Consensus Study Report

June 2021

HIGHLIGHTS

Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration

The National Academies of
SCIENCES · ENGINEERING · MEDICINE
CONSENSUS STUDY REPORT
Looking Ahead at the
Cybersecurity Workforce at the
Federal Aviation Administration

The Federal Aviation Administration (FAA) is responsible for providing the "safest, most efficient aerospace system in the world." Over the past decade, it has overseen significant upgrades to the technology used to manage aviation operations to increase the safety and efficiency of the National Airspace System (NAS). Though necessary to regular operations, these modern computing and communications systems provide a greater attack surface for criminals, terrorists, or nation-states to exploit and thereby increase the potential for cybersecurity threats to the NAS and its constituents. Expanding digitization and connectivity *without adequate cybersecurity* could have enormous consequences; disruption anywhere in the aviation sector can spread across borders, cause significant financial damages, and compromise safety. While this transition is ongoing, the FAA still needs to protect its legacy-based systems.

The future safety and security of air travel will rely, in part, on the ability of the FAA to build a workforce capable of addressing the evolving cybersecurity threat landscape. Securing the computers, networks, and data that underpin modern aviation depends in part on the FAA having enough cybersecurity professionals (**capacity**) with the right knowledge, skills, and abilities (**capability**). It also depends on the FAA's workforce having sufficient **diversity** of backgrounds and experience. Such diversity is critical in analyzing cybersecurity problems and widely understood to be a "functional imperative" for effective cybersecurity programs.

To help meet the future cybersecurity needs of the FAA, Congress called on the National Academies of Sciences, Engineering, and Medicine to examine the FAA's cybersecurity workforce challenges, review the FAA's current strategy for meeting those challenges, and recommend ways to strengthen the FAA's cybersecurity workforce. In response to this charge, the National Academies convened a 12-member Committee on the Cybersecurity Workforce of the Federal Aviation Administration. Drawn from industry and academia and representing fields such as cybersecurity, organizational psychology, human factors and ergonomics, and aviation, the committee met with experts, practitioners, and current cybersecurity employees at the FAA to learn about best practices in building a diverse cybersecurity workforce with high capacity and capability. The Congressional reuest asked the committee to include workforce size, quality, and diversity in their considerations.

Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration (2021) results from this extensive research process, providing both insight into the agency's current challenges in building its cybersecurity workforce and recommendations to ensure the future success of the FAA's cybersecurity operations. While the FAA's current cybersecurity workforce is roughly on par with industry trends for diversity and has proven capable of meeting the agency's current needs, technological change and structural pressures make the issue of cybersecurity workforce development a critical one for FAA leadership. With better use of existing programs for talent recruitment and adoption of proven practices to build a diverse talent pipeline, the FAA can ensure that it will continue to meet the cybersecurity challenges of the 21st century.

As a cybersecurity organization, the FAA faces structural stresses on its workforce. Cybersecurity professionals are highly sought after, and competition among employers for the limited talent pool is likely to grow more acute. Despite a multitude of initiatives to address the cybersecurity workforce imperative, the nation still faces a significant shortage of qualified cybersecurity professionals. The demand for talent is particularly severe in the public sector, because federal agencies must compete with private-sector firms that often provide better compensation. On top of this wage pressure, the FAA has further unique needs for its cybersecurity workforce, such as the need for employees to have a deep understanding of a highly specialized mission and technology infrastructure alongside an ability to defend against both cyber and physical safety and security threats. As the FAA faces challenges in bringing new talent into the organization due to lower public-sector wages, it also faces a future wave of retirement among its cybersecurity workforce. Like many federal agencies, the FAA has a significant fraction of employees who are or soon will be eligible for retirement. This means that within a relatively short timeframe, the FAA may have to replace a significant portion of its cybersecurity workforce amidst increasing competition for talent and ensure that the agency can retain the highly specialized, mission-specific knowledge of its retiring cybersecurity workforce.

These pressures occur against an operational backdrop in which the FAA's priority on cybersecurity defenses is amplified by growing digitization and connectivity of the NAS and aviation sector. The introduction of tools such as cloud computing and internet-connected devices into the FAA may offer significant improvements to the agency's ability to monitor air traffic and fulfill its mission, but it also offers malicious actors more avenues to disrupt critical air safety operations. In response to these changing dynamics, the FAA will need to introduce a range of skills and expertise into its cybersecurity workforce.

The FAA needs to take better advantage of existing programs and practices to bolster cybersecurity recruitment, especially if it is to build a robust and diverse cybersecurity workforce. From scholarship opportunities that pair students with public-sector organizations for internships and postgraduate employment, to spot hiring accommodations that provide agencies with flexibility to pursue in-demand talent outside the usual hiring process, the FAA has not yet taken full advantage of these programs. The FAA will need to be more effective in recruiting a cyber workforce of sufficient capacity and capability in the face of competition for cybersecurity talent, the need to be ready to replace a wave of retirees, and the need for greater diversity in its cybersecurity workforce.

Diversity is an operational imperative for the FAA and other cybersecurity organizations. Cybersecurity as a discipline incorporates a broad range of skills and knowledge, thus an effective cybersecurity workforce will need to be diverse across several axes—a consideration that includes both traditional diversity strategies such as increased engagement of underrepresented minorities and women, and other considerations such as encouraging applicants from a range of different educational institutions, previous employers, and geographic locations. Adversaries present a changing set of threat activities that challenge the imagination. To manage these tactics, cyber professionals from diverse backgrounds and representing a range of views and skillsets are required as a critical part of the workforce. Greater diversity represents an opportunity to grow the talent pool and anticipate changing national demographics. Growing this talent pool will allow the FAA to keep pace with other organizations that have made diversity a recruitment priority.

The FAA can address its challenges by learning from already-existing practices and programs within the federal government. By replicating efforts already occurring in other federal agencies, the FAA can make significant gains in improving cyber recruitment and bolstering its diversity. For instance, the popular Scholarship for Service (SFS) program helps connect cybersecurity students to federal employers and facilitate summer internships and employment after graduation. Partnerships at the institutional level can also foster the creation of a robust cybersecurity talent pipeline. Here, too, other federal agencies have established models that the FAA can adopt, including developing centers of academic excellence and scholar-in-residence programs, and collaborating in the development of specialized curricula and educational material.

The FAA can also learn from best practices within the private sector. Mirroring private-sector trends that have bolstered the role of chief infromation security officers (CISO), the FAA should consider providing the CISO role with more authority and access to agency leadership, allowing the FAA to better identify and direct responses to cybersecurity challenges and foster an organizational culture in which cybersecurity professionals and other employees can be most effective in doing so.

Changes within the FAA's organization and practices can further improve the agency's ability to attract and retain needed diverse cybersecurity talent. Some small changes to the ways in which the FAA presents itself and manages its existing workforce can lay the foundation for recruiting a strong cybersecurity workforce. For instance, the FAA offers potential employees a work environment that combines cybersecurity operations with a unique mission. While this offers an attractive opportunity for cybersecurity professionals, this was not always evident in the FAA's recruitment materials. Recruitment efforts can better highlight the opportunities to apply cybersecurity skills to the mission and in a unique operational environment, through enhanced job fair materials and more compelling job descriptions.

The FAA can emphasize efforts to reskill workers to equip them to perform cybersecurity functions. Given the wide range of skills relevant to its cybersecurity practice, reskilling current employees—including current cybersecurity staff, noncybersecurity information technology staff, and operations staff—can provide the FAA with a more readily available talent pool of future cybersecurity talent.

COMMITTEE ON THE CYBERSECURITY WORKFORCE OF THE FEDERAL AVIATION ADMINISTRATION

DIANA L. BURLEY (Co-Chair), American University; **TONYA L. SMITH-JACKSON** (Co-Chair), North Carolina A&T State University; **RODNEY C. ADKINS,** 3RAM Group; **JANDRIA S. ALEXANDER,** Booz Allen & Hamilton; **MARILYN BARRIOS,** Motorola Solutions; **CHARLES BLAUNER,** Cyber Aegis; Team8 Ventures; **MICHAEL D. COOVERT,** University of South Florida; **BARBARA ENDICOTT-POPOVSKY,** University of Washington; **ERIC GROSSE,** Security Consultant; **ROBERT S. GUTZWILLER,** Arizona State University; **KATYA LE BLANC,** Idaho National Laboratory; **NAN SHELLABARGER,** FAA (Retired); **DANIEL TALMAGE,** *Co-Study Director;* **BRENDAN ROACH,** *Co-Study Director;* **MONICA STARNES,** *Senior Program Officer, TRB;* **ADAM JONES,** *Senior Program Assistant;* **MARY ELLEN O'CONNELL,** *Interim Board Director, BOHSI;* **JON EISENBERG,** *Board Director, CSTB.*

For More Information . . . This Consensus Study Report Highlights was prepared by the Board on Human-Systems Integration based on the Consensus Study Report, *Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration* (2021). The study was sponsored by the Federal Aviation Administration. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project. Copies of the Consensus Study Report are available from the National Academies Press, (800) 624-6242 or https://nap.edu/26105.

Division of Behavioral and Social Sciences and Education

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

The nation turns to the National Academies of Sciences, Engineering, and Medicine for independent, objective advice on issues that affect people's lives worldwide.
www.national-academies.org