Hiring and Managing a Cyber Security Workforce:

What Federal Managers Need to Know

Scott J. Cameron

September 19, 2013

A service-disabled Veteran-owned small business (SDVOSB)

www.r3consulting.com

Getting to Know Each Other

Raise your hand if:

- You work in **cyber security**
- You work in **human resources management**
- You **supervise** people
- You think it is **hard to hire** cyber staff
- You are **competing** with other agencies for staff

The Context

- The United States is facing unprecedented cyber security threats from abroad and domestically
- Cyber security expertise is in great and growing demand (12x the overall job market) across our economy
- Cyber security professionals are in great demand across government
- Current federal cyber security workforce is difficult to recruit and retain

Cyber Security Threats

Former Secretary of Defense Panetta, on 10/12/12, warned:

- “We are facing the threat of a new arena in warfare that could be every bit as destructive as 9/11”
- “The three potential adversaries out there that are developing the greatest capabilities are Russia, China, Iran.”
- “Out of a scale of 10, we’re probably 8 in cyber-war skills. But potential foes] are …probably…about a 3…but they’re beginning to move up.”

Cyber Security Threats

- Defense Secretary Hagel, on 1/30/13 said defending the country from cyber attacks should "involve the full range of tools at the disposal" of the U.S.
- U.S. should employ "any authorized military operations," as well as diplomacy and law enforcement.
- "Cyber threats are real, they're terribly dangerous," Hagel told reporters on 5/31/13.
- Cyber conflict could lead to "quiet, stealthy, insidious, dangerous outcomes," from taking down power grids to destroying financial systems or neutralizing defense networks.

Cyber Security Demand across society

- Annual US societal cyber spending was about $12 billion in 2012
- Demand is greatest in market sectors involved in:
  - Finance
  - Transportation
  - Utilities
  - Communications

Cyber security demand in government

- “I think we have to develop the ability to conduct counter-operations….So we have to have both defensive and offensive capabilities.” -- Former Secretary Panetta
- Civilian agencies also need cyber expertise to:
  - Protect customer and taxpayer information
  - Protect employee information
  - Protect mission capability
  - Comply with OMB requirements
- DHS given cyber security lead for the federal government by OMB in July 2010

DHS Advisory Council Task Force on Cyber Skills

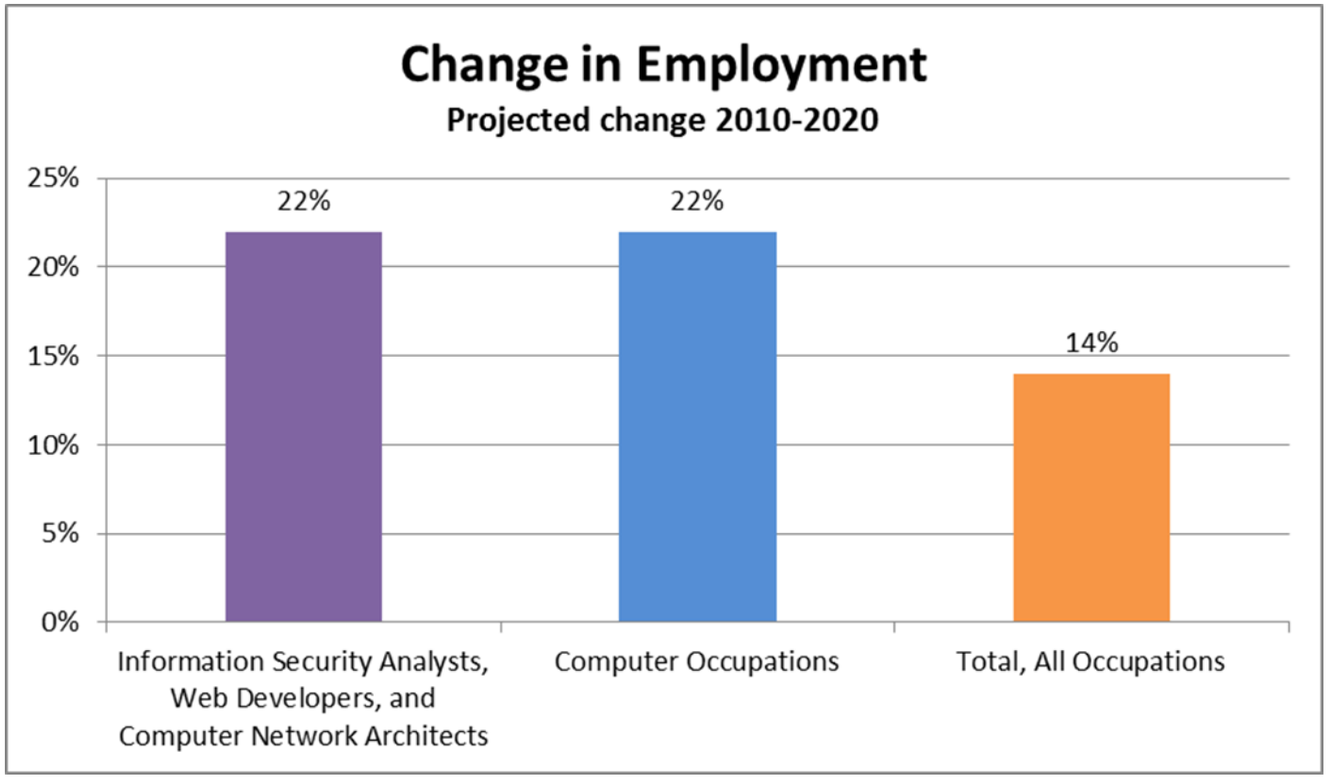
- Adopt an authoritative **list of mission-critical cyber security jobs**, and modify that list in the face of changing threats and technologies.
- Develop training scenarios that allow DHS to **properly evaluate cyber security talent** for each of the mission-critical tasks.
- Adopt a sustainable **model** for assessing the competency and progress of existing and future **cyber security talent**.
- **Establish a department-level infrastructure** that oversees the development of the cyber security workforce.
- **Streamline the hiring process** and make government cyber security jobs more enticing by emphasizing service, skills and growth potential.
- **Establish a two-year, community-college-based program** that identifies and trains large numbers of students for cyber security jobs.

DHS Advisory Council Task Force on Cyber Skills

- **Raise the eligibility criteria** for schools that participate in the Centers for Academic Excellence and Scholarship for Service programs to ensure that graduates are better prepared
- Launch a major initiative to **enhance the opportunities for U.S. veterans** to be trained for and hired in cyber security jobs.
- Use DHS direct hiring authority to **bring on at least 600 workers** with critical cyber skills.
- **Specify the skills and level of proficiency** needed in all cybersecurity-related contracting.
- Establish a pilot DHS **CyberReserve** program that ensures former DHS cyber security workers and others from outside of government are known and available in times of need.

Federal Cyber workforce challenges

- **Competing with the private sector** for talent
- **Bidding wars** against other federal agencies for talent
- **Hiring people quickly** to address a present, growing, and rapidly evolving threat
- **Hiring people smartly** to minimize internal threats (e.g.: Private Manning)
- **Effectively managing contractors** with access to sensitive information (e.g.: Edward Snowden)
- **Managing attrition**



Source U.S. Bureau of Labor Statistics, Employment Projections program

Competing with the private sector for talent

- **Sell the mission!**
  - Protecting the US nuclear arsenal or the New York City water supply is a lot more exciting than protecting Wells Fargo executives
  - Where else can you go head-to-head against the smartest people in rival countries without being in physical danger?
- **Sell the experience!**
  - After a few years, you will be wanted everywhere in the private sector
- **Leverage private sector contractors as appropriate**
  - Access to solid talent relatively quickly
  - Just because they are not your employees doesn't mean they are not your cybersecurity responsibility

Competing with other federal agencies

- **Work together** to grow the pool of applicants
- **Develop your own talent pipeline** so graduates are predisposed to come to your agency
- **Play the game:**
  - Direct Hire Authority
  - Hiring bonuses
  - Student loan forgiveness
  - Retention bonuses
  - Career ladders
  - Intellectual challenge
  - Recognition

One Valuable Applicant Pool: Veterans

- **Fast:** Non-competitive hiring authorities
- **Smart:**
  - Already passed basic security clearance
  - Public service orientation
  - VA pays for training through GI Bill
  - Already well trained by DOD
- **Compliance:**
  - Statutory requirements to promote veteran hiring
  - Executive Order requirements to promote veteran hiring

Managing Attrition

- ☑ **Onboarding practices**
- ☑ **Supervisory skills**
- ☑ **Invest in employees** (time, effort, money)
- ☑ **Do succession planning**
- ☑ **Use retired annuitants**
- ☑ **Use phased retirement** for knowledge transfer (new law, & OPM implementing regulations in process as of August 2013)

Questions?

Scott J. Cameron

Senior Vice President

R3 Government Solutions

scameron@r3consulting.com

(703) 348-7279