SFS candidates and only three even considered the opportunities. Another agency HR professional said, "We are outbid by other agencies—FBI, NSA, DHS. They have gotten exceptions where they can hire at any level... people jump ship and go to NSA."

FILLING FEDERAL CYBERSECURITY "PIPELINES" WITH UNIVERSITY STUDENTS

Scholarship for Service (SFS)

- Purpose
  Created in 2000 to increase and strengthen the number of federal information assurance professionals who protect the government's critical information infrastructure.
- Size
  About 120 SFS students graduate annually. Currently 225 students enrolled: 80 percent in master's programs, some working toward doctorates, and the rest pursuing a bachelor's degree. Total students since inception—1080; 870 graduated and entered government.
- Program Provisions
  Provides tuition, books, room and board plus an $8,000 annual stipend for the last one to two years of undergraduate study, or $12,000 a year for up to two years of graduate school. Must intern with a federal agency while in school; must work for an equivalent amount of time as received scholarship funding.
- Funding
  The scholarships are funded through grants from the National Science Foundation to 34 accredited colleges and universities around the nation. To compete, each school must be designated by NSA and DHS as a Center of Academic Excellence in Information Assurance Education.
- Job Placement
  NSF annually sponsors a career fair in January for SFS students to meet with agency representatives. In January 2009 there were 69 job booths and about 120 candidates.
- Hiring Processes and Authorities
  An advantage for agencies is the relative ease of the hiring process. Students post their résumés on an OPM Web site (www.sfs.opm.gov). Government recruiters can register on the Web site, easily contact participants directly to explore internships, long-term, full-time or permanent placement opportunities.

  Agencies may offer SFS participants recruiting incentives and can use direct hire authority for 2210 series information security positions above a GS-9 (for students who earn a master's degree).

  For other information assurance positions, agencies can appoint SFS students to internships or long-term positions using hiring authorities that include competitive examining, merit promotion, the Federal Career Intern Program (FCIP), the Student Career Experience Program (SCEP), and any appropriate noncompetitive placement authority for hiring individuals in fellowship and intern programs (5 CFR 213.3102(r)).

Defense Department's Information Assurance Scholarship Program (IASP)

- Purpose
  To assist in the recruitment and retention of highly qualified cybersecurity specialists needed for war fighting and the security of the Pentagon's information technology infrastructure.
- Program Description
  Non-Defense Department employees (students) must serve in SCEP internships at DOD during school breaks and work for DOD following graduation. Students are paired with DOD subcomponent agencies at the start of program, allowing the clearance process to begin right away. Current DOD civilian and military members may attend school either full- or part-time to earn master's or doctoral degrees (at the Air Force Institute of Technology at Wright-Patterson Air Force Base in Ohio; the Information Resources Management College of the National Defense University in Washington, D.C. in cooperation with 27 partner universities; and the Naval Postgraduate School in Monterey, Calif.).
- Size
  Twenty-five to 30 new recruitment scholarships annually from college students; 25 to 30 retention scholarships to military and civilian defense department employees.
- Program Provisions
  Provides non-DOD or military college students full tuition, required books, and selected fees, lab expenses, supplies and equipment; a stipend to cover room and board ($10,000 per year for undergrads; $15,000 for graduate students). Recipients incur a commitment to service determined by the length of the scholarship. Current DOD or military employees continue to be paid their salaries and are obligated to three years of service for every year of education.

TABLE 1

SFS GRADUATE HIRES BY AGENCY

Fiscal Year 2006 – January 2009

Agency	FY 2006	FY 2007	FY 2008	Total Hires
NATIONAL SECURITY AGENCY	53	31	29	113
DEFENSE	34	32	26	92
FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS (FFRDCs)*	27	25	12	64
CENTRAL INTELLIGENCE AGENCY	11	3	3	17
GOVERNMENT ACCOUNTABILITY OFFICE	10	4	3	17
FEDERAL RESERVE SYSTEM	5	5	3	13
JUSTICE	5	3	2	10
HOMELAND SECURITY	0	6	3	9
COMMERCE	3	3	2	8
TREASURY	0	2	4	6
Other Agencies*	16	29	13	58
Total placements as of 01/30/09	164	143	100	407

Source: National Science Foundation, SFS program data

*FFRDCS and "Other Agencies" include CMU/Computer Emergency Response Team (CERT), Aerospace Corporation, NSEP Boren Fellowship, EMRTC/division of NMT, JHU/APL, Institute for Defense Analysis (IDA), Brookhaven, Mitre Corp, Idaho National Library, Lawrence Livermore National Laboratory, Arroya Center, Pacific Northwest National Laboratory (PNNL), Los Alamos National Lab, Army Software Engineering Institute, Sandia Laboratory

Between Fiscal Year 2006 and January 2009, NSA hired 113 SFS students and DOD hired 92 of the 407 eligible SFS students. However, all of the agencies that use the program that we spoke with still view it as a good source of qualified entry-level talent despite interagency competition.

DOD operates a comparable cybersecurity program—the Information Assurance Scholarship—as both a recruitment and retention tool. It is available to college students, and Defense Department civilian employees and military officers, who pursue studies in data security, network security and other information security specialties at schools designated as Centers for Academic Excellence in Information Assurance Education. Each year, DOD awards 25-30 new recruitment scholarships for college students and another 25-30 retention scholarships to military and civilian employees.

The students who receive scholarships are required to serve internships through SCEP with DOD during breaks in the school year and work for DOD after they graduate. DOD pairs students with subcomponent agencies when they start, so those agencies can start the clearance process early.

Current DOD civilian and military members can attend school either full- or part-time to earn master's or doctoral degrees. They continue to be paid their salaries and tuition, books and other expenses are covered. Military and civilian employees agree to serve three years for every year of education covered by the scholarship.

In addition to depending upon these important "pipeline" programs for entry-level students, some government HR officials say they go directly to college campuses and have built relationships with career counselors and computer and engineering departments. For example, HR officials at GAO recruit every year at selected universities, in addition to hiring entry-level talent through SFS.

The Pentagon is also sponsoring national competitions for high school and college students that test their skills in attacking and defending digital targets, stealing data and tracing how others have stolen it. Forbes magazine reported in May 2009 that talented participants will be recruited for cybersecurity training camps in the summer of 2010 run by the military and funded by private companies. Others could be offered internships at agencies including NSA and the Department of Energy.[8]

No Comparable Talent Stream for Higher-Level Positions

Although some agencies prefer to bring in new talent as entry-level hires so they can train them to have the skills they need, most also need experienced, higher-level employees. A Treasury official said his department's hiring need for cybersecurity is at the mid-range, usually people at the GS-12, -13 and -14 levels.

CIOs and their human resources counterparts primarily rely on a limited number of ways to attract experienced talent. Most experienced mid- and senior-level hiring is done by posting jobs on the USAJOBS.gov Web site. Transfers of experienced personnel between agencies can be an important talent source, with many coming from DOD.

The Federal Energy Regulatory Commission (FERC) looks for talent in companies in industries undergoing layoffs. Others ask employees and colleagues to actively refer people they know who may have needed skills, circulate job announcements to contractors already working with them, and go to professional association meetings to search for candidates.

8 Forbes, *Pentagon Seeks High School Hackers* (May 21, 2009)

FRAGMENTED GOVERNANCE AND UNCOORDINATED LEADERSHIP HINDERS THE ABILITY TO MEET CYBERSECURITY WORKFORCE NEEDS

Responsibility for the security of the government's computer systems and critical national infrastructure is shared across numerous federal agencies, with the lines of authority frequently blurred and decision-making splintered.

This holds true not just for decisions about strategy, policy, technology and technical standards, but for the government's all-important cybersecurity workforce that must carry out the policies and perform the highly skilled day-to-day tasks of protecting the computer networks.

Currently, there is no strategic government-wide assessment of the current state of the cybersecurity workforce, its size, strengths and weaknesses. There is no federal plan projecting how many cybersecurity specialists will be needed next year or in the next five years to meet individual agency and government-wide needs, what skills and certifications they should possess, how they should be trained, or how they should be recruited into federal service.

There also is no assessment of the nature and scope of the role now being played by private contractors, and whether the balance of responsibilities is appropriate or should be changed.

In short, there is no one in government in charge of coordinating cybersecurity workforce planning or decision-making, leaving agencies on their own to find scarce talent or to come up with their own standards and requirements.

There is also uncertainty about the total size of the cybersecurity workforce. The Pentagon has publicly stated that it has more than 90,000 personnel—military, civilian and contractors—working with services and agencies deemed to be involved with cybersecurity. The non-DOD civilian cybersecurity workforce has been estimated by a variety of officials to range from 35,000 to 45,000, while the intelligence community numbers are classified.

Angela Bailey, the associate director of the Center for Talent and Capacity Policy at the Office of Personnel Management, said there is not an exact count of who is employed in cybersecurity occupations because of the varying job definitions and lack of consistency in this field across the government. "I can tell you the number of information technology specialists who specialize in 'security,' but cannot provide data on 'cybersecurity'," said Bailey. "It's a rapidly emerging area. Cybersecurity at one agency means one thing and at another it means something else. It makes it difficult to define scope or severity of a problem when it is not universally defined or agreed to as to its meaning."

Without a central coordinator, it is not surprising that we found little evidence of agencies working together to increase awareness of federal opportunities in cybersecurity and information assurance. Important exceptions to this are the SFS program and the Centers for Academic Excellence in Information Assurance Education program run by NSA and DHS to promote information assurance education at several dozen universities, across the country.

Rather than cooperate, however, in many cases agencies compete with each other for cybersecurity hires. Even within one agency a subcomponent may find itself competing against other agency subcomponents. At a recent Cyber Corps job fair, for example, DHS bureaus and subcomponents were recruiting at six different booths for SFS grads-to-be.

President Obama, in May 2009, created the post of cybersecurity coordinator in the White House, and promised "a new, comprehensive strategy to secure America's information and communications networks."

As part of this effort, the administration's publicly released documents said an interagency policy committee and the White House coordinator "should consider how to better attract cybersecurity expertise and to increase retention of employees with such expertise within the federal service."

The policy document, however, offered no details.

Critical components of the U.S. cybersecurity strategy and any workforce planning include the 16 intelligence agencies that operate under the umbrella of the Director of National Intelligence with special responsibilities at the Department of Homeland Security. The Defense Department, which is considering its own new cybersecurity military command, is also a major participant.[9]

9 The organizational members of the national intelligence community operating under the Director of National Intelligence and the Undersecretary of Defense for Intelligence include intelligence components of the Air Force, Army, Navy and Marine Corps; the Central Intelligence Agency, Federal Bureau of Investigation, Coast Guard, Drug Enforcement Administration, Defense Intelligence Agency, National Reconnaissance Office, National Geospatial-Intelligence Agency and National Security Agency; and intellegence components of the Departments of Energy, Homeland Security, State and the Treasury.

Every agency of government, from the Internal Revenue Service to the Department of Veterans Affairs and the Social Security Administration, needs to protect its internal systems, faces constant threats from intruders and has a role to play in a federal cybersecurity strategy. The Federal Energy Regulatory Commission (FERC), the Federal Reserve Board and the Federal Aviation Administration, for example, have cybersecurity responsibilities for the industries they regulate. Recent disclosures about potential attacks on the nation's power grid provide a chilling example of what an agency like FERC faces.

There are many other players in this arena whose roles must be in sync in developing a strategic plan and new policies. The National Institute of Standards and Technology sets technical specifications for computer and network security. The Office of Management and Budget rates agency compliance with the Federal Information Security Management Act (FISMA), and OPM sets hiring and job classification rules.

The Government Accountability Office and agency inspectors general have responsibilities for assessing and monitoring agency performance. Agency CIOs and CISOs have critical operational responsibilities that include planning, acquiring and managing technology, and overseeing workforce needs.

Government agencies individually face many complex demands. The Obama administration, as part of its broad-based review conducted earlier this year, identified more than 250 policy directives, executive orders and strategies related to federal information security.

It will be a challenge for the Obama administration to coordinate cybersecurity policies; however, by doing so it can bring focus and direction to solving federal cybersecurity workforce problems.

"We do not have a technology problem. We have a leadership problem. Leaders have to decide how they want to address the security issues and human capital flows from that," said Norman Lorentz, the first government-wide federal chief technology officer (CTO) at OMB during the Bush administration.

PROCESSES AND RULES HAMPER RECRUITING AND RETENTION EFFORTS

Government information technology managers, like their counterparts in other parts of the federal system, must deal with cumbersome and often inflexible rules and processes.

The Hiring Process Is Broken

Few things in government are more widely criticized than the process for hiring new employees, and the process for hiring cybersecurity talent creates its own set of unique challenges.

A September 2008 report by the DHS inspector general said the department's office of the CIO has had great difficulty hiring and retaining qualified staff to fill its authorized positions because of the "lengthy and burdensome hiring process."[10]

Intelligence agencies, such as the NSA, have more flexibility in hiring and setting compensation than the civilian agencies. Many non-intelligence agencies have less experience successfully attracting and developing cybersecurity specialists because they have a smaller cybersecurity workforce.

In interviews with CIOs and CISOs, as well as industry leaders, many remarked that it is difficult for HR to understand what their skill and experience needs are because the HR professionals do not fully understand the technical aspects of cybersecurity jobs. Specifying requirements in job announcements can be difficult because HR wants to cast a wide net to give the hiring manager enough highly qualified applicants to interview. On the other hand, the hiring manager may be looking for a very narrow set of skills or experience to fill a precise set of needs in his or her shop.

Survey respondents are also troubled by how long it takes to fill vacancies. Our survey found that 77 percent of the CIOs, CISOs and IT hiring managers were dissatisfied or very dissatisfied with the time it takes to close the deal and hire someone. Private sector employers are often able to offer jobs on-the-spot or during on campus interviews to qualified candidates. In comparison, new federal employees tell us the federal application process is plagued with lengthy delays. Frequently, job applicants

10 *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain* (OIG-08-91), Department of Homeland Security, Office of the Inspector General, September 2008

"We need to realize that it's not the work and the agencies that keep competitiveness low. It's the process."

HR official at a major government department

find that HR contacts are not knowledgeable about the status of their applications. Added to the perceived pay gap with the private sector, complicated hiring processes and lengthy delays can cause the best candidates to go elsewhere.

Fifty-four percent of all survey respondents said they were dissatisfied or very dissatisfied with delays caused by the security clearance process. New federal employees reinforced this when they mentioned that the lengthy security clearance process either caused some candidates to seek positions requiring a lower-level clearance or tempted them to work for contractors who can use them in non-secure functions or provide training until they receive their security clearances.

Government Lacks Clear Definitions for Cybersecurity Jobs

Digging deeper, one of the biggest problems with the process for hiring cybersecurity talent is government's job classification system.

The Information Technology (IT) Management Series, known in government parlance as General Series (GS) 2210, is the primary classification for federal information technology employees. Within IT, 2210 breaks into 11 sub-classification or parenthetical titles.

Although cybersecurity issues cut across many IT functions and involve very specialized skills and training, the GS-2210 security sub-classification (INFOSEC) defines this work only in broad generalities. These include "ensuring confidentiality, integrity, and availability of systems, networks, and data through planning, analysis, implementation, maintenance, and enhancement of information systems, security programs, policies, procedures and tools."

A complicating factor is that cybersecurity can be part of several different functions and job families or classifications, not just in the IT series. For example, professionals classified as GS-0854 Computer Engineers, GS-0855 Electronics Engineers and GS-1550 Computer Scientists may perform cybersecurity-related tasks or may require specific cyber-related training and knowledge. One relatively young federal employee who has been doing cybersecurity work in government for five years told us that he has worked in four different job titles and job series, even though he has always been performing cybersecurity functions. Only one job was classified as a "2210."

Since the activities and responsibilities of government cybersecurity positions are ill-defined, IT managers and human resource professionals say it is hard to describe to potential applicants and candidates what cybersecurity jobs entail, and therefore difficult to find the right talent. In addition, job seekers cannot readily identify available jobs or decide if they're qualified or interested, because they may not know how to translate "government speak" to figure out what category or job title to consider.

Line managers reported it is very difficult to accurately describe the skills they need. Many job applications require candidates to answer questions about their relevant skills and experience. These questions are important, because candidates' answers are rated to determine who is

"The first thing that needs to be done is to define the job skills and competencies needed to perform these jobs."

Agency program manager

GS 2210
INFORMATION MANAGEMENT TECHNOLOGY SERIES

The 11 sub-classifications in the 2210 job family series:

- Policy and Planning
- Network Services
- Enterprise Architecture
- Data Management
- Security
- Internet
- Systems Analysis
- Systems Administration
- Applications Software
- Customer Support
- Operating Systems

qualified. However, hiring managers' ideas of what these questions should be do not always fit cleanly within the "official" job description in the occupational series. Further, some "old" jobs—such as fraud detection, network management and engineering—now include cybersecurity functions that are not reflected in the position descriptions.

Many experts we spoke to believe the government classifications must be updated by creating a cybersecurity specialty that defines a core set of required skills and replaces the current broad definitions.

A program manager at a large government department said OPM needs to be more proactive and update job descriptions across the board for IT security to meet today's realities. "The current job titles are meaningless. The skills and the certifications aren't comparable across agencies," noted one HR professional who recruits cybersecurity talent.

Some of the job categories outside the 2210 series are also outdated and need revision. For example, the position classification for Computer Science Series GS-1550 is dated January 1988, well before the Internet was widely used.

According to an OPM official, the impetus for this kind of change must come from the government information technology community. This official said that various parties in the government information technology sector have not reached agreement among themselves on many of the issues, making it hard for OPM to take any meaningful steps.

No Career Path for Cybersecurity Workers

Experts also call for the creation of a career path for cybersecurity specialists that will help job candidates and employees understand how to gain increased experience, responsibility and pay increases, thereby promoting retention. A defined career path also will help agencies grow the expertise they need by describing the knowledge and competencies required for career progression.

A prestigious commission convened by the Center for Strategic and International Studies last year cited the importance of developing such a career path, finding that it would allow individuals to "move to more senior positions as experience is gained, without moving to different career fields, to be compensated according to increased skills, and to expect that particular field will provide for continued training and advancement."[11]

> "We need to be able to keep them happy by allowing them to grow in the field and stay active."
>
> HR professional in the intelligence community

This report noted that there are very specific cybersecurity skills not described in current job classifications that should require minimum entry requirements and specialized training. Examples include "vulnerability analysis, intrusion detection, digital forensics, reverse engineering, protocol analysis, penetration testing, secure network engineering, and computer network attacks."

Greg Wilshusen, director of information security issues for the GAO, told a House Oversight and Government Reform subcommittee in May 2009 that members of the cybersecurity government workforce should be viewed as professionals, getting certified in specific skills and becoming licensed. He said the profession must take actions on its own, but added that it would be helpful if Congress played a role.

"It's more than just passing an exam, but actually licensed and bonded," he said. "We do this with real estate sales people. We do it with people who groom dogs. We do it with lawyers and countless other professions."

There have been several cybersecurity workforce initiatives in government seeking to revise job classifications and competencies, but they appear to be operating on unilateral tracks.

The Federal CIO Council IT Workforce Subcommittee is conducting a comprehensive appraisal of the IT workforce for the federal community to develop a cybersecurity skills matrix. The intelligence community is separately working on its own project to define cybersecurity competencies.

The Defense Department, by far the largest information technology employer in the government, has successfully defined the competencies its cybersecurity employees

11 *Securing Cyberspace for the 44th Presidency*, The Center for Strategic and International Studies, December 8, 2008.

need. In 2006, the Pentagon created an Information Assurance Training, Certification and Workforce Management Plan that established certification standards across the entire DOD information security enterprise based on commercial specifications. DOD requires all civilian, military and contract employees to obtain the training and certifications they need to meet or exceed work requirements.

About 30 percent of the DOD information assurance workforce has been certified, and the goal is full department compliance by 2011. George Bieber, director of the DOD program, said the initiative will create a framework to improve workforce management and allow DOD to set baselines that will help place people with the right skills in the right jobs at the right times.

In October 2007, DHS issued a resource guide known as the Information Technology Security Essential Body of Knowledge (EBK) for government workforce planning. Noting that the rapid advances in the digital environment "have been nonlinear and sometimes chaotic, leading to disparities in the composition of the information technology workforce," this "umbrella document" seeks to create a national baseline of essential knowledge and skills for IT security professionals.

Pay Limitations Make It Harder for Government to Compete for Top Talent

Our survey found salary ranges for information security personnel pose a challenge for some agencies when it comes to recruiting and hiring top talent.

Only 30 percent of CIOs and CISOs said they were satisfied or very satisfied with the compensation package they could offer prospective employees. One CIO told us that pay is not competitive for the top talent he needs, "and even when human resources thinks the pay is generous, it is not enough."

Fifty-one percent of CIOs, CISOs and hiring managers and 55 percent of HR professionals said they were dissatisfied or very dissatisfied with their ability to compete with the private sector for qualified candidates. Some agencies take full advantage of hiring incentives already available, such as relocation bonuses, student loan repayment commitments and tuition reimbursement for future courses, but others do not. An HR professional at a small agency that recruits highly-technical information security talent said private industry has a leg up. "There are some industries you just can't compete with for salaries," she said.

Intelligence agencies and those not tied to the GS scale have pay flexibility that can make them more competitive with the private sector, but not all agencies have this flexibility. This difference results in intelligence agencies having a pay advantage over their non-intelligence counterparts for new hires.

Salary limitations also hurt retention. Although data are not available on specifically why employees leave cybersecurity positions, HR professionals, CIOs and CISOs told stories of valued employees being lured away by the private sector and other agencies with pay flexibilities for reportedly multiples of what they were earning. In the survey, CIOs and CISOs felt that low salary and a lack of advancement opportunities were major causes of attrition.

The salary issue cuts across the board, from new hires to experienced professionals.

UniversumUSA conducts an annual survey of more than 40,000 U.S. undergraduates, asking them the characteristics they seek in their first employers. Universum's Survey of Ideal Employers™ (2008) found undergraduates with IT backgrounds and interests in cybersecurity or information security expected to earn at least $57,000 for their first job after graduation.

In contrast, an entry-level hire starting at a GS-7 position (if they qualify with at least a 3.0 GPA from a four-year college) will start around $45,194 or $53,234 (GS-9) for someone with a master's degree. Prior relevant experience or other factors can provide the basis for a higher starting salary.

Recently hired employees and agency hiring managers reported that the private sector cybersecurity pay rates are higher.

Definite assets for federal employers, however, are the benefits package and workplace flexibilities government offers. Among survey respondents, 65 percent were either satisfied or very satisfied with both benefits and flexibilities. The Universum survey found that students highly value work/life balance and view government/public service as strong in this area.

Savvy agencies create compensation packages that take full advantage of non-financial benefits. Many applicants at all experience levels are eager to "make a difference" or

give back through government work, and are willing to consider total compensation (the full package of salary, benefits and incentives). In these cases, when the critical importance of cybersecurity work is emphasized and other benefits are explained, government is more competitive. As several new employees told us when we asked them why they continue to work in cybersecurity for the federal government, despite the lure of the contractor world, they stay because, "It's fun!"

THERE IS A DISCONNECT BETWEEN HIRING MANAGERS AND GOVERNMENT'S HR SPECIALISTS

In addition to finding limited coordination on cybersecurity matters across different agencies, our research found that government's HR professionals and the CIO/CISO community do not always seem to be on the same page.

Disconnect within Agencies

Within agencies, our survey and interviews identified a disconnect between hiring managers and human resources, with both groups suggesting that there are problems with collaboration.

CIOs, CISOs and IT hiring managers, for example, think the problems are more severe than HR professionals do when it comes to applicant quality and hiring timeliness. While 33 percent of CIOs, CISOs and hiring managers were unhappy with candidate quality, only 10 percent of the HR managers were dissatisfied. And 61 percent of the HR managers (compared to only 40 percent of CIOs, CISOs and hiring managers) said they were satisfied or very satisfied with the quality of job candidates.

There is also evidence that IT managers and their agency HR colleagues do not always work cooperatively. Thirty-eight percent of the CIOs, CISOs and hiring managers were dissatisfied or very dissatisfied with the level of collaboration with the HR department, while 31 percent of the HR managers said they, too, were unhappy with the level of collaboration.

> "The human capital management process is broken. Operations and HR people should be joined at the hip and collaborate across government."
>
> Norman Lorentz, the former government-wide CTO at OMB

A technology specialist at one government agency said he hired three people last year using the 2210 series for IT specialists, but it was a struggle writing a precise job description and then getting the talent he needed. "HR says pick a series. You are constrained in how you write the questions" for assessing the applicant's relevant skills. In the end, this official said he did not feel he was getting the best possible candidates from the process.

A frustrated CIO at a major government department said his HR people "don't know the difference between good and bad candidates. They don't get it. We don't have enough good people. They just don't get it unless they are enmeshed in our world."

But there are two sides to this story. An agency HR official said hiring managers and CIOs "don't always understand that it must be a fair and open application process." HR professionals are often forced to be the guardians of multiple rules, regulations and procedures, which are perceived by many as barriers to timely hiring decisions.

TABLE 2

DISCONNECT BETWEEN CIO/CISO COMMUNITY AND HR PROFESSIONALS

CIO/CISOS/HIRING MANAGERS ■ COMPARED TO *HR MANAGERS* ■

	Dissatisfied or Very Dissatisfied		Neutral or Don't Know		Satisfied or Very Satisfied	
Quality of candidates	**33%**	*10%*	**26%**	*29%*	**40%**	*61%*
Number of qualified candidates who apply	**41%**	*34%*	**29%**	*21%*	**30%**	*45%*
Time to pass security clearance	**54%**	*46%*	**33%**	*29%*	**13%**	*25%*
Time to hire	**77%**	*52%*	**3%**	*10%*	**20%**	*38%*
Level of collaboration between HR and hiring managers	**38%**	*31%*	**26%**	*14%*	**36%**	*55%*

Source: March 2009 survey of CIOs, CISOs, hiring managers and HR managers. Partnership for Public Service and Booz Allen Hamilton.

"HR should be savvy with creating duties and qualifications, but managers often want something so specific that no one qualifies," said the HR official. "Managers need to be honest about what they are looking for and then use those factors to emphasize what they need."

And sometimes the process works. A CISO at a major department said he may be an exception, but he has not had a problem with HR. "When I have a vacancy, I meet with HR, go through a set of standard questions to find the ones I need and send them a draft of the job announcement. They review and send it back. There is a very quick turnaround."

While this anecdote shows that the system can work, overall we found a serious disconnect between HR professionals and line officials in many agencies. CIOs, CISOs and hiring managers are frustrated that the hiring process is inflexible, onerous, time-consuming and slow—in the end it does not even yield the quality and quantity of applicants they want. HR professionals feel they are serving their clients and meeting their needs, but also must carefully adhere to established rules and procedures to assure a fair and impartial process.

Agencies Frustrated with OPM

CIOs, CISOs and HR professionals were particularly dissatisfied with the working relationship they have with the Office of Personnel Management. The question in our survey was, "When it comes to identifying and recruiting qualified candidates for your cyber/information security positions, how satisfied are you with the level of collaboration between your organization and OPM?" Of the respondents, 41 percent of the CIOs/CISOs and 38 percent of HR managers reported being either dissatisfied or very dissatisfied at the level of collaboration with OPM.

Much of the dissatisfaction with OPM seems to stem from difficulties obtaining or using "direct hire authority" (DHA) for cybersecurity positions. In 2003, OPM provided government-wide direct hire authority for Information Technology Management (Information Security), GS-2210, GS-9 and higher jobs. DHA can be declared for jobs where there is documented to be a critical hiring need or severe shortage of candidates. Using this authority, an agency can hire without regard to competitive ratings and rankings, veterans' preference, and other procedures.

When HR professionals who responded to our survey were asked which hiring authorities worked well, many mentioned DHA, because it simplifies the competitive process. But some are dissatisfied with the scope of the direct hire guidelines and argue the authority is too limited.

Federal cybersecurity leaders are saying that major government departments need wider authorities to recruit and hire specialized cybersecurity talent. OPM has been asked by at least one CHCO to provide additional latitude in granting direct hire authority for information security jobs in the 2210 occupation series starting at the GS-7 level, and also to add more categories outside the 2210 series that are cybersecurity-related. These include classifications in computer science, electronic engineering, computer network forensics, computer defense and network attack.

This CHCO said that OPM's current cybersecurity-related policies and classifications are inadequate for today's fast-changing and sophisticated cybersecurity world. "These positions cannot be filled under existing competitive and excepted appointing authorities," he said. "These authorities require up-to-date OPM classification and qualification standards. However, as currently written, those standards do not address the competencies we require."

Agencies do not see OPM as helping them solve problems hiring cybersecurity talent, and some refer to OPM as part of the problem rather than the solution. Nonetheless, OPM must balance its responsibilities to protect the merit hiring process and assure compliance with hiring regulations (such as open competition and veterans' preference) with the need to help agencies find the talent they need. This is often a difficult balance.

"We recognize there are considerable challenges," said OPM's Angela Bailey about the frustrations agencies have with recruiting cybersecurity talent. "It is made even more difficult when the term 'cybersecurity' means different things to different leaders/agencies. A step in the right direction is to pull all of the interested parties together in one room and define cybersecurity."

RECOMMENDATIONS FOR AGENCIES
WHAT CAN BE DONE RIGHT NOW

Many of government's cybersecurity workforce challenges are systemic and can only be addressed with the support of the White House and Congress. But there are a number of things agencies with cybersecurity-related functions can do on their own right now.

The first step agencies should take is to focus on meeting their cybersecurity talent needs by putting someone in charge. Agencies should not wait for direction from the White House's new cybersecurity coordinator to take this step. This individual should be given adequate authority and resources to meet hiring goals and should be held accountable for achieving results.

This individual should be charged with leading an effort to hire, train and retain civil servants with technical expertise. In addition, agencies must invest adequate resources and personnel to manage cybersecurity talent, including contractors. That includes having people on staff with proven competence in monitoring contracts and overseeing the contractor workforce.

Our research identified a number of successful strategies individual agencies and private organizations are using to meet their cybersecurity talent needs, which should be shared and adopted.

Based on these best practices, we have developed a *Checklist for Cybersecurity Talent Management* (see Appendix).

We have also outlined a model for acquiring and managing talent. The Total Talent Management Model includes four phases:

1. **Sourcing and recruitment** focuses on locating talent to inspire the best potential candidates to consider working in federal service and encourage people to pursue the learning that can lead to a federal cybersecurity career.

2. **Job announcements** tell potential applicants what skills are needed and what the job entails; **marketing** gets that information to potential applicants in a persuasive and compelling way.

3. **A plan for selecting the right talent and closing the deal** after a candidate successfully completes the application includes ensuring that line managers and the human resources office are working together and helping candidates get through the tough security clearance requirements for cybersecurity positions.

4. **Onboarding and retention** are essential to minimize the time it takes new employees to reach full performance level and maximize the length of time high-performing cybersecurity talent stays at an agency.

TOTAL TALENT MANAGEMENT MODEL

SOURCING AND RECRUITMENT

As described earlier, many agencies use the SFS program as their primary entry-level recruitment tool, in large part because the SFS students are well-trained and easy to find, thanks to Web access to the students' résumés. Other agencies build long-term relationships with targeted universities, getting to know key faculty members and educating the campus community about job opportunities. Some even serve on curriculum advisory boards, helping influence the curriculum so graduates have the skills the agency needs.

Another important source of entry-level talent—and a great way to "test" the fit of potential future full-time employees—is through a formal internship program, which can become a pipeline for permanent positions.[12] Since the SFS program requires a federal summer internship, it is possible to dovetail the SFS requirement with federal internship programs: the Student Temporary Employment Program (STEP) and Student Career Experience Program (SCEP).[13] The Department of Justice uses STEP to identify potential candidates and begin the security clearance process for SFS students early so they can start working as permanent employees right after graduation.

Agencies use these student programs to bring on non-SFS students as well, such as students from Centers for Academic Excellence institutions. Others use the flexibilities inherent in SCEP, which allows them to non-competitively hire students after they graduate (by successfully completing a prescribed number of hours), often bringing them back for consecutive summers, building loyalty and skills that can directly contribute to the agency later.

Interns heading back to campus undoubtedly share their satisfaction or dissatisfaction with their internship experiences. The Partnership for Public Service's Federal Service Student Ambassadors program has been successful at helping agencies prepare interns to go back to their campuses and share experiences and broader information about federal jobs and internships with their peers.

Some agencies settle for hiring entry-level talent because new graduates are easier to find and recruit than mid- and senior-level talent. Many experienced people may not be actively looking for a new job. Agencies need to aggressively seek out these so-called passive candidates. Hence, proactive sourcing involves analyzing where the right sources of talent are and how to contact them.

For more experienced talent, agencies that simply post job announcements on USAJOBS.gov may not be successful. More proactive methods include publicizing job announcements in the contracting community, advertising on technology Web sites, encouraging employees to make referrals and approaching private-sector businesses facing layoffs to connect with employees who have key skills. Transfers from other government agencies are also a big source of new hires. Overall, if agencies do not have specific sourcing and recruiting strategies for hiring above the entry-level, this can be a hit or miss proposition.

We recommend that agencies adopt the following best practices for sourcing and recruitment:

- **Decide what skills, competencies and level of experience to target;**
- **Develop a thoughtful, creative recruiting plan;**
- **Identify a recruiting champion to take initiative and marshal resources in carrying out the plan;**
- **Reach outside ordinary channels to connect with passive candidates who might be interested even if they're not actively looking for a new position, or who know other candidates;**
- **Use Web sites and approaches in addition to USAJOBS.gov, such as social networking sites (Facebook, LinkedIn) and technology sites (dice.com, GovLoop.com);**
- **Build upon well-established relationships with potential sources of candidates (e.g., contractors, national associa-**

TABLE 3

UNIVERSITIES WITH THE MOST SFS GRADUATES FROM 2006-2009 (AS OF 1/30/09)

Institution	Total
University of Tulsa	53
Carnegie Mellon University	51
Naval Postgraduate School	27
North Carolina A&T	25
Syracuse University	25
New Mexico Tech	22
Mississippi State	21
Polytechnic University (Brooklyn, NY)	21
University of Nebraska	21
University of North Carolina	20
Other Universities	167
Totals	453

Source: National Science Foundation, SFS program data

12 *Leaving Talent on the Table: The Need to Capitalize on High Performing Student Interns*, Partnership for Public Service, April 2009

13 Agencies can convert a STEP to a SCEP position and use the hours towards non-competitive eligibility

tions, universities with certified information assurance programs) or establish new relationships with a commitment to sustain them; and

- **Create strong, collaborative relationships between HR and line/hiring managers.**

SOURCING AND RECRUITMENT
THE FEDERAL ENERGY REGULATORY COMMISSION

Recruitment Coordinator Alitza Vega has an innovative approach to getting potential cyber candidates to take a look at her small agency, the Federal Energy Regulatory Commission (FERC). FERC's college recruitment program has been very active over the past few years building relationships on campuses across the nation. By taking a proactive approach, FERC has been able to develop a pipeline of highly qualified applicants ready to fill cybersecurity positions at the Commission as the need arises.

For mid- and senior level talent, FERC has active hiring managers who network with industry professionals, seek out potential candidates for higher level positions and encourage them to apply to Commission vacancies.

"One challenge that agencies face is the differing objectives for cybersecurity professionals across the board," explained Vega. Because of unique needs, FERC is also collaborating with engineering programs at accredited universities to develop curricula specifically designed to educate students in the fields of power engineering and cybersecurity. "Our positions require competencies in the areas of power engineering and policy formulation in addition to cybersecurity. This multi-disciplinary focus is not the same for all agencies." FERC's approach illustrates the success an agency—even a small one—can achieve through innovation, perseverance and building lasting relationships.

MARKETING JOBS AND JOB ANNOUNCEMENTS

How can an agency convey in a clear and compelling way to potential applicants what the job is like and what skills are needed? And, how does an agency create a process that encourages qualified candidates to apply? If job announcements sound "bureaucratic," applicants might quickly decide not to apply. The job application is like the bait that can reel in the perfect catch, but it also has to help the hiring manager determine which applicants have the necessary skills. Applicants also want an agency to communicate with them throughout the process so they know where they stand.

Rarely do line managers and HR professionals work together to identify the best strategy for getting information about the job opening to potential candidates. Throughout our interviews, we found distinct undertones of discomfort about how HR and line managers collaborate or don't collaborate to develop job announcements.

We recommend that agencies adopt the following best practices for marketing jobs and creating job announcements:

- **Hold early meetings between line managers and HR to agree on the skill and competency needs for the positions to be filled;**
- **Create a good collaboration between HR and the line managers to develop a job announcement that clearly describes what the job is and assessment questions that specifically identify what skills and experience the hiring managers are seeking;**
- **Agree on how to get the word out about the job to potential applicants, and then divide up and jointly execute those tasks;**
- **Test the draft job application by asking a relatively new cybersecurity hire in the agency to pilot test the application and point out any obscure, confusing language or "government-ese";**
- **Establish a time shortly after the job is posted to review the applications to see if quality candidates are applying; if not, change the strategy or the announcement;**
- **Identify an individual to be on call to answer questions about the application process. This "go-to" person should walk candidates through the process, including connecting them with line managers who can answer questions about the job.**

MARKETING JOBS AND JOB ANNOUNCEMENTS
DEPARTMENT OF JUSTICE

At the CIO's office at the Department of Justice (DOJ), human resources personnel and hiring managers work closely to find cybersecurity talent, focusing on speeding up the time to hire, a particular problem reported in our survey and by focus group participants. Jason Walsh, a management and program analyst, explained that the team of human resource professionals within the CIO's office created a standard set of actions which are used in the hiring process. They identified 28 steps which they now use as a template to speed up the time it takes to fill a position. Walsh clarified that they don't use all 28 steps for every position, but just those needed.

To fill a position, the Director of Information Technology Security Staff / Deputy CIO, Kevin Deeley, and the CIO's Director of Human Capital Management and Analysis, Donna Hill, work together to craft a job announcement that clearly lays out the technical needs of the position. They follow a structured timeline to identify responsibilities for both HR and the hiring manager. Personnel analysts "have to give a weekly status update to managers on where they are in the chain, while constantly communicating with the cybersecurity candidate to advise of their status," Walsh explained. This provides a high level of accountability and a continued focus on decreasing the time to hire, thereby helping DOJ compete with other employers more renowned for cybersecurity work.

SELECTING TALENT AND CLOSING THE DEAL

How does an agency select the right talent from the pool of candidates and then get that candidate to say "yes"?

Communication and timeliness are big issues. Recently hired employees told us that applicants do not understand why it takes government so long to make hiring decisions, why they are not kept informed about the status of their applications or why they have such a hard time finding someone to answer questions. Bad experiences can reinforce stereotypes about slow and bureaucratic government, and can cause good people to go elsewhere as they accept other jobs or just drop out.

OPM's End-to-End Hiring Initiative lays out an 80-day model for the complete hiring process.[14] Using this model, agencies can successfully plan to speed up the decision process, getting approvals in advance for recruitment bonuses, using direct hire authorities, arranging interviews in an efficient way and expediting hiring by putting required paperwork online. Similar to helping candidates complete job applications, HR must clearly and continually communicate with candidates throughout the hiring process.

Once the job offer has been made, the compensation package can be a barrier. Entry-level candidates may have salary expectations that are out of reach. For mid- or senior-level employees, salary gaps may be even greater. Smart agencies are prepared to present a compensation package to the best candidates that provide attractive benefits and/or financial incentives to offset any salary gap. The package can include recruitment and relocation bonuses, student loan repayment[15] and professional development opportunities. Training opportunities can be especially attractive.

We recommend agencies adopt the following best practices for selecting the right talent and closing the deal:

- **Establish an efficient, timely selection process that meets OPM's 80-day hiring guidelines by examining and decreasing the number of steps in the hiring process;**
- **Devise an interview process that effectively screens and attracts candidates. Such a process should allow the candidate to meet the key people who will make the hiring decision, as well as other relatively new employees who can help motivate the candidate to say "yes" to the job offer;**
- **Identify a lead person for each interviewee who will help the candidate through the selection process, including answering questions about both the organization and the work. Especially for mid- and senior-level candidates, the lead person should work with the interviewee to identify what the candidate most values (financial or other incentives) and communicate to HR what the candidate's priorities and interests are, to help close the deal;**
- **Reach agreement in advance on the package of hiring incentives; and**
- **Collect data on the results and success of recruiting and hiring, tracking such metrics as the number of interns converted to permanent positions, the number of applicants received from target schools or from other targeted sources, acceptance rates from "first choice" candidates for each position, and the number of positions filled compared to the number of vacant positions.**

CLOSING THE DEAL
THE GOVERNMENT ACCOUNTABILITY OFFICE

GAO's line and HR staff work closely and successfully to attract candidates with needed skills. In addition to using Scholarship for Service students as a major source for entry-level talent, GAO has developed and nurtured relationships with a few carefully selected universities. An important part of GAO's hiring plan is its summer internship program, which provides a "trial" period for both students and the agency to see if the student would be a good fit when he or she graduates. In the fall, interns who have shown they are good performers can be offered a permanent position to begin when they graduate from college.

GAO incentives for entry-level employees include a two-year rotation program through the IT functions of the agency, a career path for the first two years, workplace flexibilities and financial incentives such as student loan repayment. Because GAO is not on the GS salary system and has a "banded" pay system instead, new hires can be paid according to their relevant experience. This can help reduce what might otherwise be deal-breaking pay differentials between GAO and private-sector companies.

Other aspects that make working at GAO attractive to entry-level and experienced candidates are mentoring programs, and training and certifications, especially important factors for cybersecurity talent. GAO also provides opportunities to work in its advanced "cyber lab," which features many state-of-the-art technologies. GAO tries to offer a "complete package" to close the deal with the talent it wants to hire.

14 Office of Personnel Management, http://www.opm.gov/publications/EndToEnd-HiringInitiative.pdf

15 This may be an underused financial incentive as only 219 out of more than 6,000 federal employees who received student loan repayments in 2007 were IT employees. Source: OPM's *Federal Student Loan Repayment Program Fiscal Year 2007* http://www.opm.gov/oca/pay/studentloan/html/FY2007StudentLoanRepaymentReport.pdf

ONBOARDING AND RETENTION

Good onboarding minimizes the time it takes for a new employee to reach "full performance level" and maximizes the time a high-performing employee stays with the agency.[16] New employees need to be welcomed into the agency and made to feel part of the team right away, but they also must receive training to succeed. If a new employee starts before the final security clearance is received, it is even more important that during the waiting period his or her work be meaningful. Research shows that a new employee decides in the first six months whether he or she has made a mistake in selecting his or her new job and whether to stay.

Too often, agencies think of onboarding simply as orientation during the first few days on the job. However, smart agencies build retention into their strategic workforce planning and understand that good onboarding helps drive high retention. These agencies tailor their generic onboarding programs to new cybersecurity hires. The most effective onboarding programs continue to provide support to new hires for up to a year after they start.

Another important incentive to retain cybersecurity professionals is training, especially as part of a career path. New hires told us that it was important to them to stay at the "top of the game" in the fast-moving cybersecurity field. On the other hand, employees report that all too often they find training spotty or not directed at skills they need to hone, and say they have to fight to get the okay for the time and the funding from supervisors to attend important conferences and training sessions.

We recommend that agencies adopt the following best practices for onboarding and successful retention:

- **Develop onboarding programs for all new employees, but also have special programs for new cybersecurity employees to acclimate them, introduce them to colleagues and immediately familiarize them with the agency's cybersecurity work;**
- **Implement training and development programs, including rotations to different parts of the agency that do cybersecurity work, to grow skills and knowledge, and include a career path with opportunities to earn appropriate certifications;**
- **Make new employees feel connected to the mission by using them in recruiting and outreach programs at universities and high schools;**
- **Identify financial and nonfinancial incentives to help retain employees, including student loan repayment and tuition reimbursement for continuing education; and**
- **Encourage networking across the agency's cybersecurity workforce (including field locations) to build loyalty and help create a framework where all cybersecurity resources can be mobilized if needed.**

16 *Getting On Board: A Model for Integrating and Engaging New Employees*, Partnership for Public Service and Booz Allen Hamilton, May 2008

RECOMMENDATIONS FOR THE ADMINISTRATION AND CONGRESS

Attracting, hiring, training, retaining and effectively managing cybersecurity talent is an increasingly high priority for the federal government as well as the private-sector. In addition to our recommendations for agencies in the previous section, we call for more systemic reforms at multiple levels. The new White House cybersecurity coordinator will naturally be the point person for these actions, bridging differences between agency CIOs and CISOs, the CIO Council, CHCOs, leaders in the intelligence community, central agencies (especially the Office of Personnel Management) and, in some instances, congressional leaders.

THE WHITE HOUSE CYBERSECURITY COORDINATOR SHOULD:

- **Develop a government-wide strategic blueprint** to acquire, train and retain the cybersecurity talent the federal government needs. The White House should work with OPM and both intelligence and non-intelligence agency leaders to develop and implement this plan. The plan should assess the current cybersecurity workforce and provide guidance on the appropriate roles for federal employees and for private contractors. It should include measures to gauge the "health" and capacity of the cybersecurity workforce going forward.
- **Enlist the support of the private sector and academic communities** in a nationwide effort to enhance America's pool of cybersecurity talent, similar to what was done during the space race. The shortage of IT expertise in America creates elevated risks not only for our federal government, but also the private sector, which protects our economic and communications infrastructure from cybersecurity threats as well. The White House should issue a nationwide "Call to Service" and lead public, private, academic and other communities in a nationwide effort to promote math, technology and science education, and develop and train more cybersecurity experts in America.
- **Devise new, up-to-date job classifications for cybersecurity functions in government and establish certification requirements** for each job category using the best practices in the commercial arena. The new classifications and requirements should be developed in conjunction with OPM and key government principals in the defense, intelligence and civilian information security fields.

OPM SHOULD:

- **Create a dedicated, high-level, high-priority team** to work with agencies to identify and remove barriers related to cybersecurity recruiting, hiring and retention. Through this workgroup, OPM should produce a government-wide talent management plan to identify enterprise-wide issues and solutions, including issues relating to the multi-sector cybersecurity workforce. This plan should also incorporate needs and strategies from agency talent management plans.
- **Fix the federal hiring process.** Fixing the federal hiring process will help agencies bring in needed cybersecurity talent and, indeed, improve all governmental hiring. OPM's End-to-End Hiring Initiative provides hiring process guidelines that are a step in the right direction, but much more work is needed to effect real change and to alter the public's perception that federal hiring is red tape-bound. Addressing hiring complexities specific to cybersecurity is essential, but other broad changes—such as those proposed in S. 736, the Federal Hiring Process Improvement Act of 2009—are key, too. The result should be a hiring process that is more timely, transparent and user-friendly—to both external applicants and internal cybersecurity leaders and hiring managers.
- **Resolve long-standing problems around classification, position descriptions and other "technical" HR matters that currently make posting and filling federal cybersecurity positions complex and/or difficult.** This includes updating materials and procedures to remove hiring barriers, standardizing positions, enabling career paths and supporting agency efforts to compete successfully with the private sector. Specifically, OPM should focus on resolving issues around the "2210 series."
- **Establish a clearinghouse and forums that will increase collaboration** and idea sharing among federal agencies around recruiting, hiring and training cybersecurity talent. OPM should enlist the support of the White House cybersecurity coordinator to help elevate the importance of these forums in the eyes of agency leaders.
- **Give agencies greater flexibility** in using direct hire authority, ability to expedite the recruitment and employment of top talent, and incentives to help compete against the private sector.
- **Work with the intelligence community and non-intelligence agencies to define a government-wide career path**

for federal cybersecurity specialists, starting at the entry-level. The career path should include interagency rotations. The process for defining a career path for cybersecurity should address the need for certifications and how they can be reliably awarded and assessed; where appropriate, this information should dovetail with classification standards and position descriptions.

- **Continue to seek ways to expedite the security clearance process**, including more efficient ways to submit information as well as clearance reciprocity across agencies.
- **Collect, analyze and use agency-specific data** on new hires and departing cybersecurity talent (e.g., exit interview data) to evaluate recruiting and hiring success, and to develop strategies to further improve and streamline recruiting, hiring, training and security clearances.
- **Expand the number of universities offering cyber/information assurance curricula** by engaging the private sector, foundations and agencies that jointly operate the Scholarship for Service (NSF, DHS, OPM), and NSA and DHS, which run university Centers for Academic Excellence programs.

CONGRESS SHOULD:

- **Provide significant funding to develop and keep federal cybersecurity talent knowledgeable at a "state of the art" level of readiness through training and development.** Require periodic reporting (if classified, with a version suitable for the public and the press) on the accomplishments and progress of training programs, including inter-agency collaboration in creating such programs.
- **Ensure adequate funding of successful programs that provide graduate and undergraduate scholarships in the cybersecurity field.** Existing programs at current funding levels are inadequate to build a sufficient pipeline of talent in cybersecurity. In particular, Congress should enact the Roosevelt Scholars Act,[17] which would provide scholarships in mission-critical fields in exchange for a service commitment and provide increased funding for the government-wide Scholarship for Service program and DOD's Information Assurance Scholarship program. Require annual reports on the success of these programs focusing on the number of students participating (including the number who convert to permanent positions), the characteristics and quality of the university-based programs, and retention of these graduates after completing their service requirements.
- **Provide oversight** by requiring the national cybersecurity coordinator and the director of OPM to report on progress meeting government-wide talent management plan goals, identifying and addressing cybersecurity talent human capital challenges, and successfully hiring and retaining needed cybersecurity talent. Priority information should include the nature and result of collaboration across intelligence and non-intelligence agencies and the results of those efforts, measured by effective hiring (e.g., expanded college/university level education and pipelines), high retention, effective training and high performance. In addition to highlighting numeric trends in cybersecurity talent hiring and retention, the report should specifically address progress made by OPM in solving the hiring problems faced by agencies, including information on updated classification systems, hiring authorities in use, decreases in time to hire, manager satisfaction with new hires and security clearance approvals. If any of this information is deemed to be classified, an unclassified version should be made available to the public and the press to maximize transparency and accountability.

17 *The Roosevelt Scholars Act* was introduced in the 110th Congress by Representatives David Price (D-NC) and Christopher Shays (R-CT). The *Roosevelt Scholars Act of 2009* will be introduced shortly in the House by Representative Price. Senator George Voinovich (R-OH) will be the lead sponsor in the Senate. For more information, please visit ourpublicservice.org/roosevelt.

"The federal government must develop a career field for cyberspace professionals, from initial entry all the way to SES. There are a few cyber scholarship opportunities available for college students, and we do a very poor job of managing their careers. . . . If we do not immediately address this problem, we will never be able to secure the federal government's networks."

Marcus H. Sachs, Director, SANS Internet Storm Center

Before the House Committee on Oversight and Government Reform, May 5, 2009

APPENDIX A
SELF-ASSESSMENT CHECKLIST FOR CYBERSECURITY TALENT MANAGEMENT

Reviewer:	Date:

MAKING CYBERSECURITY A TOP PRIORITY	Not Yet	Started	Complete
Is cybersecurity noted as a priority in the agency's strategic workforce plan?			
Is there a clearly identified, knowledgeable and respected champion for cybersecurity at the agency who serves as the focal point around meeting cybersecurity human capital needs? Does he/she report regularly on results to the CIO or other designated leader?			
Does he/she have the support of agency top leaders—line as well as human capital? Does he/she have the authority and command of resources needed to achieve goals specified in the workforce plan?			
Does the agency's total talent management plan include learning from and collaborating with cybersecurity leaders in other agencies, bureaus, or departments? With appropriate private sector corporations and universities? Is the cybersecurity champion empowered to work with others to learn about best practices, align resources and collaborate to fulfill cybersecurity talent needs?			
Does the agency's strategic workforce plan for cybersecurity talent include contractors? Does the talent management plan include training staff properly to manage the contractor workforce?			
Has your agency developed a career path for cybersecurity talent? Does the career path address development and training as well as the knowledge and competencies needed for advancement?			

SOURCING AND RECRUITMENT	Not Yet	Started	Complete
Does your agency collect and use data to track the success of and make systemic changes to improve sourcing and recruitment?			
Do your HR and line cybersecurity staff work together to identify the best ways to find promising job candidates? Do they share responsibility for publicizing job openings? Are they creative about going out to possible candidates?			
Are your recruiters prepared to clearly and persuasively explain the agency's cybersecurity work and workforce needs to job candidates? Do your recruiters understand (and can therefore explain) the agency's total talent management plan for cybersecurity talent?			
Do your recruiters include experienced professionals who have hands-on knowledge about the agency's cybersecurity work and talent needs?			
Does your agency have dedicated HR professional(s) assigned to work with job candidates and applicants to help promising candidates work through the job application process? Who will really provide support?			
ENTRY-LEVEL			
Does the agency establish and maintain partnerships and in-depth relationships with selected universities that have cyber-related curricula or programs, such as the Centers for Academic Excellence? Does your agency use the Scholarship for Service program? If not, why not?			
Does your agency have an internship program as a centerpiece of its entry-level recruiting? As part of your internship programs, do you have a student ambassadors program for student-led recruiting on campus after internships?			
Working with professors at target universities, do you program work, projects, provide mentoring, etc. with students to develop sustainable "pipelines" for federal cybersecurity jobs?			
Do you use new hires, alumni and former interns for on-campus recruiting?			
Does your agency use social networking Web sites, such as Facebook or LinkedIn, to connect with potential recruits?			
MID- AND SENIOR-LEVEL			
Does your agency actively seek referrals from current cybersecurity employees to identify possible job candidates?			

Do recruiters look for companies and organizations with employees/members with matching skill sets, including current contractors?			
Does the agency have a program partnering with private sector companies to recruit talent for "encore" careers?			

JOB ANNOUNCEMENTS AND MARKETING JOBS	Not Yet	Started	Complete
Do hiring managers and HR collaborate to create job announcements that are streamlined, user-friendly and intriguing to potential candidates? Do you rigorously excise "government speak" from announcements?			
Are you able to track and record the source (e.g. university, company) of applicants to measure recruiting and marketing results?			
Do job announcements sell candidates on the agency's total talent management plan for cybersecurity employees, including special programs such as rotational programs or professional development opportunities?			
Is there a friendly, easy-to-reach, knowledgeable HR contact for candidates who sees his/her job as helping candidates successfully navigate the application process? Is there a content specialist contact as well?			

SELECTING TALENT AND CLOSING THE DEAL	Not Yet	Started	Complete
Does your agency use data to track the reasons why applicants do and do not accept job offers to improve the success rate?			
Do hiring managers and HR collaborate to fully make available hiring incentives and to utilize compensation and benefits (e.g., relocation or hiring bonuses, tuition reimbursement, additional leave, telework where possible, flexible work schedules, etc.)?			
Does HR prepare packages to make offers quickly after interviews? Does HR prepare on-the-spot offers for exempted positions (e.g. direct hire, FCIP)?			
Is someone keeping in close communication with applicants during the process to assure they know the agency is still interested in them and to answer questions?			
Do you track time to hire specifically for cybersecurity positions and actively work towards achieving time goals? Do you keep applicants informed of where they stand in the application process?			
Do you track the length of time to get a security clearance? Do you actively work with applicants to expedite the security clearance time? Do you look for innovative ways to bring new hires on board to do productive work before the security clearance has been granted?			

ONBOARDING AND RETENTION	Not Yet	Started	Complete
How do you familiarize new hires about the agency's mission and goals? Are there onboarding activities and a program specifically for new cybersecurity employees during the first year of employment? Are new hires asked to evaluate and make suggestions for improving the onboarding program?			
Is your career path for cybersecurity professionals clearly laid out and fully implemented?			
Do you track the development of critical cybersecurity skill sets? Do you have a formal program for training and development to grow skills and keep cybersecurity employees at "state of the art" knowledge levels? Does this include working with cybersecurity components in other agencies?			
Does the agency offer rotations within different offices in the agency that are involved with cybersecurity functions to broaden the knowledge of and build working relationships between the agency's cybersecurity employees?			
Does your agency gather employee and supervisor feedback on ways to improve the engagement of the cybersecurity workforce?			
Do you have a mentoring program?			
Do you use financial retention bonuses and other incentives or rewards to keep the best talent?			
Do you track attrition, the reasons why cybersecurity employees leave the agency and where they go? Do you use this information to address problems in or improve agency operations?			

APPENDIX B
METHODOLOGY AND CONTRIBUTORS

METHODOLOGY

The Partnership for Public Service, supported by Booz Allen Hamilton, conducted this study from January through June 2009. The goals of the project were to review the "health" and capacity of the federal cybersecurity workforce, identify obstacles in recruiting, hiring and retaining cybersecurity talent, and determine effective strategies to overcome those obstacles. Findings and recommendations regarding the cybersecurity workforce were generated after an extensive review of literature, reports, news articles and congressional testimony, as well as information from federal officials involved in hiring cybersecurity employees. Sixty-nine officials from 18 departments/agencies/subcomponents participated in a survey about recruiting, hiring and retaining employees for cybersecurity positions. Recently hired cybersecurity professionals and agency human resources professionals were also interviewed in focus groups. Numerous subject matter experts within government and in the private sector were also consulted about the current state of the federal cybersecurity workforce and about agency initiatives to address hiring challenges. Although much effort was made to collect information that represented the perspectives of the major participants in the federal cybersecurity arena, we were not able to speak with all key players. For example, we did not have in-depth discussions with intelligence community cyber leaders (although we did speak with intelligence community human capital leaders) and did not speak with the individuals conducting the "60-day" review of federal cybersecurity for President Obama, which was ongoing during our work.

CONTRIBUTORS TO THIS REPORT

Partnership for Public Service

Bob Lavigna, Vice President for Research
Brooke Bohnet
Janelle Callahan
Bob Cohen
Sally Jaggar
Bevin Johnston
Josh Joseph
John Palguta
Leslie Ann Pearson
Erin Preston
Lamar Robertson
Eloise Salmon
Lara Shane
Max Stier

Booz Allen Hamilton

Abe Zwany, Vice President
Jeff Akin, Principal
Robin Palchus

APPENDIX C
PARTICIPANTS AND SURVEY RESPONDENTS

Congressional Budget Office
Jim Johnston
Chief Information Officer
Stephanie Ruiz
Deputy Assistant Director for Management, Business and Information Services

Corporation for National and Community Service
Raymond Limon
Chief Human Capital Officer

Court Services and Offender Supervision Agency
Bill Kirkendale
Chief Information Officer

Department of Defense
John Grimes
Chief Information Officer
Kennetha King-Marbury
Keystone Program Manager
Ken Rauch
Manager, Special Employment Programs

Department of Education
Harry Feely
Deputy Chief Information Officer, Federal Student Aid
Phillip Loranger
Acting Director, Information Assurance

Department of Energy
Carol Williams
Deputy Chief Information Security Officer
Jeanne Beard
Director, Office of Corporate Information and Services

Department of Homeland Security
Tom Cairns
Chief Human Capital Officer
Jeff Eisensmith
Deputy Chief Information Security Officer
Tiina Rodrigue
Chief Technology Officer, Chief Information Security Officer, Security Information Officer
Tameka Bullock
Management and Program Analyst
Christopher Chase
Headquarters Recruitment Program Manager
Maura Daly
Deputy Chief Learning Officer
Steven Friend
Information Security Systems Manager, Federal Law Enforcement Training Center
Erin Hayes
Deputy Director, Workforce Planning, Staffing Policy, Recruitment and Veterans Outreach
John H. Morrison, Jr.
Senior Policy and Project Analyst
Steven Novack
Director, Workforce Management Division
Brenda Oldfield
Director of Cyber Education & Workforce
Ian Pannell
Corporate Recruitment Program Manager
Paul Plasencia
Veterans Outreach Program Manager

Department of Housing and Urban Development
Joyce Little
Acting Chief Information Officer

Department of Interior
Steven Held
Larry Ruffin
Acting Chief Information Security Officer
Joan Tyler
Director, Division of Information Security & Privacy

Department of Justice
Vance Hitch
Chief Information Officer
Kevin Deeley
Deputy Chief Information Officer
Director, Information Technology Security Staff
Carrie Gilbert
Office of the Chief Information Officer
Deputy Director, Information Technology Security Staff
Peter Crichlow
Office of the Chief Information Officer
Information Technology Security Staff, IT Specialist (INFOSEC)
Donna Hill
Office of the Chief Information Officer
Director, Human Capital Management & Analysis
Jason Walsh
Office of the Chief Information Officer
Personnel Analyst, Human Capital Management & Analysis

Department of Transportation
Sherri Ellis
Information Assurance Team Lead

Department of the Treasury
Michael Duffy
Deputy Assistant Secretary/Chief Information Officer
Lawrence Gross
Associate Chief Information Officer
Rick Hastings
Deputy Chief Human Capital Officer
Edward Roback
Associate Chief Information Officer for Cyber Security

Federal Aviation Administration (Department of Transportation)
Michael Brown
Chief Information Security Officer

Federal Bureau of Investigation (Department of Justice)
Donald Packham
Executive Assistant Director, Human Resources Branch

Federal Energy Regulatory Commission
Matt Dale
Energy Industry Analyst (Cybersecurity)
Jerry Taylor
Senior Engineer
Alitza Vega
Recruitment Coordinator

Federal Maritime Commission
Hatsie Charboneau
Director of Human Resources

Garcia Strategies, LLC
Greg Garcia
President, Garcia Strategies, LLC
Former Assistant Secretary for Cyber Security & Communications, Department of Homeland Security

Government Accountability Office
Gregory Wilshusen
Director, Information Security Issues
Naba Barkakati
Chief Technologist
Barbara Sauter
Human Capital Consultant
Charles Vrabel
Assistant Director

General Services Administration
Kurt Garbars
Chief Information Security Officer

Internal Revenue Service (Department of the Treasury)
Robert Buggs
Human Capital Officer
Alfred Hollimon
Veterans and Special Emphasis Program Manager
Pamela Judy
Management/Program Analyst (HR for Cybersecurity)

Grant Thornton LLP
Norm Lorentz
Director, Global Public Sector

Lockheed Martin
Lee Holcomb
Director of the Center for Cyber Security

National Archives and Records Administration
Sandra Paul-Blanc
Deputy Chief Information Security Officer

Nuclear Regulatory Commission
Patrick Howard
Chief Information Security
Paul Ricketts
Senior Information Technology Security Officer

Office of the Director of National Intelligence
Ronald Sanders
Intelligence Community Chief Human Capital Officer
Elizabeth Kolmstetter
Intelligence Community Deputy Chief Human Capital Officer

Office of Management and Budget
Suzanne Lightman
Lead Information Policy Analyst

Office of Personnel Management
Janet Barnes
Chief Information Officer
Angela Bailey
Deputy Associate Director, Center for Talent and Capacity Policy

Overseas Private Investment Corporation
Antenette Williams
Talent Program Manager

SANS Institute
Allen Paller
Director of Research

Social Security Administration
John Smith
Chief Information Security Officer
Cindy Mayhle
Director of Information Security & Assurance
Merrily Davis
Systems IT Recruitment Manager

United States Mint (Department of the Treasury)
Rene Smeraglia
Chief Information Security Officer

United States Geological Survey
A. Wiser

Department of Veteran Affairs
Traci Hummer
Director of Talent Management Office
Lisea M. Johnson
Human Capital Planning Development and Outreach Office, Management Analyst

Scholarship for Service Program/Information Assurance Scholarship Program Alumni
Devin Cassidy
Alumnus of the Scholarship for Service Program
Alex Eisen
Alumnus of the Information Assurance Scholarship Program (Department of Defense)
Patrick Kelly
Alumnus of the Scholarship for Service Program
John LaGuardia
Alumnus of the Scholarship for Service Program (Department of Homeland Security)

PARTNERSHIP FOR PUBLIC SERVICE

1100 New York Avenue NW
Suite 1090 EAST
Washington DC 20005

202 775 9111 phone
202 775 8885 fax
ourpublicservice.org

Booz | Allen | Hamilton

13200 Woodland Park Road
Herndon VA 20171

703 984 1000 phone
boozallen.com