

Readying the Next Generation Cyber Workforce

Acquiring, Developing, and Retaining Cyber Professionals

Ready for what's next.

Booz | Allen | Hamilton



Table of Contents

A Disconnect Between Today's Cyber Demands and the Current Workforce	1
Shaping and Building Tomorrow's Cyber People	4
Case Study: Defining Cyber Roles for the Office of Personnel Management's CIO Council	5
Booz Allen's Cyber People Readiness Suite	7
Cyber People Competency Evaluation	7
Cyber People Planning	8
Cyber People Development	8
Cyber People Talent Management	9
Cyber People Advancement	9
Cyber People Leadership	10
Summary of Cybersecurity Talent Study	11
Conclusion	12
About Booz Allen	13
Principal Offices	Back Cover

A Disconnect Between Today's Cyber Demands and the Current Workforce

"It's the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox—seen and unseen—is something that we experience every day."

– President Barack Obama¹

Given today's highly interconnected global economy and multinational network infrastructure, effective cybersecurity is critical to the sustainable prosperity of the United States. As our nation conducts more business electronically year after year, our citizens, businesses, and government agencies potentially leave themselves vulnerable to an increasing amount of malicious behavior online. Cyber criminals stole approximately \$1 trillion worth of intellectual property from businesses worldwide. This statistic does not include the even more common costs from personal information theft that results in loss of customers. Moreover, the United States had the most malicious overall activity measured by Symantec in 2008 and 2009², thus demonstrating the need for our nation and citizenry to become more vigilant when it comes to cybersecurity.

To effectively secure the information that fuels both our national defense and our economic prosperity, we need to ensure that we have a highly trained and qualified cyber workforce at the ready. The cyber workforce is our nation's most valuable asset today and must remain a national priority in the years ahead if we expect to remain a cyberpower.

Describing the challenge presented by the cyber threat as "daunting" may be an understatement, as cyberattacks originate from multiple, evolving sources and infiltrate networks with increasingly complex, dynamic methods. Further dramatizing the effect of the threat is the volume of penetration attempts made to US private and public sector networks each month. Put together, the workforce requirements for fulfilling the mission need to be equally deep in their knowledge and dynamic in their deployment to stay ahead of the nation-states and actors (foreign and domestic) whose interests include fracturing the public trust and/or stealing critical information vital to the interests of the United States.

Army General Keith B. Alexander, the head of the US Cyber Command, estimates that cyber criminals probe the US Department of Defense networks and systems 250,000 times per hour, or approximately six million times a day.³

In order for the United States to maintain its leadership position in the global market and defend against increasingly aggressive and complex attacks, we must invest in people to drive cyber initiatives in government, finance, healthcare, technology, and more. Without the right skills to stabilize and capitalize on the opportunity presented by the cyber frontier, we stand to lose ground as a major global cyberpower.

¹ "Remarks by President on Securing Our Nation's Cyber Infrastructure", speech by President Obama, May 29, 2009.

² Symantec Corporation, *Symantec Internet Security Threat Report, Volume XV*, April 2010.

³ Brewin, Bob, "Cyberattack Estimate: 250K an Hour," *Nextgov.com*, June 3, 2010.

The United States must take a more concerted approach to seize the opportunities of being a cyberpower—a nation that strategically employs information and communications technologies to enable economic growth, empower society, and enhance security—while managing the ever-changing risks in this Digital Age. It is critical for the future of our economy, society, and national security. Our nation’s government and business leaders must take action in four vital areas: policy and governance, planning and operations, technology and research & development, and human capital. At Booz Allen, we are focusing our intelligence and vast experience in human capital management, or what we call *Cyber People Readiness*.

“We can’t do national security without considering the economic impact. The two are inextricably connected. The national strategy is part of that component.”

*– Howard Schmidt,
cybersecurity coordinator of
the Obama Administration⁴*

The key questions then become: Does the United States have the appropriate people to take advantage of new cyber opportunities and remain a cyberpower? Do human resource (HR) managers and hiring managers have the knowledge and tools to find the

right kind of cyber professionals? If our nation does not have immediate access to highly educated and qualified people, will that impact our economy and security 5, 10, or even 20 years down the road?

Currently, there is a disconnect between today’s cyber organizational demands and finding high-quality people to fill mission gaps. According to the “Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce” study conducted by Booz Allen with the Partnership for Public Service in 2009, 33 percent of chief information officers (CIOs), chief information security officers (CISOs), and hiring managers were unhappy with candidate quality.

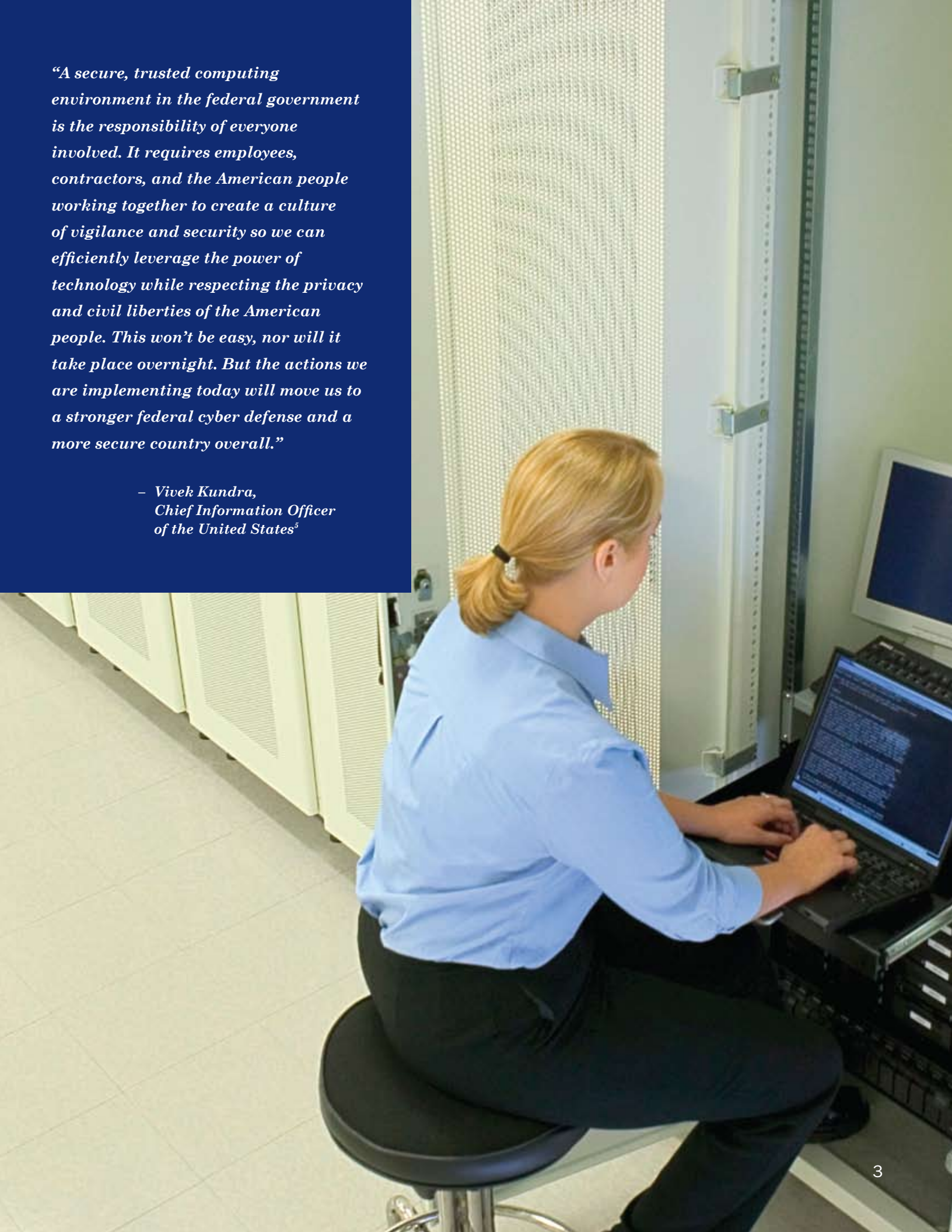
Consequently, because the United States cannot achieve cyber leadership without addressing “the people question” first, we must look at our workforce as a critical component to develop in tandem with advanced technologies, improved processes, and new/refreshed policies to produce and execute a truly effective national cybersecurity plan.

⁴Howard Schmidt, cybersecurity coordinator of the Obama Administration, speaking at the US Strategic Command Cyber Space Symposium in Omaha, NE, May 27, 2010.

⁵Vivek Kundra, Chief Information Officer of the United States, “Faster, Smarter Cybersecurity,” *Federal IT Dashboard Blog*, April 22, 2010.

“A secure, trusted computing environment in the federal government is the responsibility of everyone involved. It requires employees, contractors, and the American people working together to create a culture of vigilance and security so we can efficiently leverage the power of technology while respecting the privacy and civil liberties of the American people. This won’t be easy, nor will it take place overnight. But the actions we are implementing today will move us to a stronger federal cyber defense and a more secure country overall.”

*– Vivek Kundra,
Chief Information Officer
of the United States⁹*



Shaping and Building Tomorrow's Cyber People

More than ever, organizations, especially government agencies, need to plan for the future as significant numbers of our aging federal workforce plan for retirement over the next several years. With this mass exodus of federal personnel, as well as the need to fill new cyber roles, organizations will demand this new type of talent. The US Department of Labor, Bureau of Labor Statistics, *Occupational Outlook Handbook, 2010-2011 Edition*, estimates that the number of IT jobs will increase by more than 791,000 (approximately 17 percent) within the next 10 years⁶.

To meet this cyber talent demand, HR managers and hiring managers must begin cyber skills assessment and talent acquisition preparations today. As they continue to evolve their efforts to address their piece of the comprehensive cyber challenge, they should consider a number of critical questions, among them:

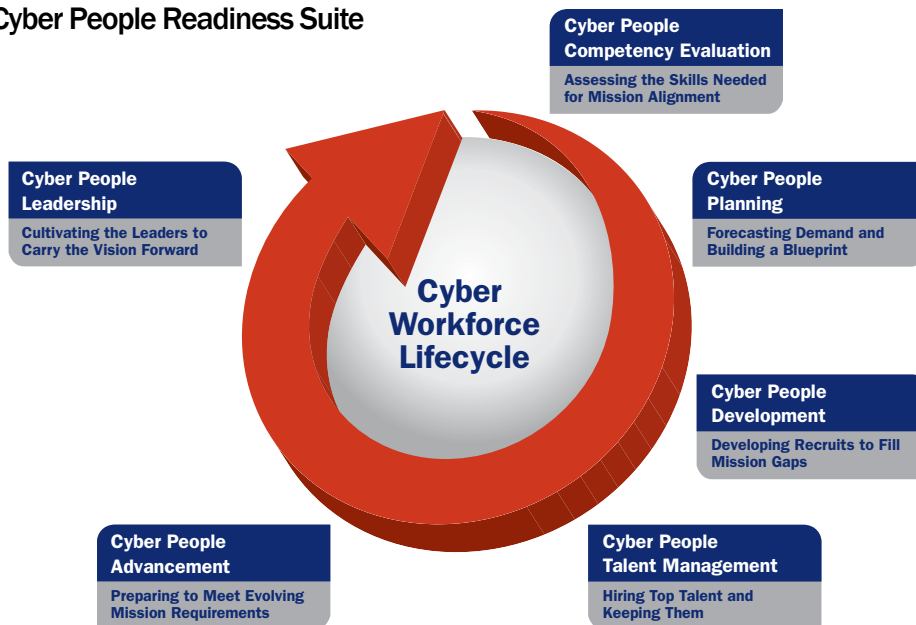
- What cyber skills does my organization need now and in the future, and what competencies are emphasized in cyber mission operations?
- Is our current supply of talent enough to meet my organization's cyber requirements?

- What should my cyber workforce look like and how does my organization build it?
- How does my organization recruit for cyber roles that continue to emerge and evolve and how can I fill these roles quickly and effectively?

And the list of questions goes on.

Booz Allen HR specialists have been asking themselves the very same questions since cyber became a part of our nation's vernacular earlier in this decade. Because Booz Allen has been engaged in defining cyber roles and competencies with government agencies like the Office of Personnel Management (OPM), Office of the Director of National Intelligence, and Department of Homeland Security, our firm is uniquely positioned and has the right building blocks and approach in place to help agencies acquire, develop, and retain cyber talent for the mission today, as well as to help them establish the right programs, processes, and protocols to create the cyber leaders of tomorrow.

Booz Allen's Cyber People Readiness Suite



⁶Chief Information Officers Council, *NetGeneration: Preparing for Change in the Federal Information Technology Workforce*, p. 25, April 2010.

Case Study: Defining Cyber Roles for the Office of Personnel Management's CIO Council

The Office of Personnel Management (OPM) CIO Council was established by an executive order in 1996 and then codified into law by Congress in the E-Government Act of 2002. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal government agency information resources. The council's role includes developing recommendations for IT management policies, procedures, and standards; identifying opportunities for sharing information resources; and assessing and addressing the needs of the federal government's IT workforce.

Council membership is comprised of CIOs and Deputy CIOs from federal executive agencies, such as the US Departments of Agriculture, Defense, Health and Human Services, Homeland Security, the National Science Foundation, the Social Security Administration, among others.

Additional members of the council include liaisons from the Chief Acquisition Officers Council, Chief Financial Officers Council, Chief Human Capital Officers Council, and other groups selected by the CIO Council's Executive Committee. The CIO Council serves as a focal point for coordinating challenges that cross agency boundaries. CIO Council Committees meet these challenges by producing documents and presentations through sustained efforts of subcommittees and working groups.

While OPM is responsible for defining job roles and skills across government agencies, currently, there is no standard definition of a Cyber CISO because skills, requirements, and even titles vary from agency

to agency. Numerous publications govern information security policies and standards within the federal government. It is challenging for information security professionals to synthesize and interpret available content in the context of department or agency information security practices and initiatives. Different perspectives exist on information security training standards and frameworks, key information security roles and role definitions, relevant competency models and skill sets, and the role that certifications play within the information security workforce. This has led to ambiguity and inconsistency in information security practices across the federal government.

The IT Workforce Committee, in partnership with the Information Security & Identity Management Committee (ISIMC), and Booz Allen worked together to develop a unified perspective on federal information security roles, functions, and responsibilities. Booz Allen and information security experts from across government identified and prioritized 11 unique IS roles. For a Cyber CISO, a set of Workforce Development Matrices were created to establish a common definition of the CISO role and identify critical job responsibilities, competencies and skills, certifications and credentials, and learning resources.

As a result, when the need arises to hire IS personnel in the cyber arena, OPM and federal agencies now have clearly defined cyber roles. The Workforce Development Matrices can be used to support various strategic human capital initiatives such as recruitment, staffing, career learning and development, performance management, and succession planning.



Booz Allen's Cyber People Readiness Suite

Booz Allen has the unique ability to build cyber talent and capacity in government, civil, and business organizations. Our experts have helped organizations define the skills and capabilities critical for successful job performance across cyber roles and functional areas of expertise, as well as behaviors that exemplify the progressive levels of proficiency associated with these skills. Defining, developing, and mapping these skills to cyber roles will enable businesses and government agencies to begin targeted recruitment, selection, and employee development initiatives.

Booz Allen's Cyber People Readiness Suite (see page 4) contains the modules necessary to get your workforce Cyber-ready by acquiring, developing, and retaining talent. Each of the six modules is interrelated, starting with defining roles and evaluating competencies and ending with the cultivation of true cyber leaders. Additionally, the modular services can be customized to meet the unique and complex needs of client missions. Our experience is that most clients have a solution already developed for many of these components, and that they may be interested in an external perspective that could improve the performance of one or more of them. Therefore, our solution is designed for that situation, allowing our clients to engage quickly and effectively to address any of the modules.

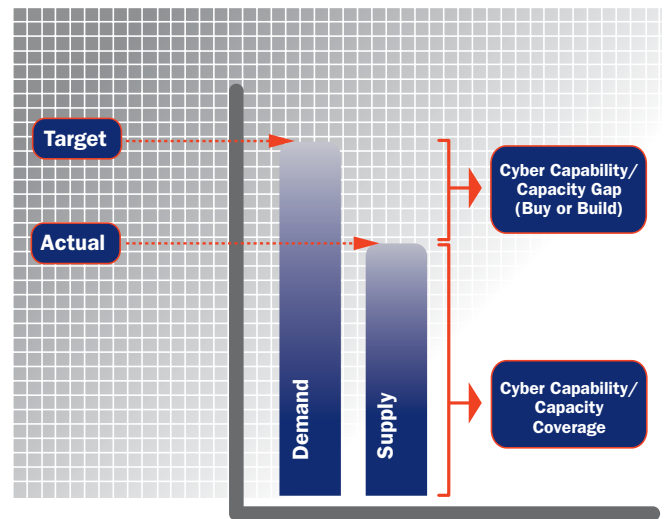
Cyber People Competency Evaluation Assessing the Skills Needed for Mission Alignment

Booz Allen's approach to strategic skills assessment is a critical first step in building Cyber People Readiness. Our human capital experts help organizations define the skills and capabilities that are required to meet the mission, including successful job performance across roles and functional areas of expertise, as well as behaviors that exemplify the progressive levels of proficiency associated with these skills. Defining and

developing these skills provides a solid foundation upon which targeted recruitment, selection, and employee development initiatives are designed to help hiring managers and HR professionals build talent and capacity within their organizations.

Booz Allen's skills assessment expertise stems from much of the work performed internally by its own cyber consultants. Based on our analysis and client experiences, we identified 23 critical cyber roles—ranging from intelligence analysts to network operations planning and software engineering—to accommodate the broad yet deep-level requirements of sophisticated missions and initiatives. We have leveraged this knowledge and employed it within our client environments, so they can meet the new cyber challenges.

Cyber Functional Skills Development



Booz Allen's Cyber People Readiness Suite

Cyber People Planning

Forecasting Demand and Building a Blueprint

Our approach to workforce planning provides organizations with the information needed to make proactive decisions around building a talented workforce that possesses the critical skills necessary to deliver on mission requirements at the organizational level. Booz Allen's workforce planning specialists have substantial experience in organizational transformation, human capital, business analysis, and strategic planning. Since the cyber mission—and the agencies, policies, protocols and processes associated with it—is incredibly dynamic, organizations need the ability to model their future workforce in an equally dynamic way. Booz Allen's planning service helps clients reconcile the strategic direction of their workforce capabilities and the workforce changes needed to perform their ever-evolving missions.



Cyber People Development

Developing Recruits to Fill Mission Gaps

This service allows hiring managers and HR professionals to find and leverage the right recruiting channels to establish a robust talent pipeline and fill the talent void within their organizations. Booz Allen can evaluate the balance of skills required to fulfill an agency's cyber mission requirements, and determine the best channels to cultivate the candidate flow required to meet those demands—today and in the future. Through market research, we help clients identify the best marketing/branding venues, social networking sites, professional associations, universities, and scholarship programs for tapping into talent needs. And, we can design and implement candidate screening processes to ensure hiring decisions are legally defensible and yield the highest quality candidates, given the agency's culture and occupational demands.

Cyber People Talent Management

Developing Top Talent and Keeping Them

The newness, complexity, and evolution of the cyber environment can make it difficult to chart career paths because HR and hiring managers are currently mapping out job roles in the cyber landscape as they develop in real time. However, career advancement opportunities play a significant role in attracting and retaining a capable workforce, so it is critical for organizations to create career paths for their talent. Organizations can optimize their career development programs by integrating training and development opportunities that facilitate continued career progression and target individual developmental needs.



Cyber People Advancement

Preparing to Meet Evolving Mission Requirements

Through recent engagements with cyber-related government agencies and organizations, Booz Allen consultants have learned that cyber professionals want more than a generic orientation developed for the first few days on the job. This workforce is expected to be groomed to meet tomorrow's demands and evolving mission requirements. Career development and training are key factors in where they decide to work. In addition to Booz Allen's Cyber University, the firm employs more than 1,400 professional staff in the training, education and performance support (TEPS) community, assisting a wide range of clients in all aspects of learning and education support services. Through these types of programs, our clients can rest assured that our knowledge of the latest tools, technologies, and cyber skills will help them meet current and future mission requirements.

Booz Allen's Cyber People Readiness Suite

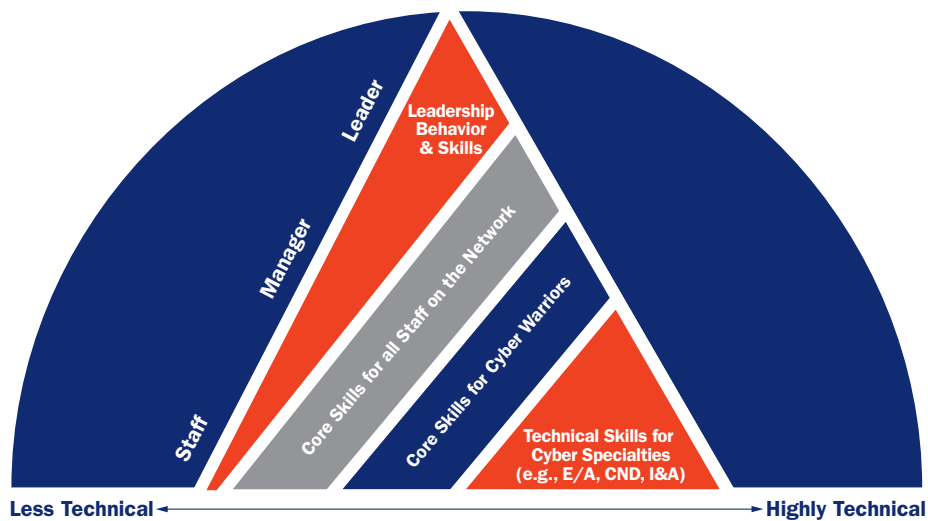
Cyber People Leadership

Cultivating the Leaders to Carry the Vision Forward

The cyber environment demands that organizations continue to cultivate strong leadership to face highly complex challenges and continuous change. Booz Allen's Cyber Leadership development approach is a framework that is anchored to an organization's mission, vision, values, goals, strategy, and culture, so that organizations can identify the right leaders, provide them with the right experience, advance them throughout the organization, and transform them through immersive learning and coaching support. Cyberpower involves organizational change on a scale that is unprecedented—the pressures on cyber leadership include an operating knowledge of cyber skills as well as exceptional dexterity in such skills as negotiations, cross-agency coordination and communication, international policy and law, and multicultural awareness. As such, it is imperative that we groom the visionaries in each organization who will help shepherd the cyber talent through the change required to meet current and future challenges.



Cyber Leader Career Trajectory



Summary of Cybersecurity Talent Study

In July 2009, Booz Allen conducted research with the Partnership for Public Service (PPS), titled “Cyber In-Security: Strengthening the Federal Cybersecurity Workforce” to learn more about our cybersecurity talent in government. While cyber touches much more than just government and security, we learned that our nation needs more cyber education and training initiatives to create cyber-savvy people.

This study, which surveyed chief information officers (CIOs), chief information security officers (CISOs), IT hiring managers and HR professionals across 18 federal agencies, found four major challenges that present a threat to identifying and hiring the quality and quantity of cyber people that organizations demand.

1. Our current pipeline of talent is inadequate to meet agency needs.
 - 60 percent of CIO/CISOs are unsatisfied with the quality of cyber applicants
 - 70 percent of the same group are unsatisfied with the quantity of cyber applicants
 - Demand for cyber talent is greater than what current program pipelines provide
2. Fragmentation of responsibility and funding hinders recruitment effectiveness.
 - There is no strategic government-wide assessment of the cyber workforce’s size, strengths, and weaknesses, or scope of the role being played by private contractors
 - Varying job definitions and a lack of consistency make it difficult to define scope or severity of the issue
 - Rather than cooperate, many agencies compete with each other for new talent
3. Complicated HR processes and rules hamper recruitment and retention efforts.
 - 77 percent of CIOs, CISOs, and IT managers are unsatisfied with the time it takes to hire someone
 - 54 percent of respondents are “dissatisfied” or “very dissatisfied” with delays caused by the security clearance process
 - Intelligence agencies have more flexibility than civilian agencies when hiring and setting compensation
4. A disconnect exists between HR and hiring managers.
 - 38 percent of CIOs, CISOs, and hiring managers and 31 percent of HR managers are unsatisfied with the current level of collaboration
 - Hiring managers suggest HR officials may lack specialization needed to identify qualified candidates
 - HR officials suggest hiring managers are not always aware of the rules, regulations, and procedures

The government hiring process is broken. Respondents to the survey characterized the government hiring process as inflexible, onerous, time-consuming, and slow. In some cases, HR contacts could not even track the status of job applications. And in the end, the process does not even yield the quality and quantity of applicants they want. To make matters worse, a perception among job applicants persists that salaries are better in the private sector. In fact, 51 percent of CIOs, CISOs, and hiring managers and 55 percent of HR managers are dissatisfied or very dissatisfied with their ability to compete with private sector for qualified candidates.

Download the entire study at www.boozallen.com/consulting-services/services_article/42415933

Conclusion

Through its proximity to the cyber environment and what is required to achieve true cyber readiness, Booz Allen uniquely understands the current state of cyber recruitment practices and the challenges confronting HR and hiring officials poised on the front lines of our nation's cyber defense. While very good practices already are employed in select pockets of the government and commercial sectors, significant opportunity for improvement remains.

While cyber is new to many HR professionals and hiring managers, government agencies and businesses should not feel overwhelmed by what is needed. Having Booz Allen as a partner in the staffing process will enable organizations to take action today to make an impact on their recruiting efforts and build a competent, cyber-ready workforce.

We have learned that government agencies and businesses need to think beyond traditional, prescribed processes to recruit their cyber talent. Sourcing and recruitment practices need to be viewed as a marketing and outreach program, not just a job posting to a Web site like USA Jobs. Recruiters also need to think beyond hiring, as onboarding, development, training, and retention

are critical to building for the future. Additionally, they need to consider how to create career paths, starting with entry-level positions through managers to the highest leadership levels.

For organizations that need assistance in selecting, grooming, and building a highly skilled cyber workforce, Booz Allen has the know-how and is ready to align with your mission. For decades, Booz Allen has helped organizations tackle complex, multidimensional challenges. In fact, it is what we do best. We understand what it will take to transform today's workforce into tomorrow's leaders.

A major challenge is envisioning what the cyber workforce will look like in the future, but we have learned a tremendous amount through our work with government officials and business executives. Booz Allen is at the forefront of what is required to build a comprehensive cyber workforce today and we are sharing our best practices with our clients worldwide. Our human capital consultants and services will meet the needs of any organization seeking to enhance its position in the current and future environment. Make sure your organization is Cyber People Ready by partnering with Booz Allen.

About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, the firm is a major provider of professional services primarily to US government agencies in the defense, security, and civil sectors, as well as to corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning strategy and organization, technology, operations, and analytics—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant’s problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm’s many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 23,000 people, and has annual revenues of approximately \$5 billion. *Fortune* has named Booz Allen one of its “100 Best Companies to Work For” for six consecutive years. *Working Mother* has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999. More information is available at www.boozallen.com.

To see how Booz Allen can help your cybersecurity workforce effort, please contact one of our consultants:

Jeff Akin

Principal
akin_jeffrey@bah.com
703/984-3753

Michael Parmentier

Principal
parmentier_michael@bah.com
703/984-0081

Roseann Ryba

Principal
ryba_roseann@bah.com
410/684-7819



Principal Offices

ALABAMA

Huntsville
256/922-2760

CALIFORNIA

Los Angeles
310/297-2100

San Diego
619/725-6500

San Francisco
415/391-1900

COLORADO

Colorado Springs
719/387-2000

Denver
303/694-4159

FLORIDA

Pensacola
850/469-8898

Sarasota
941/309-5390

Tampa
813/281-4900

GEORGIA

Atlanta
404/659-3600

HAWAII

Honolulu
808/545-6800

ILLINOIS

O'Fallon
618/622-2330

KANSAS

Leavenworth
913/682-5300

MARYLAND

Aberdeen
410/297-2500

Annapolis Junction
301/543-4400

Lexington Park
301/862-3110

Linthicum
410/684-6500

National Business Park
301/543-4400

Rockville
301/838-3600

NEBRASKA

Omaha
402/522-2800

NEW JERSEY

Eatontown
732/935-5100

NEW YORK

Rome
315/338-7750

OHIO

Dayton
937/781-2800

PENNSYLVANIA

Philadelphia
267/330-7900

SOUTH CAROLINA

Charleston
843/529-4800

TEXAS

Houston
281/280-5800

San Antonio
210/244-4200

VIRGINIA

Alexandria
703/822-8920

Arlington
703/526-2400

Chantilly
703/633-3100

Charlottesville
434/975-8100

Falls Church
703/845-3900

Herndon
703/984-1000

McLean
703/902-5000

Norfolk
757/893-6100

Stafford
540/288-5000

WASHINGTON, DC

202/548-3061

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com by clicking the "Offices" link under "About Booz Allen."

Booz | Allen | Hamilton

delivering results that endure