Cybersecurity Workforce Shortage

Janel M Nelson

Question to be answered

Is the United States on track to solve the cybersecurity manning issue?

Hypothesis: The government is not taking appropriate action

Topics of Discussion

- Examination of the issue
- Problem identification: past and current administrations
- Roles and responsibilities
- Synopsis of actions taken
- Analysis of actions
- Recommendations
- Conclusion

Examination of the Issue

- Breaches and shortages on the rise
  - 30,000 federal data security incidents in 2016
- Government perks aren't enough
  - Only 15% cybersecurity personnel would not consider leaving
  - Up to 18% non-active job seekers contacted daily
- U.S. at risk of losing advantage
  - China #1 producer of science/engineering undergraduates
    - 49% of all bachelor's degrees awarded in China vs 33% for the U.S
  - Global high-tech manufacturing - US:29%, China: 27%

Problem Identification: Past administrations

- 2000 National Plan for Information Systems Protection
- 2003 National Strategy to Secure Cyberspace
- 2010 NICE established – framework released 2014
- 2015 Federal Cybersecurity Workforce Assessment Act passed
- 2016 Federal Cybersecurity Workforce Strategy

Problem Identification: current administration

Roles and Responsibilities

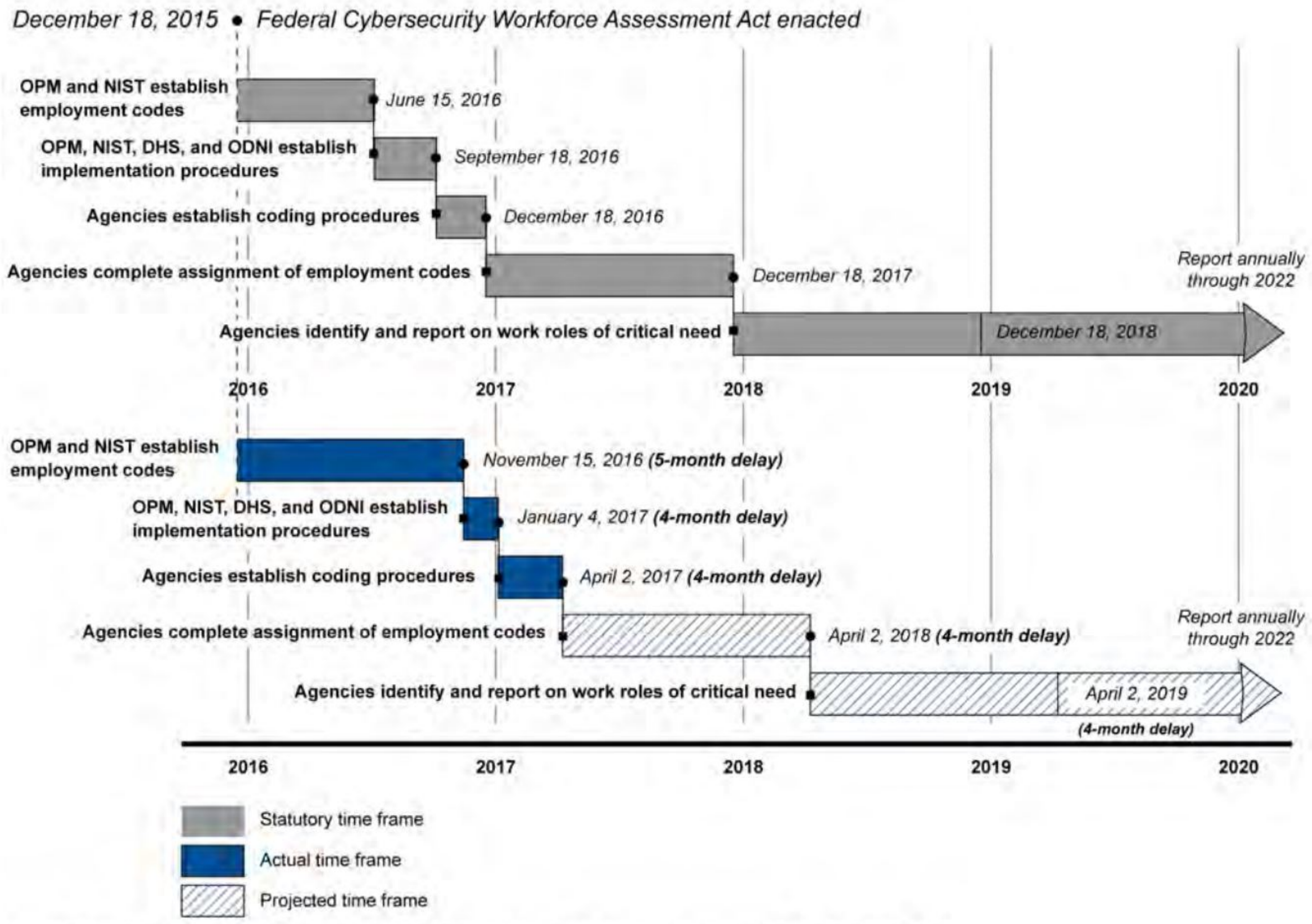
Agency	Role	Source
NIST	Develop framework for coding structures	Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines.
OPM	Develop a cybersecurity coding structure for human resource integration using the National Initiative for Cybersecurity Education (NICE) Framework	Federal Cybersecurity Workforce Assessment Act of 2015
All Federal Agencies	Use NICE Framework to code cybersecurity positions and find gaps	Jan 4th 2017 memorandum from OPM / Federal Cybersecurity Workforce Assessment

Synopsis of Actions

- **Workforce Assessment Act actions to date**
- **The National Initiative for Cybersecurity Careers and Studies (NICCS)**
- **CyberCorps®: Scholarship for Service (SFS)**
- **Center of Academic Excellence (CAE) designation**
- **Federal Tech/Cyber Hiring and Recruitment Events**
- **Direct Hire**
- **Compensation Flexibilities**
- **Reskilling federal employees**

Synopsis of Actions: Workforce Assessment Act

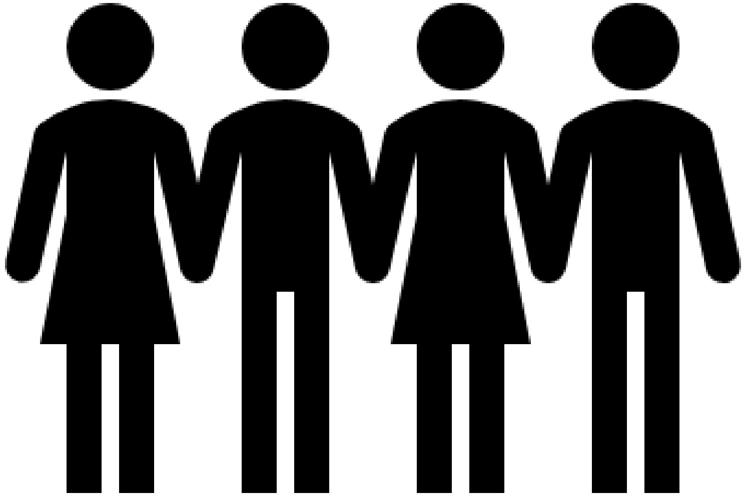
Figure 4: Prior Delays Resulting in Later Implementation of the Provisions of the Federal Cybersecurity Workforce Assessment Act of 2015, as of March 2018



Source: GAO analysis of NIST and OPM information and of the Federal Cybersecurity Workforce Assessment Act of 2015 | GAO-18-466

Analysis of Actions

- Adherence to NICE Framework
  - Coding and baselining: 21/24 complete as of June 2018
- Recruiting
  - Tech Fairs-dHS hired 700 through job fairs, first federal hiring event in Nov 2017
  - Student engagement: 1300 students from 122 academic institutions
- Scholarship/grant programs
  - CyberCorps®: SFS: $70M spent in 2017
  - IASP:Funding alloted for <100 student scholarships ($5M funds ~40 students)
- Government cybersecuity spending
  - Rising since 2017 with exception of R&D
- Government bonuses and hiring incentives
  - $3.4 billion in fiscal year 2015 on special and incentive pays
  - Less than 6% of employees received special payments
- Direct Hire: May hiring event by USCC yielded 70 on-the-spot interviews with 18 hires
- Reskilling pilot outcome?



What does it take to hire and retain cybersecurity professionals?

"A higher calling will basically supersede the attractiveness of compensation in the commercial sector" -- Maj. Gen Patrick C. Higby

How does Israel address the issue?

- 250 cybersecurity companies over $3 billion in annual revenues, ~ 5% of global market

- Cybersecurity education starts in middle school. Israel is the only country with cybersecurity elective in high school matriculation exams

- Recruits engineers/programmers to teach and helps volunteer teachers get jobs in IT companies

- Federal investment in 5 academic research centers of $75-100 million

Recommendations

- **Recommendation 1: Build talent through secondary education**
  - **Training for technical trades a norm**
  - **IT on equal footing with math, science, and English**

- **Recommendation 2: Build talent through primary educational**
  - **IT courses in grade school**

- **Recommendation 3: Foster cadre of IT teachers**
  - **Entice members leaving service and industry**

- **Recommendation 4: Grow post-secondary cybersecurity education degree interest**
  - **More funding for cyber education**
  - **Make a national calling**
  - **Centralized and well-maintained application process**

- **Recommendation 5: Emply government accountability and measures of effectiveness**
  - **Framework for evaluation and assessment of education similar to Israel**
  - **Task agencies for significant action and enforce deadlines**

Final thoughts……

School core curriculum adopted in 1893

Bill Gates quote on education staying status quo:

"We're kind of spoiled by being a leading country in the world. We'll have to get used to giving that up–if you're not training your workforce, you certainly don't have the most vibrant economy and you won't be able to afford a military that's stronger than all other countries' put together. In the long run, your human capital is your main base of competition. Your leading indicator of where you're going to be 20 years from now is how well you're doing in your education system." (Kamenetz, 2013, para. 8)

Recap

- Cybersecurity manning shortfall – issue for decade+
- Roles and responsibilities: NIST, OPM, all agencies
- Synopsis and analysis of actions: NICE, hiring flexibilities, scholarships/grants, spending, and recruiting
- Recommendations
- Conclusion

Questions?