Securing a Nation:

Improving Federal Cybersecurity Hiring in the United States

March 2021

burningglass TECHNOLOGIES

Table of Contents

1.	Introduction	pg 4
2.	Key Findings	pg 6
3.	Quantifying the Federal Cybersecurity Jobs Ecosystem	pg 10
4.	The Current Landscape of Federal Cybersecurity Hiring	pg 12
5.	Actions the Federal Government Can Take to Enhance its Cybersecurity Workforce	pg 19
6.	Resources & Acknowledgments	pg 25

1.

Introduction

In the 21st Century, there are perhaps no jobs more crucial to our national and personal security than those in cybersecurity. And nowhere are the perils of the cybersecurity talent shortage more severe than for the nation's most consequential cybersecurity employer: the federal government.

Already, there are myriad examples illustrating the consequences of insufficient federal cybersecurity defenses. The most recent federal breach to hit the headlines — the 2020 attack that targeted vulnerabilities in software from vendors such as Microsoft, SolarWinds, and VMware – was among the most devastating, and underscores the need for a strong federal cybersecurity workforce. This attack also gave increased urgency to the numerous legislative proposals and federal initiatives already underway to bolster the nation's cybersecurity posture.

Prior work has been done to document and address the key challenges and opportunities for the federal cybersecurity workforce. This includes the seminal report on the nation's cybersecurity landscape from the Cyberspace Solarium Commission that highlights actions legislators and policymakers may take to more effectively "recruit, develop, and retain cyber talent while acting to deepen the pool of candidates for cyber work in the federal government."[1] Much work has also been done to describe federal cybersecurity jobs using a consistent nomenclature and skills framework, including efforts to map federal jobs to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Moreover, in 2016 Burning Glass partnered with CompTIA and NICE to develop the website CyberSeek.org, which includes an interactive heatmap of supply and demand for cybersecurity jobs across the country, as well as a cybersecurity career pathway, to provide actionable data to the cybersecurity community across the United States.

However, further data about the specific needs of the federal cybersecurity workforce are needed to guide federal policymakers and hiring managers — data that historically have been in short supply. The goal of this research, therefore, is to both build upon prior efforts to understand the challenges and opportunities related to building the federal cybersecurity workforce, as well as leverage Burning Glass's database of more than one billion current and historical job records to provide new data on the federal cybersecurity workforce. Our hope is this will serve as an important step toward quantifying the magnitude of the challenges facing the federal cybersecurity workforce and support continued efforts to enhance the impact of potential solutions.

1 "United States of America Cyberspace Solarium Commission," King, Gallagher, 2020, www.solarium.gov.

2.

Key Findings

The federal government loses nearly one out of every five cybersecurity workers every year

The annual turnover rate for federal cybersecurity jobs is 18%, compared to the 14% turnover rate for other federal IT jobs. Moreover, of all workers hired into cybersecurity roles within the federal government over the past five years, 27% left the federal government within one year. Therefore, the federal government has a challenge retaining all cybersecurity workers, but retention problems are especially pronounced for new hires. This leaves many critical cybersecurity jobs unfilled and hinders the nation's ability to protect against cyber threats.

Overall federal cybersecurity salaries cannot keep up with more lucrative offers in the private sector, but entry-level salaries are comparable to private-sector salaries

On average, cybersecurity jobs in the private industry advertise salaries that are 23% higher than cybersecurity jobs in the federal government. This pay disparity creates a hurdle for recruiting top talent and increases the risk of workers leaving for higher salaries outside of the federal government. However, average federal entry-level cybersecurity salaries are within $2,500 of entry-level salaries in the private sector, suggesting that the federal government can effectively compete for workers who are starting their careers in cybersecurity and invest in strategies aimed at training and retaining them.

Federal cybersecurity jobs are less likely to demand the latest skills

Jobs requirements for private industry cybersecurity jobs are 87% more likely to request emerging skills — such as Cloud Security and DevOps — than federal cybersecurity jobs. This both reduces workers' capacity to defend against evolving threats, but also may discourage workers from applying for federal jobs if they want to keep their skills current.

The federal cybersecurity workforce is underemphasizing roles responsible for securing IT infrastructure

In the federal government, 27% of cybersecurity jobs fall in the Securely Provision category of the NICE Workforce

Framework, which is responsible for architecting secure IT infrastructure. By comparison, 61% of all cybersecurity jobs in the private sector are in the Securely Provision category. While this may be due to multiple factors, the stark contrast with the private sector suggests that the federal government is underemphasizing the roles necessary to build a secure digital infrastructure.

Federal cybersecurity jobs are nearly four times more likely to request a graduate degree compared to the private sector — but federal jobs pay considerably less

About 14% of federal cybersecurity job openings request a graduate degree, compared to only 4% of private cybersecurity jobs. Yet government pay for graduate degree holders isn't competitive. In fact, average federal salaries for graduate cybersecurity degree holders are $17,000 less than what private employers pay cyber workers with only a bachelor's degree. This constrains the talent pool from which the federal government can hire cybersecurity workers, and presents challenges attracting and retaining workers who can make significantly more money working in the private sector.

Yet the federal government is also dramatically more open than the private sector to hiring cybersecurity talent without a college degree. This is potentially a significant advantage, as the government's demand for cybersecurity workers is outstripping the collegiate talent pipeline

Some 46% of federal cybersecurity jobs are open to workers without a bachelor's degree. By contrast, eight in 10 private sector cybersecurity roles demand a bachelor's. That could give the government an edge in recruiting. In recent years, graduates from cybersecurity degree programs have grown 205%. While this growth is impressive, it is far outpaced by the 252% growth in demand for entry-level workers in core federal cybersecurity jobs. That's more than double the increase in demand in the private sector.

The federal government has multiple levers it can pull to expand its recruiting pipeline and enhance its cybersecurity workforce

If the federal government expands recruiting for core cybersecurity jobs — that is, the jobs solely focused on cybersecurity — to consider all workers in computer and math occupations, it can expand its available talent pool by over 3,130% while also tapping into a more diverse talent pool. Even if the federal government only focuses on hiring workers with any form of transferrable cybersecurity experience, it can still expand its recruiting pool for core cybersecurity workers by 267%. There are also multiple actions the federal government can take to modernize the skills of its workforce, improve retention and mobility with career pathways, and support the broader ecosystem of cybersecurity hiring and workforce development.

3.

Quantifying the Federal Cybersecurity Jobs Ecosystem

To research the federal cybersecurity hiring landscape, Burning Glass analyzed its database of over 1 billion historical job records and over 300 million career histories, as well as the Integrated Postsecondary Education Data System (IPEDS) data from the National Center for Education Statistics, to produce a dynamic picture of the current and future states of the cybersecurity workforce.

To isolate federal cybersecurity jobs, Burning Glass used its universal cybersecurity definition, which identifies job descriptions requiring skills, certifications, job titles, or occupations related to cybersecurity. Burning Glass also breaks the cybersecurity workforce into core cybersecurity jobs which are focused primarily on cybersecurity — such as information security analysts — and cyber-enabled jobs which have additional responsibilities in addition to cybersecurity — such as network administrators. Federal postings were then isolated by identifying a list of 165 employer names, which map back to federal U.S. government departments.

Burning Glass also mapped cybersecurity jobs to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework by reviewing the tasks, knowledge, skills, and abilities associated with each work role in the framework and mapping them to the closest corresponding skills, job titles, job posting keywords, and certifications captured in Burning Glass's database. In some cases, multiple NICE work roles can be mapped to one job opening.

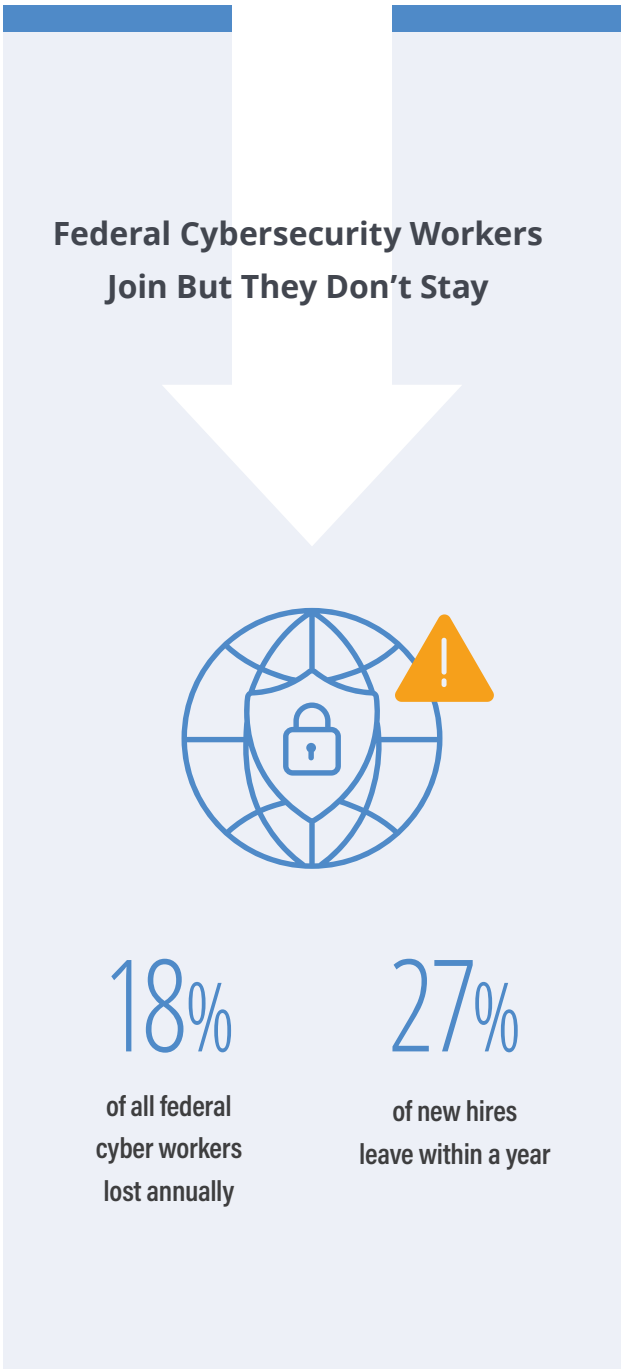
4.

The Current Landscape of Federal Cybersecurity Hiring

Burning Glass's analysis focused on two goals: understanding the state of the federal government's cybersecurity workforce and recruiting practices today; and assessing the needs and challenges facing the federal cybersecurity workforce of tomorrow. The following findings explore the key insights uncovered throughout this analysis.

Federal cybersecurity workers are harder to retain than other IT workers

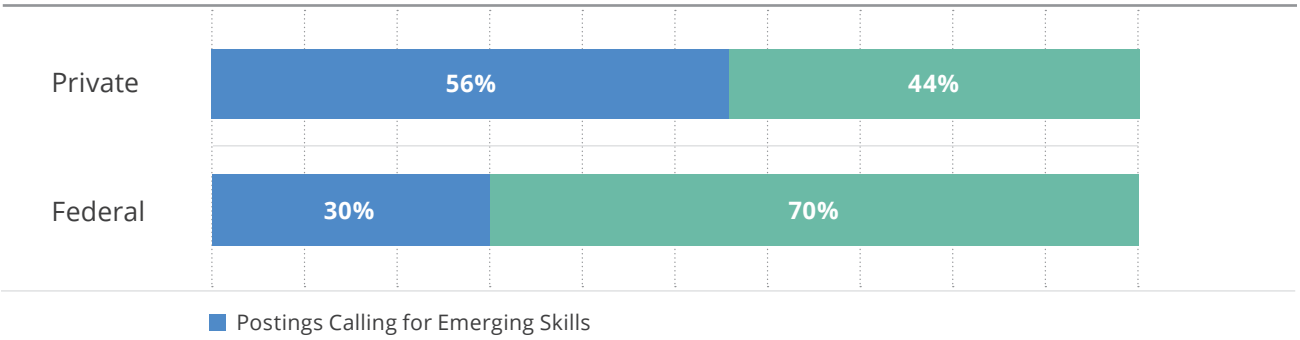
Retaining cybersecurity workers is crucial to maintaining our national cyber defenses, both to ensure sufficient workforce capacity and to prevent the loss of important institutional and operational knowledge. However, the annual turnover rate for federal cybersecurity jobs is 18%, compared to 14% for other federal IT jobs. In practical terms, this means the federal government loses nearly one out of every five cybersecurity workers every year. Moreover, of all workers newly hired into cybersecurity roles within the federal government over the past five years, 27% left the federal government within one year. This suggests that not only does the federal government have a challenge retaining cybersecurity workers in general, but these retention problems are especially pronounced for new hires. This leaves many critical cybersecurity jobs unfilled and hinders the nation's ability to protect against cyber threats.



Federal cybersecurity jobs are less likely to be future-ready

Cybersecurity threats are rapidly evolving as sophisticated cyberattackers constantly reinvent the tools and tactics they use to infiltrate our digital infrastructure. Therefore, cybersecurity workers must constantly evolve as well, and keep their skills current to protect against emerging cyber threats. However, job requirements for private sector cybersecurity jobs are 87% more likely to request emerging skills than requirements for federal cybersecurity jobs. For some key skills the difference is even more dramatic: demand for Python and DevOps in cybersecurity jobs, for example, is 15 times and 30 times greater, respectively, in the private sector than in the public sector. Not investing in future-ready skills both reduces the capacity of the current federal workforce to leverage new technologies and capabilities to defend against evolving threats, but also may disincentivize other workers from applying for federal jobs if they want to keep their skills current.

Federal Cybersecurity Jobs are Less Likely to Request Emerging Skills

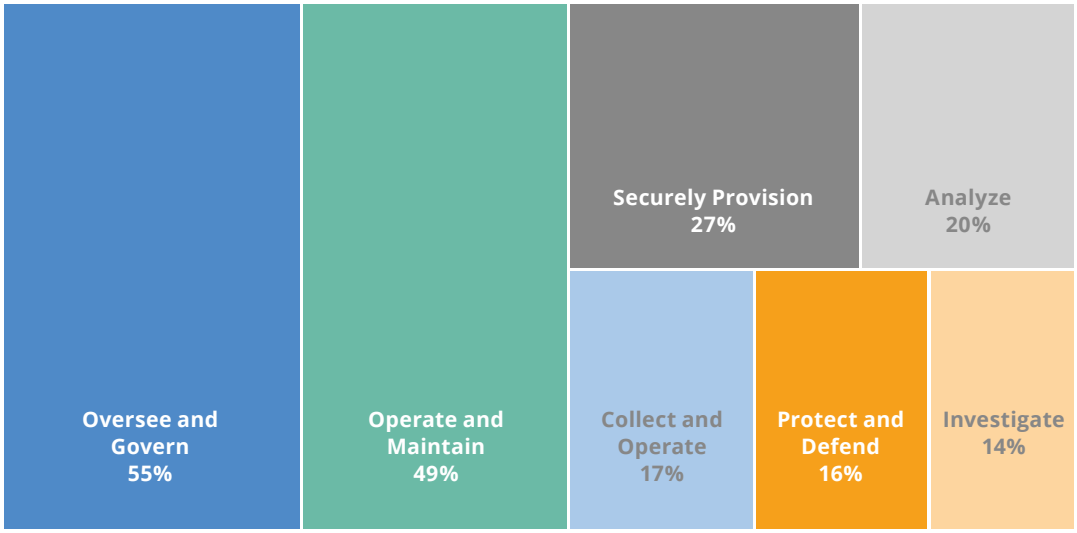


The federal cybersecurity workforce is underemphasizing roles responsible for securing IT infrastructure

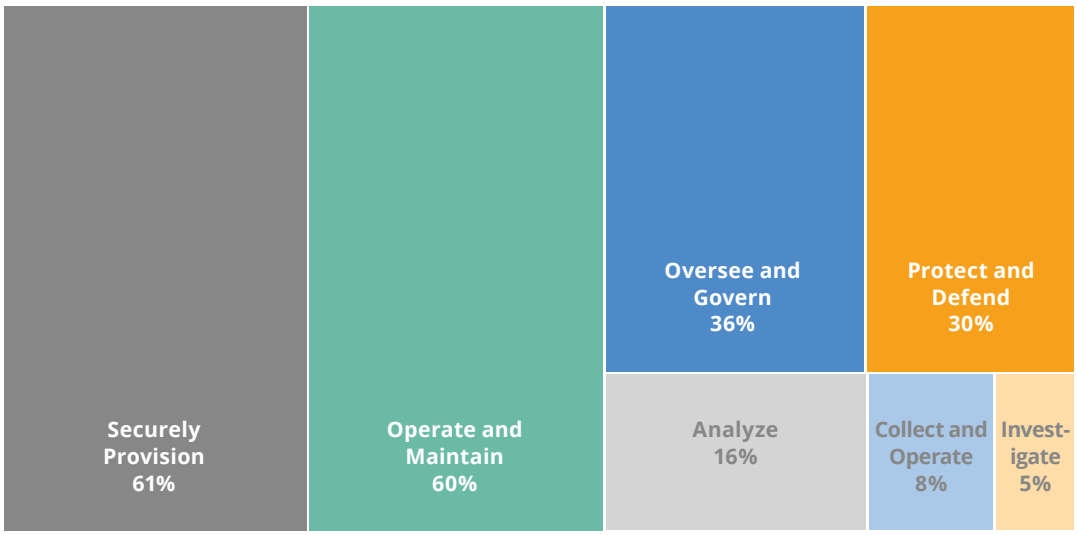
In the federal government, 27% of cybersecurity jobs fall in the Securely Provision category of the NICE Workforce Framework, which describes work that is responsible for architecting secure IT infrastructure. The largest categories of federal jobs fall into the Oversee and Govern category (55%) devoted to management and training, followed by the Operate and Maintain category at 49%, which covers support and maintenance.

By comparison, 61% of all cybersecurity jobs in the private sector are in the Securely Provision category. While this may be due to multiple factors, the stark contrast with the private sector suggests that the federal government is underemphasizing the roles necessary to build a secure digital infrastructure. This increases the risk of building the government's digital infrastructure on a shaky foundation.

Federal NICE Workforce Categories Distributions



Private NICE Workforce Categories Distributions

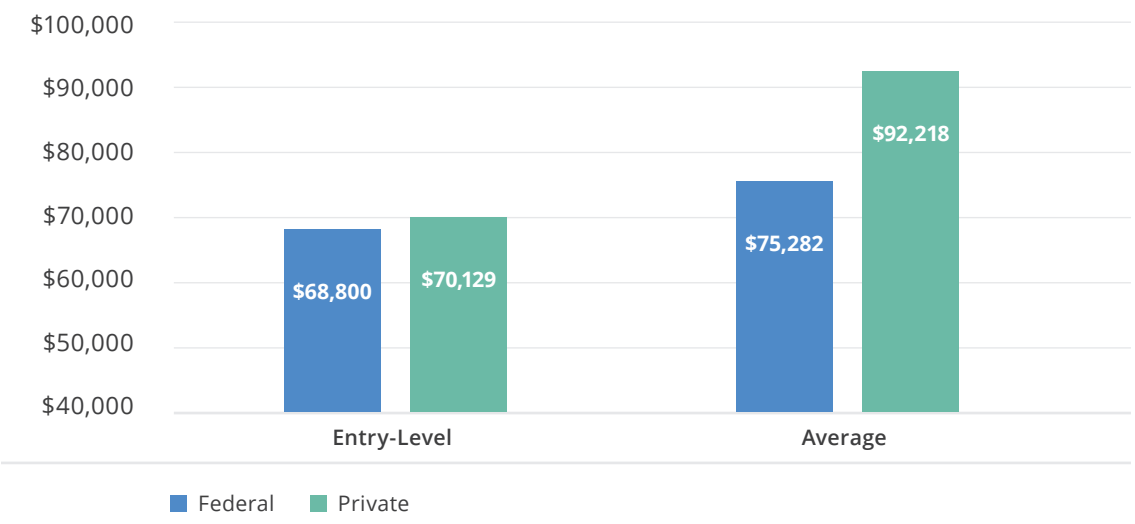


Federal cybersecurity salaries cannot keep up with more lucrative offers in the private sector, but entry-level salaries are comparable

When talent shortages are present, the result is often an arms race for scarce talent that drives up salaries and forces employers to offer compensation in close alignment with market norms. However, cybersecurity jobs in the private sector pay on average 23% more than cybersecurity jobs in the federal government. This pay disparity creates a hurdle for recruiting top talent and increases the risk of workers leaving for higher salaries outside of the federal government.

Despite this overall pay disparity, average federal entry-level cybersecurity salaries are within $2,500 of entry-level salaries in the private sector, suggesting that the federal government can effectively compete for workers who are starting their careers in cybersecurity and invest in strategies aimed at growing and retaining them.

Federal Salaries Competitve at Entry-Level; Below Average Overall



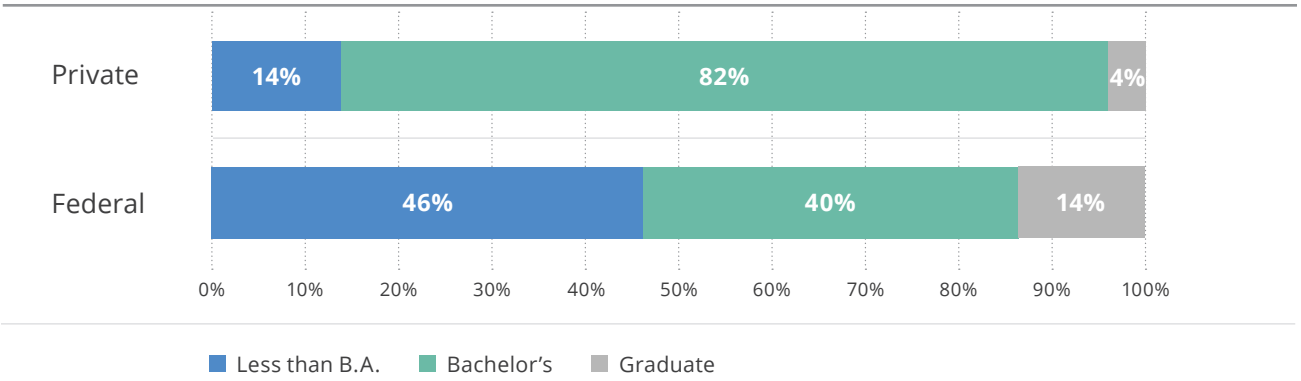
Federal cybersecurity jobs are nearly four times as likely to request a graduate degree compared to cybersecurity jobs in the private sector

Aside from increasing salaries, another way employers may respond to talent shortages is by reducing hiring requirements, such as educational requirements. However, close to 14% of federal cybersecurity job openings request a graduate degree compared to only 4% of private cybersecurity jobs, suggesting the federal government may be overemphasizing the need for advanced cybersecurity degrees. Furthermore, the federal government does not pay a significant premium for these heightened education levels. Advertised salaries for these graduate-level cybersecurity roles in the federal government are nearly $17,000 less than the average for bachelor's-level roles in the private sector. This constrains the talent pool from which the federal government can hire cybersecurity workers, and presents challenges in attracting and retaining workers who can make significantly more money working in the private sector.

Yet the federal government is also dramatically more open than the private sector to hiring cybersecurity talent without a college degree. This is potentially a significant advantage, as the government's demand for cybersecurity workers is outstripping the collegiate talent pipeline

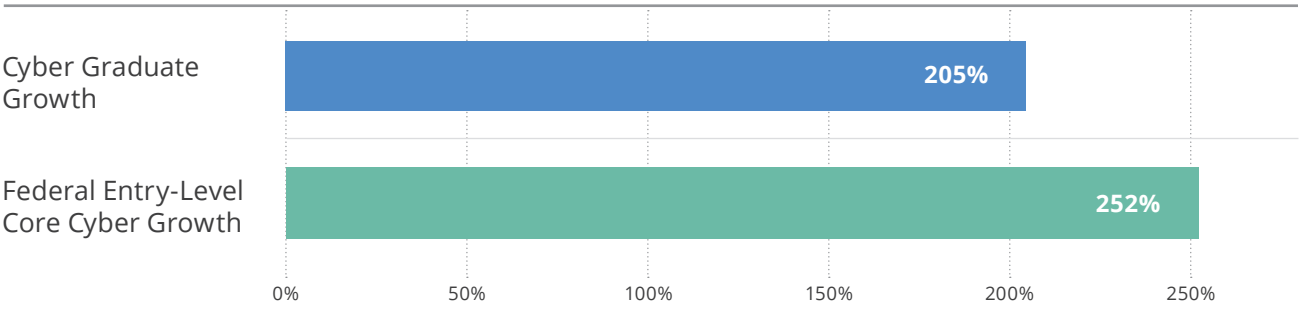
There is, however, a bright spot to the federal government's education requirements. The federal government is much more likely than private employers to request less than a bachelor's degree, suggesting that they do recruit from a larger pool of cybersecurity workers who do not have a four-year degree than many private employers. More than four in 10 federal cybersecurity jobs (46%) are open to workers with less than a bachelor's degree. By contrast, 82% of private sector cybersecurity roles demand a bachelor's.

What are the Minimum Education Requirements for Federal Cybersecurtity Jobs?



If the government's preference for a graduate degree narrows the recruiting pool in some roles, being open to non-college talent makes it easier to recruit in others. To build the next generation of cybersecurity workers — not just for the federal government but for all the nation's employers — the education system must train new cybersecurity talent. Educational institutions have recognized this need for more cybersecurity workers, creating 400 new cybersecurity programs from 2013 to 2018 and growing the number of graduates from cybersecurity degree programs by 205%. While this growth is impressive, it is far outpaced by the 252% growth in demand for entry-level workers in core federal cybersecurity jobs. Therefore, the federal government's increasing demand for new cybersecurity workers cannot be met by simply hiring new graduates.

Cybersecurity Graduates Not Keeping Up with Growing Federal Demand



5.

Actions the Federal Government Can Take to Enhance its Cybersecurity Workforce

Although the federal cybersecurity workforce faces a variety of challenges, there are multiple levers the federal government can pull to build a robust pipeline of future-ready cybersecurity workers for the federal government. Here, we outline eight opportunities to develop and enhance the federal cybersecurity workforce. Many of these opportunities are already being leveraged in some capacity by agencies across the federal government, but we present them without offering a position on the current adoption or efficacy of existing initiatives so that they may be understood outside of the lens of existing policies to spur new, innovative practices.

1 | Expand recruiting to include workers in skill-adjacent talent pools

Hiring workers who have direct experience in cybersecurity may speed up time-to-value after their start date, but recruiting solely from experienced workers also limits the pool of potential candidates. Exploring the full compass of federal recruitment efforts is beyond the scope of this report, and we express no position on whether the federal government is exhaustive in its current recruitment of workers from all available talent pools. We do find, however, that expanding recruitment of core cybersecurity workers to skill-adjacent fields – where workers have a majority of the skills needed to succeed in cybersecurity, even if they are not currently working in core cybersecurity jobs – can dramatically increase the number of workers in the candidate pool.

For instance, if the federal government expands recruiting for core cybersecurity jobs – that is, the jobs solely focused on cybersecurity – to consider all workers in computer and math occupations, it can expand its available talent pool by 3,130%. Even if the federal government only focuses on hiring workers with any form of transferrable cybersecurity experience, it can still expand its recruiting pool for core cybersecurity workers by 267% above existing workers with primary responsibilities related to cybersecurity.

2 | Recruit from more diverse talent pools

Just as recruiting from skill adjacent fields can increase the overall talent pipeline for cybersecurity jobs, so too can it increase the diversity of the talent pipeline. The need for a more diverse cybersecurity workforce is well-documented[2] and many fields that are skill-adjacent to cybersecurity have more diversity among their ranks. For example, only 11% of all Information Security Analysts in the U.S. are female and only 13% come from historically disadvantaged populations. By comparison, 36% of Systems Analysts are female, and 17% of computer support and network specialists come from historically disadvantaged populations – still not ideal representations, but nonetheless better than Information Security Analyst.[3] Recruiting from roles such as these with greater diversity – as well as recruiting from geographies or schools with more diverse populations, such as historically black colleges and universities – can open the federal government's cybersecurity talent pipeline to workers with new perspectives and backgrounds.

3 | Modernize capabilities through rearchitected role descriptions and targeted training of future-ready skills

Building future-ready skills is necessary to keep pace with rapidly evolving threats. The federal government is currently less likely to require emerging skills than the private sector. But it can close this gap by reconsidering and modernizing skill requirements, then adjusting job postings and employee development goals to align with the new skill profiles. The federal government can also upskill its existing workforce through targeted training opportunities directed at high-value, high-growth skills. This may have the added benefit of increasing retention and reducing the need to hire for new capabilities in the federal workforce.

Another related solution federal agencies are beginning to experiment with is public-private talent sharing partnerships. In this model, a private organization and the federal government trade cybersecurity workers with each other for a specified duration of time. This can help federal workers build new skills and experience in the private sector, while also offering a new pipeline of skilled talent from the private sector to support the federal government's cybersecurity needs.

2 Congress Passes Thompson Legislation to Establish a DHS Intelligence and Cybersecurity Diversity Fellowship Program," Committee on Homeland Security, 2020, https://homeland.house.gov/news/legislation/congress-passes-thompson-legislation-to-establish-a-dhs-intelligence-and-cybersecurity-diversity-fellowship-program.

3 Labor Force Statistics from the Current Population Survey, U.S. Bureau of Labor Statistics, 2020, www.bls.gov/cps/cpsaat11.htm.

4 | Increase compensation of all kinds to compete with private sector compensation levels

The higher salaries offered by private employers are a powerful lure for cybersecurity talent. The federal government may not be able to match private sector salaries in all cases, but bringing salaries closer to private sector norms for cybersecurity workers will support improved talent acquisition and retention. In some cases, this may be achieved by separating security workers from overly broad role classifications to increase pay levels, or by increasing types of compensation other than base salaries, such as offering bonuses or emphasizing strong benefits and vacation packages.

5 | Reevaluate credential and experience requirements to make pay more competitive

Where the federal government cannot raise salary levels enough to compete with private employers, there may be opportunities to reduce hiring requirements and expand the pool of candidates from which the federal government recruits. Heightened experience or credential requirements reduce the pool of available workers to those with the highest salary expectations, but loosening these restrictions can have a dramatic impact on salary levels. It also is easier for the federal government to compete with private sector compensation levels when credentials are lowered. For example, the average advertised salary for federal cybersecurity jobs requesting someone with a bachelor's degree is $75,395 – over $20,000 less than the average advertised salary for bachelor's-level cybersecurity workers in the private sector. However, the average salary for federal cybersecurity jobs requiring less than a bachelor's degree is $59,863 – only about $4,200 below the average for sub-baccalaureate cybersecurity jobs at private companies. Similar pay differentials exist when certification or experience requirements are lowered as well, suggesting the federal government should evaluate across the workforce where heightened experience or credential requirements are essential versus just preferred.

6 | Build new opportunities for upward mobility

The federal government is outpacing the private sector when it comes to offering entry-level and sub-baccalaureate opportunities for cybersecurity workers. This presents an opportunity to parlay the federal government's robust entry-level pipeline into long-term employees by increasing opportunities for upward mobility. This could be accomplished by defining clear career pathways that map out developmental goals into managerial positions, as well as building more gradations within existing roles to increase advancement opportunities for individual contributors. This will also support efforts to retain more workers by giving them clear opportunities to further their careers within the federal government.

7 | Standardize cybersecurity role descriptions and nomenclature across the federal government.

Currently, federal cybersecurity hiring is spread across numerous agencies – for this research we found 165 different federal entities recruiting for cybersecurity workers – many of which describe similar jobs using different language. These differing descriptions of responsibilities and skills may or may not align with the language of educators or other employers, making it difficult to coordinate cybersecurity workforce development across such a fragmented hiring and training ecosystem. Standardizing the language used to describe cybersecurity work and skill needs across the federal government will ensure consistency in hiring requirements, streamline the process for identifying similar workers across the federal workforce, and enable easier mappings between skills and training.

A clear opportunity related to these goals is adopting the NICE Framework and using it to describe cybersecurity work across the federal government. Much work has already been done to promote adoption of the NICE Framework – such as executive orders encouraging its utilization across the federal government, as well as efforts to map existing roles to the Framework across agencies – and federal teams can build upon these foundations to further utilize the shared standards and nomenclature afforded by the NICE Framework.

8 | Support the broader ecosystem of cybersecurity workforce development

While there are steps the federal government can take to enhance its recruitment, development, and retention of cybersecurity workers today, these steps will have minimal impact if there remains a dearth of broader cybersecurity talent tomorrow. Therefore, the federal government must invest in building the broader ecosystem of cybersecurity education and workforce development through whatever means it has at its disposal – such as direct investment through grants or other budgetary measures; incentives aimed at catalyzing new opportunities for students and transitioning workers pursuing careers in cybersecurity; and broader sharing of information and data about the challenges and opportunities within the cybersecurity workforce. These types of actions will not only help build the federal government's cybersecurity workforce but also help develop the broader cybersecurity workforce and strengthen the ranks of those protecting our nation's most vital digital assets.

6.

Resources and Acknowledgments

Additional Resources

- **CyberSeek**
  CyberSeek.org
- **National Initiative for Cybersecurity Education (NICE)**
  www.nist.gov/itl/applied-cybersecurity/nice
- **NICE Framework Resource Center**
  www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
- **Cyberspace Solarium Commission**
  www.solarium.gov
- **NICCS**
  niccs.cisa.gov

Authors

Burning Glass Technologies

William Markow
Managing Director

Nomi Vilvovsky
Research Analyst

Acknowledgments

The authors would like to thank numerous individuals both within and outside of the United States government who contributed ideas, information, or other support for this research.

We would like to give special thanks to Rodney Petersen and Danielle Santos from the National Initiative for Cybersecurity Education (NICE), Laura Bate from the Cyberspace Solarium Commission, and individuals from the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) who graciously offered their time and insights to support this report.

Burning Glass Technologies
66 Long Wharf | Floor 2
Boston, MA 02110
+1 (617) 227-4800
www.burning-glass.com

Burning Glass Technologies delivers job market analytics that empower employers, workers, and educators to make data-driven decisions. The company's artificial intelligence technology analyzes hundreds of millions of job postings and real-life career transitions to provide insight into labor market patterns. This real-time strategic intelligence offers crucial insights, such as which jobs are most in demand, the specific skills employers need, and the career directions that offer the highest potential for workers. For more information, visit burning-glass.com.

burningglass® TECHNOLOGIES