Delivering Government Solutions in the 21st Century
Reform Plan and Reorganization Recommendations
Solving the Federal Cybersecurity Workforce Shortage

Department of Homeland Security and the Office of Management and Budget

Summary of Proposal: The Federal Government struggles to recruit and retain cybersecurity professionals due to a shortage of talent along with growing demand for these employees across the public and private sectors. The Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), working in coordination with all Federal departments and agencies, will establish a unified cyber workforce capability across the civilian enterprise. This Administration will work towards a standardized approach to Federal cybersecurity personnel, ensuring Government-wide visibility into talent gaps, as well as unified solutions to fill those gaps in a timely and prioritized manner.

THE CHALLENGE

The Federal Government struggles to recruit and retain cybersecurity professionals due to a shortage of talent along with growing demand for those employees across the public and private sectors. The workforce shortage compounds the Government’s challenges in responding to a constantly evolving threat environment and achieving its many IT-dependent missions.

In the past, each Federal department and agency was responsible for addressing its own cybersecurity workforce gaps independently, which has led to disaggregated and redundant Federal programs. As a result, the Government lacks a comprehensive, risk-derived understanding of which cybersecurity skillsets the Federal enterprise needs to develop and which positions are most critical to fill.

Moreover, the manner in which departments and agencies recruit, hire, train, retain, and compensate cybersecurity personnel varies by agency. This uneven approach has created internal competition for talent, which in turn creates disparities and discontinuities that degrade agencies’ ability to defend networks from malicious actors and respond to cyber incidents. A unified approach to attracting and retaining cybersecurity talent within the Federal Government would better support the Government’s cybersecurity enterprise.

Finally, there have not been continuous, strategic investments made in U.S. education programs to strengthen a pipeline for future cybersecurity talent. The abundance of redundant Federal programs focused on strengthening cybersecurity education illustrates how the Government’s role building the cybersecurity talent pipeline remains ill-defined.

THE OPPORTUNITY

This Administration can strengthen Federal cybersecurity and improve agencies’ ability to carry out their missions by identifying and closing workforce gaps in the near term, and can ensure long-term viability by building the cybersecurity talent pipeline.
WHAT WE’RE PROPOSING AND WHY IT’S THE RIGHT THING TO DO

To improve recruitment and retention of highly qualified cybersecurity professionals to the Federal Government, this Administration will develop a standardized approach to identifying, hiring, developing, and retaining a talented cybersecurity workforce in a timely and prioritized manner.

In the near term, this Administration will prioritize and accelerate on-going efforts to reform the way that the Federal Government recruits, evaluates, selects, pays, and places cyber talent across the enterprise.

Taking Stock of the Current Cybersecurity Workforce and Identifying Gaps

Human Capital personnel from across the Executive Branch are currently working with the Office of Personnel Management (OPM) to categorize the Federal cybersecurity workforce, using the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework, as required by the Cybersecurity Workforce Assessment Act of 2015). By Fall 2018, the Federal Government will have catalogued the entire cybersecurity workforce to better understand our current set of knowledge, skills, abilities, and identify any gaps; this catalog will give us Government-wide insight into where our most pressing needs are, and, for the first time, enable the development of an enterprise-wide approach to the recruitment, placement, and training of cybersecurity talent.

Using the NICE Framework analysis, the Federal Government will be able to determine which workforce gaps are most critical to address the current cybersecurity threat landscape. DHS, as the lead agency for the protection of Federal IT networks, is best positioned to drive this prioritization with Federal agencies and OMB. By the first quarter of Fiscal Year (FY) 2019, all CFO Act agencies, in coordination with DHS and OMB, will develop a list of critical vacancies across their organizations. By the end of FY 2019, all CFO and non-CFO Act agencies will have a prioritized list of critical vacancies. OMB and DHS will analyze these lists and work with OPM to develop a whole-of-government approach to identifying or recruiting new employees or reskilling existing employees in FY 2019.

Developing Innovative Recruitment, Retention, and Mobility Strategies

As agencies prioritize their cyber workforce needs, they will likely need to adopt innovative hiring techniques to ensure the best and brightest cyber talent can seamlessly enter the Federal Government. To address this challenge, the Department of Homeland Security received authority, through the 2014 Border Patrol Pay Reform Act, to modernize the traditional personnel system. With this new authority, DHS is working to create a new Federal hiring system called the Cyber Talent Management System (CTMS), exempting DHS from many of the requirements and restrictions in existing law under Title 5 for hiring and compensation of cybersecurity professionals. With an agile and innovative personnel system, DHS will be better equipped to compete for cyber talent with the private sector—speeding up the hiring process, attracting talent from non-traditional educational backgrounds, using innovative tools to assess applicants, and offering more flexible performance-based compensation. DHS will also be able to align prospective cybersecurity talent to the most pressing cybersecurity needs and will allow these technical professionals to accelerate their careers as rapidly as their aptitudes allow. In order to implement CTMS, by the first quarter of FY 2019 OMB, through its Office of Information and Regulatory Affairs (OIRA), will work with DHS to promulgate the necessary regulatory notices. By the end of FY 2019, DHS will work...
with OMB and all Federal agencies to measure the performance of CTMS and determine how to expand the system so that all departments and agencies can leverage it to address their personnel gaps.

One of the main hindrances to a seamless entry into the Federal Government is the security clearance process. The success of this initiative partly hinges on the success of the Government’s security clearance reform initiative, as discussed in a separate Executive Branch reorganization proposal in this Volume. In addition to the Government-wide security clearance solution, OMB, DHS, and OPM will work with agencies to review workforce characteristics to rationalize security clearance requirements in order to expedite the vetting and onboarding process.

The NICE Framework Federal workforce assessment is expected to confirm what has been known for some time: that cybersecurity employees’ skills and competencies vary across the Government. OMB will consult with DHS to standardize training for cybersecurity employees, and will work to develop an enterprise-wide training process for Government cybersecurity employees.

As part of creating a modern hiring and compensation system that rewards cyber expertise, the Executive Branch should also evaluate opportunities to make cybersecurity positions more mobile than traditional Government jobs. Flexibilities that allow workers to easily move from one position to another, or from one agency to another, would appeal to cyber talent in the agile and fast-paced cybersecurity industry. This mobility is also useful during a major cybersecurity incident, allowing agencies to surge capacity for incident response activities. OMB, in coordination with departments and agencies, will develop a work plan to implement this initiative by the end of FY 2018. Departments and agencies will begin to exercise these authorities by the end of FY 2019.

As an alternative or supplement to surge capacity, a mobile workforce will allow agencies to surge capacity for incident response activities. OMB, DHS, and DOD will evaluate what workforce gaps might exist that would be needed during a major Federal cybersecurity incident to determine the requirements for a Federal cybersecurity reservist program. As part of this analysis, OMB, DHS, and DOD will evaluate the existing authorities of Federal agencies to rapidly mobilize talent, including those of the U.S. Digital Service, which recruits talent from the private sector. These organizations will also evaluate the feasibility of extending a reservist program to support non-Federal major cybersecurity incidents within the United States, such as those affecting critical infrastructure. These programs will be coordinated with existing cyber services, including those in the National Guard.

**Reskilling Employees to Fill High-Value Cybersecurity Roles**

In addition to hiring new cybersecurity talent, the Government must look for opportunities to maximize the potential of its existing workforce. This includes efforts to reskill employees whose skills have become less relevant due to automation. OMB, DHS, and OPM will build aptitude and skills assessments to identify and select current Government staff who can be reskilled to fill critically-needed cybersecurity jobs. By reskilling the current workforce, agencies will be able to quickly shift its workforce into the highest-priority vacancy gaps. OMB and DHS will establish a job reskilling work plan by the first quarter of FY 2019. OMB and DHS will then update the CIO Council on a quarterly basis on the implementation of the reskilling work plan.
Building a Pipeline of Cybersecurity Talent

While solving the immediate needs of the Federal workforce is a major challenge, the Administration will also work to educate America’s youth to build an enduring cybersecurity talent pipeline. As part of the FY 2020 Budget development process, OMB will evaluate options to rationalize the size and scope of current Federal cybersecurity education programs, including the National Science Foundation (NSF)’s CyberCorps, the Scholarship for Service program, the National Security Agency (NSA)/DHS Centers for Academic Excellence program, NSF and NSA’s GenCyber Program, the Department of Labor’s apprenticeship program, DHS’s Cybersecurity Education and Training Assistance Program, the U.S. Army Cyber Center of Excellence, and the U.S. Navy Information Operations Command program, among others.

While the cybersecurity workforce shortage has been a known challenge for Federal agencies, no other Administration has taken a whole-of-Government approach to fixing it. OMB and DHS look forward to solving this major challenge through smart analysis and creative solutions.