

Acquiring the Right Talent for the Cyber Age

The Need for a Candidate Development Plan



by

Jeff Akin

akin_jeffrey@bah.com

Roseann Ryba

ryba_roseann@bah.com

Eric Vazquez

vazquez_eric@bah.com

Booz | Allen | Hamilton

delivering results that endure

Table of Contents

The Cyber Human Capital Challenge for Government 1

Creating a Candidate Development Plan..... 1

 Program—Knowing What to Look For 1

 Message—Knowing What to Say..... 2

 Channels—Knowing Where to Look..... 3

The Booz Allen Approach—Cyber People Ready 4

 Cyber People Competency Evaluation 4

 Cyber People Planning..... 4

 Cyber People Development..... 5

Conclusion..... 5

About the Authors 6

About Booz Allen 7

Principal Offices Back Cover

Acquiring the Right Talent for the Cyber Age

The Need for a Candidate Development Plan

The Cyber Human Capital Challenge for Government

The Cyber Age is here. The Internet has transformed the way individuals, businesses, and governments interact. Networks, computers, software, and mobile devices are allowing information exchange that was never possible before, and this new communications infrastructure holds incredible promise for all aspects of society. Digital health, smart energy grids, e-commerce, and Gov 2.0 are all visions of the Cyber revolution, and in order to maximize the benefits of this incredible technology transformation, organizations need people with new sets of digital competencies, and new ways of thinking about security. This is particularly true in the federal government, where both cybersecurity and cyber enablement will have an enormous impact on national security and economic stability. For the United States to maintain its position as a global leader, federal agencies will need to build workforces equipped with a range of emerging cyber skills.

Right now, the demand for that cyber talent is far exceeding supply. In 2009, Booz Allen collaborated with the Partnership for Public Service (PPS) on a research report titled, “Cyber In-Security: Strengthening the Federal Cybersecurity Workforce.” The study revealed that federal IT leaders and HR managers need an influx of cyber talent to meet agency missions, but are unhappy with the quantity and quality of current applicants. Recruiting efforts are plagued by a lack of consistency in job descriptions, poor incentive structures, an overly complex hiring process, and confusion surrounding necessary skill requirements. These challenges are preventing the federal government from competing with the private sector for top technology professionals, and the talent gap poses a serious threat to America’s position as a global power.

“...public service should be a career of choice for the most talented Americans. Yet the complexity and inefficiency of today’s Federal hiring process deters many highly qualified individuals from seeking and obtaining jobs in the Federal Government.”

— President Obama¹

Federal recruiting and hiring processes are broken, but acquiring cyber talent isn’t simply a process problem. Agencies can improve position descriptions and use competency models to better screen applicants, yet that still won’t get to the root of the challenge. To bring the right cyber professionals into the federal government, every agency needs a comprehensive candidate development plan.

A candidate development plan starts with a clearly defined value proposition. What can your agency offer prospective candidates? What types of opportunities are cyber professionals seeking? Are you aligning your career opportunities to the values of the talent pool? The federal government has much to offer future cyber leaders, but agencies must develop compelling messages delivered through channels that reach the best candidates. A good candidate development plan consists of three essential components:

- **Program**—Knowing what to look for
- **Message**—Knowing what to say
- **Channels**—Knowing where to look

Creating a Candidate Development Plan

Program—Knowing what to look for

Identifying the right talent starts with an organizational assessment that defines the skills needed to meet

¹ Presidential Memorandum – *Improving the Federal Recruitment and Hiring Process*, May 11, 2010, www.whitehouse.gov/the-press-office/2010/05/11/presidential-memorandum-improving-federal-recruitment-and-hiring-process

mission requirements. The Cyber Age demands some new technical competencies, as well as an evolution of existing talent. For example, computer forensics experts and network analysts are still extremely important, but their skills may need to be expanded or modified when deployed in the cyber context. The cybersecurity landscape is dynamic and has changed rapidly over the past 10 years. Organizations used to worry about a virus taking down their network; now invasive monitoring is a more pressing concern. The fear of network failure has been replaced by the fear of information theft, and agencies need personnel that have the knowledge and skills required to combat these emerging threats.

The need for secure, trusted systems will play a large role in shaping demand for cyber talent over the next decade. The US Department of Labor predicts that network systems analysts, data communications analysts, applications software engineers, and systems software engineers will experience significant increases in job growth to meet cyber demands². Federal agency IT leaders will need to understand how these skills support their mission and create workforces with the right mix of complimentary technical talents.

Identifying the right cyber people goes beyond technology skills. Recruiting efforts must take into account other key attributes like leadership and diversity. Some of the biggest achievements and conflicts of the 21st century are going to have a cyber component, and federal agencies need technology leaders that are capable of strategic, big picture thinking. Identifying and evaluating leadership potential is an essential component of the cyber recruiting process because the next generation of technology leaders will be on the front lines, protecting our national security and economic stability.

Cyber threats are often faceless, but they are not without culture. To fully understand a threat, it helps to know where it came from. Governments and organizations from all over the world use a multitude of techniques to disrupt and monitor high-value information networks. To establish the best cyber

defense and response capabilities, federal agencies should strive to build diverse workforces representing a variety of cultures. Americans who have experience or extensive training in foreign cultures often have incredible knowledge and insight into the methods of cyber terrorists who originate from those regions. Tapping into the diversity of the United States holds extraordinary value for analysis and threat removal.

Message—Knowing what to say

Most of the cyber talent in today's workforce is coming from the "Net Generation,"³ or the 18- to 29-year-olds who have grown up around technology their entire lives. These young professionals view work slightly differently than previous generations. "Net-Geners" aren't interested in slowly working through the bureaucracy of large organizations. They tend to sample various occupations and move on quickly when they don't see clear-cut opportunities for professional development. In a recent survey conducted by the Gallup Organization for the Council on Excellence in Government, 52 percent of Net-Geners said the single most important factor in considering a job in government would be opportunities for growth and advancement.⁴ That's a powerful piece of data that federal agencies can use to their advantage when attracting top talent.

Young cyber professionals want to know how they will be developed over time. They want to see a plan for improving their skill sets and exposing them to experiences that enable upward advancement. Cyber professionals want to see career paths; government organizations must create them and communicate their benefits to potential hires.

Training is an important part of any career path, and the public sector is in a unique position to offer high quality training programs to cyber professionals. In the private sector, most entry-level training activities are directly attached to near-term financial ROI expectations. The government's expansive mission and responsibility set requires investment in cultivating talent over time to effectively marry cutting-edge

2-4 Federal Chief Information Officers Council, *NetGeneration: Preparing for Change in the Federal Information Technology Workforce*, www.cio.gov/Documents/NetGen%2Epdf, April 2010

technology skills with a progressively informed view of the historical threat patterns. Access to long-term, consistent training opportunities involving the latest cyber technologies is something that the government can deliver that many other organizations can't, and it's a crucial differentiator for federal IT leaders to emphasize when approaching cyber candidates.

Exposure to cutting-edge technologies and top technology training wasn't always something that the federal government could offer, but that's rapidly changing. The Obama Administration's emphasis on open government is making federal IT a new center of IT innovation. The push for increased transparency, accountability, and collaboration is exposing federal IT professionals to the latest innovations involving cloud computing, and it's also becoming a place where young technologists feel like they can affect positive change. According to recent research from nGenera Insight⁵ and the Council for Excellence in Government,⁶ one of the most important factors that young workers consider when job hunting is the desire to make a difference. This is particularly true when citizens are asked to serve by people whose opinions they respect—whether it be parents, teachers, peers, or elected officials. Federal IT is experiencing a positive perception shift, and it's something that federal agencies can incorporate into their communications to attract top cyber professionals.

Channels—Knowing where to look

Once an agency has identified the necessary cyber skills it needs, and determined its value proposition, it's time to find the talent. Some universities have developed cyber programs that produce candidates with a great foundation for a future in federal IT. The challenge is that every technology organization knows about these programs and the competition is fierce. To meet the cyber needs of the federal government, IT leaders and HR managers need to get creative. To locate cyber talent, agencies need information on the activities cyber professionals enjoy, and the forms of media they pay attention to.

The vast majority of talent in all disciplines is passive—they aren't aggressively looking for new employment. Because of this, it's important for federal agencies to brand themselves and create organizational awareness amongst passive audiences. Web sites are a great place to start. The Web is typically the first interaction candidates have with an organization, and this is particularly true of younger recruits. Effective sites have a clean visual look, strategic messaging, and the social media tools that tech-savvy people have come to expect from Web interaction.

Cyber professionals are like most people, except that they tend to understand technology on a deeper level and incorporate it regularly into their daily lives. Cyber specialists often enjoy activities like gaming, and they are typically early adopters of social media tools for connecting with friends and coworkers. Online communities and collaboration platforms are extremely important resources for reaching cyber talent, and platforms like Second Life, Facebook, Twitter, and LinkedIn have proven to be effective communications platforms. It's important for federal agencies to establish brand awareness and identity within these online talent pools, and online engagement shows that your organization values technology and implements it to improve communications, collaboration, and efficiency.

Offline communities, like universities and professional organizations, are still important recruiting resources. Targeted industry events can be fruitful if professionals attend because the content is timely and relevant, but to achieve broad talent acquisition goals, agencies must operate as their own recruiting mechanisms. The power of referrals, particularly within the cyber community, cannot be overstated. People want to hear about career opportunities from people they trust, and employees' networks of colleagues are extremely valuable talent pools to mine. Creating tangible incentives for current employees to bring external cyber talent into the agency is an effective first step.

⁵ Erickson, Tamara and Denis Hancock, *Engaging and Assessing Net Gen Talent: Approaches for Recruiting and Hiring the Right Net Gens* (nGenera Corporation, 2008), 8-9ut

⁶ The Council for Excellence in Government, *The Appeal of Public Service: Who...What...and How?*, May 2008, 4.

The Booz Allen Approach— Cyber People Ready

To help federal agencies acquire the cyber talent they need to meet mission requirements, Booz Allen Hamilton has developed a modular approach that details the steps involved in executing a strategic candidate development plan.

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.

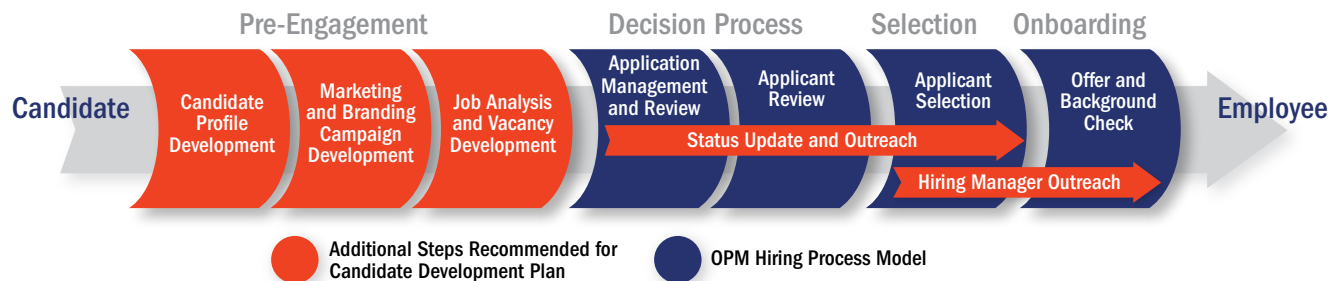
Booz Allen’s skills assessment expertise stems from much of the work performed internally by its own cyber consultants. Based on our analysis and client experiences, we identified 23 critical cyber roles—ranging from intelligence analysts to network operations planning and software engineering—to accommodate 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 new cyber challenges—faster and with greater effectiveness.

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

Exhibit 1 | Candidate Development Plan



Source: Booz Allen Hamilton

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 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 for cultivating 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. We can also 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.

Implementing a Candidate Development Plan Within the Traditional Hiring Process

Candidate development plans are designed to support traditional hiring procedures at key points in the

process. Many of these tactics need to be in place before the candidate engagement even starts—namely profile development, message development, and the creation of a targeted marketing plan. Exhibit 1 illustrates how agencies can design, develop, and implement a Candidate Development Plan around the US Office of Personnel Management (OPM) hiring model to dramatically improve the performance of the cyber talent acquisition process.

Conclusion

President Obama recently issued a memorandum entitled, “Improving the Federal Recruitment and Hiring Process” to address the “complexity and inefficiency” in today’s system. The administration’s recommendations are focused on quickly and efficiently pushing quality candidates through the federal hiring process. This is extremely important for attracting cyber professionals because without that process efficiency, other recruiting investments will be wasted as quality personnel are turned off by the overall experience.

By the same token, process efficiency upgrades will be wasted if agencies don’t invest in comprehensive candidate development plans. Moving personnel efficiently through a system that delivers the wrong messages to the wrong candidates won’t improve talent acquisition. Agencies need value propositions that speak to the next generation of IT leaders, because the governments that are successful in acquiring the top cyber talent will position themselves as the political and economic leaders of the Cyber Age.

About the Authors

Jeff Akin is a leader in the firm's Strategy & Organization business, and works with federal government agencies and Fortune 500 organizations to redefine their HR strategies, align people with business models, accelerate their paths to differentiated performance post-M&A/organizational restructuring, develop multi-year workforce models, and design and execute strategic candidate attraction/capture plans. As a recognized cyber workforce development thought leader, Jeff has briefed many government agencies in the US DoD, DHS, and Intelligence Community.

Roseann Ryba leads the firm's Strategy & Organization team in Central Maryland, primarily serving the Intelligence Community (IC). She is a skilled coach and facilitator, who has led strategic planning and team effectiveness workshops for public and private sector clients. Roseann earned a master's degree in Human Resource Development from the American University, and is on the Board of Directors for Leadership Anne Arundel, a volunteer organization dedicated to developing leaders in the community.

Eric Vazquez is the Strategic Recruiting Capability Lead for the firm's Human Capital Management team, and has 11 years of experience in many areas of strategic recruitment. Recent clients include the DHS, the MCRC, and the Naval Sea Systems Command, where he led the development and deployment of groundbreaking federal recruiting innovations that are being adopted across the US Navy. Eric is a seasoned presenter, and has served as Conference Chair at the Strategic Recruiting for Government Conference.

Contact Information:

Jeff Akin
Principal
akin_jeffrey@bah.com
703/984-3753

Roseann Ryba
Principal
ryba_roseann@bah.com
410/684-7819

Eric Vazquez
Senior Associate
vazquez_eric@bah.com
703/984-0149

About Booz Allen

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 learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Principal Offices

ALABAMA

Huntsville

CALIFORNIA

Los Angeles

San Diego

San Francisco

COLORADO

Colorado Springs

Denver

FLORIDA

Pensacola

Sarasota

Tampa

GEORGIA

Atlanta

HAWAII

Honolulu

KANSAS

Leavenworth

MARYLAND

Aberdeen

Annapolis Junction

Lexington Park

Linthicum

Rockville

NEBRASKA

Omaha

NEW JERSEY

Eatontown

NEW YORK

Rome

OHIO

Dayton

PENNSYLVANIA

Philadelphia

SOUTH CAROLINA

Charleston

TEXAS

Houston

San Antonio

VIRGINIA

Alexandria

Arlington

Chantilly

Charlottesville

Falls Church

Herndon

McLean

Norfolk

Stafford

WASHINGTON, DC

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."