Filling the Skills Gap to Develop a Cyber Workforce

There's a shortfall of roughly 3 million cybersecurity professionals worldwide, including about 500,000 in North America, according to the 2018 Cybersecurity Workforce Study by the International Information System Security Certification Consortium ((ISC)2). Subsequently, the federal government doesn't have enough employees to meet its cybersecurity needs. Even worse, shortfalls in federal cybersecurity talent expose the U.S. to economic, strategic, and national security risks.

Knowing where an agency's skills gaps exist can help its workforce evolve to successfully overcome any cybersecurity obstacles. This resource will help your organization understand its shortage of cybersecurity professionals and how to protect its assets with its existing workforce. Choose the scenario that best describes your agency's current cybersecurity workforce, then check out a fitting solution for your challenges.

SCENARIO #1

My agency has little to no cybersecurity talent but can't afford new workers with its current budget constraints.

SOLUTION #1:

Your agency should host an **apprenticeship, internship, or work-study program**. Agencies that host these initiatives increase their short-term cybersecurity capacities while building long-term talent pipelines. Participants gain practical cybersecurity experience and skills that are attractive to future employers. For agencies with tight budgets, these programs are an affordable alternative to permanently hiring employees.

SCENARIO #2

My agency has little to no cybersecurity talent but has budget dollars for hiring new staff.

SOLUTION #2:

Your organization should recruit new cybersecurity talent from academic institutions that have been designated as a **National Center of Academic Excellence (CAE)** in cybersecurity. The CAE program aims to "reduce vulnerability in our national information infrastructure by promoting higher education and research in Cyber Defense (CD) and to produce a growing number of professionals with expertise in CD disciplines." Cybersecurity programs must meet rigorous criteria for their institutions before becoming CAEs in Cybersecurity Defense Education (CDE), Cyber Operations (CO), or Research (R). Eventually, these institutions generate quality, well-educated cybersecurity recruits for agencies to hire.

SCENARIO #3

My agency has little to no cybersecurity talent but a surplus of employees in other areas.

SOLUTION #3:

Your agency is a prime candidate for **reskilling**, or training individuals with the aptitude for completely new occupations. One option is the Federal Academic Alliance (FAA), which provides higher education opportunities to federal workers at reduced tuition rates to address governmentwide skills gaps, including cybersecurity. The Office of Personnel Management (OPM) currently endorses 15 colleges and universities for FAA. FAA participants can use the program's benefits to become educated for competent, long-term cybersecurity work.

SCENARIO #4:
My agency has a large amount of cybersecurity talent that could use more training to better protect our organization.

SOLUTION #4:
Your organization should examine **upskilling**, or providing training to individuals in the same occupation on new skills using new methods. For example, cyber competitions such as the President's Cup Cybersecurity Challenge for federal civilian and military employees can assess your agency's cybersecurity talent with hands-on experiences. These events teach participants about threats that are prevalent in the workplace; they also improve teamwork, communication, leadership, and problem solving. Upskilling saves money by taking the employees agencies already have and teaching them additional responsibilities.

SCENARIO #5:
My agency has a large amount of cybersecurity talent but little diversity.

SOLUTION #5:
Your agency should research **partnering with community colleges.** Community colleges help diversify cybersecurity talent pipelines by offering affordable and practical education options to diverse student populations. For example, these schools often offer online classes aimed at helping students complete their studies while working. The associate degrees these schools provide are often great pathways to entry-level employment in fields such as cybersecurity.

SCENARIO #6:
My agency has a large, diverse cybersecurity workforce that isn't engaged in our mission.

SOLUTION #6:
Your agency might consider boosting engagement through **involvement with K–12 cybersecurity education**. For instance, the federal GenCyber Program provides summer cybersecurity camps for K–12 students and teachers. By teaching young people interested in cybersecurity, government employees can apply their skills in fulfilling, tangible ways. The students they instruct could someday create a larger, more diverse pool of cybersecurity talent nationwide.

Filling the skills gap to create a strong cybersecurity workforce is essential to safekeeping America's economic, strategic, and national security interests.

Excelsior College offers online undergraduate and graduate degree programs across many fields, including cybersecurity. The college also offers internships for credit to help fill the growing need for cybersecurity professionals.

Excelsior College, one of the 15 colleges and universities that are part of the FAA, partners with more than 100 community colleges across the U.S. It was designated as a CDE CAE in 2014, and in 2019 earned re-designation through 2024.

To learn more about Excelsior College's cybersecurity degree programs, courses, and initiatives for the federal government, visit **excelsior.edu/partner/feducation**

EXCELSIOR COLLEGE®

GovLoop is the knowledge network for government - the premier online community connecting 300,000+ federal, state and local government innovators.

govloop