The National Academies of
SCIENCES · ENGINEERING · MEDICINE

Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

CONSENSUS STUDY REPORT

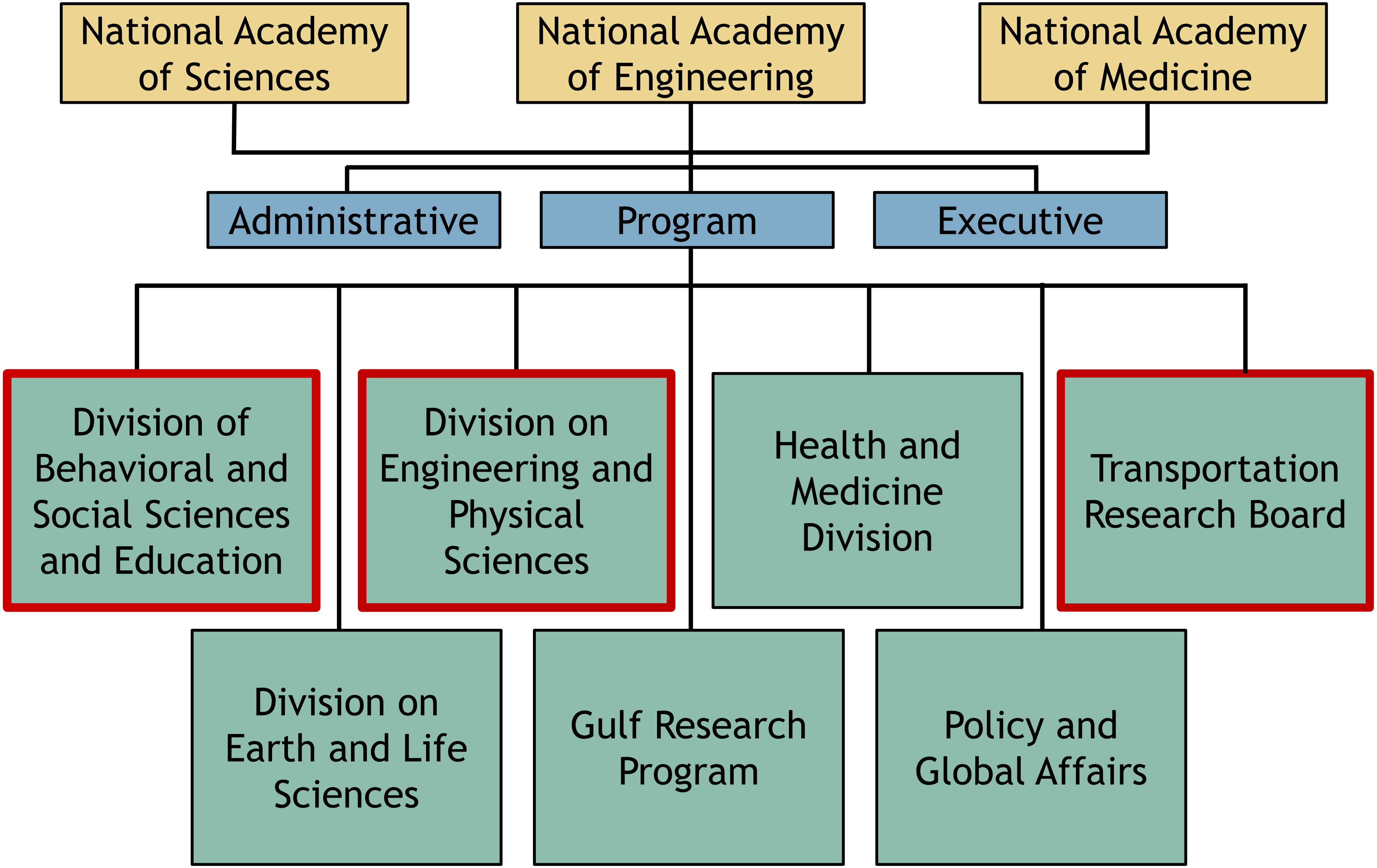
Looking Ahead at the **Cybersecurity Workforce** at the **Federal Aviation Administration**

The National Academies of Sciences, Engineering, and Medicine

… are private, nonprofit, nongovernmental.

… provide independent, objective analysis and advice to the nation to solve complex problems and inform public policy decisions related to science, technology, and medicine.

… operate under an 1863 congressional charter to the National Academy of Sciences, signed by President Lincoln.



National Academy of Sciences

National Academy of Engineering

National Academy of Medicine

Administrative

Program

Executive

Division of Behavioral and Social Sciences and Education

Division on Engineering and Physical Sciences

Health and Medicine Division

Transportation Research Board

Division on Earth and Life Sciences

Gulf Research Program

Policy and Global Affairs

Committee

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)

Staff
DANIEL TALMAGE, Co-Study Director
BRENDAN ROACH, Co-Study Director
ADAM JONES, Senior Program Assistant
TOBY WARDEN, Board Director, BOHSI
JON EISENBERG, Board Director, CSTB
MONICA STARNES, Senior Program Officer, TRB

Reviewers

LEISEL BOGAN, Director, Congressional Digital Service Fellowship
DAVID J. DEROSIER, Department of Biology (emeritus), Brandeis University
MICHAEL A. ECHOLS, CEO, Max Cybersecurity LLC
R JOHN HANSMAN, Director, International Center for Air Transportation, Massachusetts Institute of Technology
MICHAEL P. HUERTA, CEO, MPH Consulting, LLC
NANI LEE, consultant, Waimea-South Kohala, Hawai’i
MICHELLE MONSEES, consultant, Fairfax County, VA
FREDERICK L. OSWALD, Department of Psychology, Rice University
JUAN PEREZ, Chief Information and Engineering Officer, UPS

Monitor
JENNIE S. HWANG, H-Technologies Group, Case Western Reserve University,
Coordinator
WESLEY L. HARRIS, Aeronautics and Astronautics, Massachusetts institute of Technology

FAA Reauthorization Act of 2018

Section 549, of the 2018 FAA Reauthorization Act calls for a Study on the Cybersecurity Workforce of FAA and states that:

(a) STUDY.—Not later than 1 year after the date of the enactment of this Act, the Administrator shall enter into an agreement with the National Academy of Sciences to conduct a study on the cybersecurity workforce of the Administration in order to develop recommendations to increase the size, quality, and diversity of such workforce, including cybersecurity researchers and specialists.

(b) REPORT TO CONGRESS.—Not later than 180 days after the completion of the study conducted under subsection (a), the Administrator shall submit to the appropriate committees of Congress a report on the results of such study.

Statement of Task

Pursuant to Section 549 of the FAA Reauthorization Act of 2018, a National Academies consensus study committee will (1) examine the Federal Aviation Administration's (FAA's) cybersecurity workforce challenges, (2) review FAA's current strategy for meeting those challenges, and (3) provide recommendations related to strengthening the FAA's cybersecurity workforce, including consideration of its size, quality, and diversity. The study will consider cybersecurity workforce challenges agency-wide, including in such major functional areas as National Airspace System management, enterprise computing and communications infrastructure, air traffic control system acquisition and modernization, unmanned aircraft systems, and safety regulation. The study will take into account how the FAA's cybersecurity workforce needs are likely to change over time.

Continued on next page

Statement of Task

Areas to be explored include the following:

- The current and future cybersecurity landscape for the FAA and its mission areas;
- Management and human resource approaches and strategies to achieve current and future desired outcomes that meet cybersecurity workforce needs, including recruitment and flexibilities, selection, retention, training, education, certification, and compensation considerations;
- Cybersecurity organization structure, workforce strategies, and best practices of other government and private sector organizations with relevant missions, including air traffic management and aviation safety assurance;
- Statutory, regulatory, and other institutional constraints on recruitment and flexibilities, hiring, retention, and compensation of cybersecurity workers;
- Strategies to strengthen the cybersecurity workforce by attracting and retaining candidates from diverse backgrounds, including age, race, gender, and geography;
- FAA organizational structure, culture, and norms that affect the cybersecurity workforce;
- The U.S. labor market in cybersecurity expertise and commercial competition for qualified candidates; and
- The existing structure used by the FAA to define the diverse set of workforce cyber knowledge, skills, and abilities, and its alignment with frameworks such as the National Initiative for Cybersecurity Education.

The committee's evidence base, analysis, findings, conclusions, and recommendations will be set forth in a final report.

Study Timeline

- Contract started in October 2019
- First committee meeting February 2020 in person
- Held 4 more virtual meetings
- Received data and presentations from government, academia, and industry speakers
- Numerous committee chapter calls during report writing, discussions, and consensus building
- Report release June 2021

Presenters

Larry Grossman, Federal Aviation Administration

Steven Hernandez, Department of Education

Alfred Lewis, Boeing

Peter Cooper MSc FRAeS, Pavisade Cybersecurity

Victor Piotrowski, National Science Foundation

Rodney Petersen, National Institute of Standards and Technology

Steven Cook, North Carolina A&T State University

Ambareen Siraj, Tennessee Tech; Women in Cybersecurity

Michael Worden, Raytheon

Heather Romero, Raytheon

Commander Jamie Embry, United States Coast Guard

Juan Perez, UPS

Gail Greenfield, Mercer Consulting

Frederick R. Chang (NAE), Southern Methodist University

Patrick Mana, Eurocontrol

Dominic Nessi, Los Angeles International Airport

Mauricio Velasquez, Diversity Training Group

Ahmed Hussein, Federal Aviation Administration

Mary Ellen Zurko, Lincoln Lab

Sadie Perez, Federal Aviation Administration

Earl Crane, Carnegie Mellon University

Patricia Gilbert, NATCA

Gilman Louie, Alsop Louie Partners

Charlie Lewis, McKinsey and Company

Dr. Shane Stailey, Idaho National Laboratory

Dr. Sean McBride, Idaho State

Samuel Visner, National Cybersecurity Federally Funded Research Center

Anne Audet, Department of Transportation

Rick Kempinski, Partnership for Public Service

Lucy Cunningham, Partnership for Public Service

Leisel Bogan, Congressional Digital Service Fellowship

Report Outline

- Summary
- Chapter 1 - Introduction about the project and the committee
- Chapter 2 – Sets the stage for the reader on the FAA
- Chapter 3 – Introduces the adapted Employee Lifecycle
- Chapter 4 – Continues the adapted Employee Lifecycle
- Chapter 5 – Gives an expanded summary of the report

Committee Definition of Diversity

The committee considers diversity to include, in the context of the FAA's workforce needs, both the broad array of characteristics generally associated with diversity such as race, ethnicity, sexual orientation, and gender, as well as less frequently considered factors that shape an individual's identity. These other factors include, but are not limited to, geographical, national, academic, institutional or military affiliation, socio economic status, and linguistic background.

Challenges and Opportunities

- Supported by Findings, Conclusions, and Recommendations
- Focused on immediate or urgent issues
- Ordered by themes in report, not necessarily importance.

Challenge 1

Expansion of the FAA's digital footprint also increases vulnerability and risk, and so, increases the need for more robust cybersecurity due to these potential new threats.

Conclusion 2-2: The cyber landscape of the FAA is continuously evolving. Accordingly, the future FAA cybersecurity workforce will need to adapt in order to simultaneously support traditional enterprise infrastructure and security operation center needs, as well as provide subject matter expertise and program oversight of cybersecurity integration into all aspects of FAA's missions.

Finding 3-1: The complexity of challenges that cybersecurity professionals address requires a workforce with a diversity of experiences and cognitive approaches, making diversity a functional imperative of cyber operations.

Challenge 2

The cybersecurity labor market is highly competitive within the federal sector, nationally, and globally—and likely to become more so.

Finding 2-5: The pool of qualified cybersecurity talent is limited and recruitment challenges will persist.

Finding 3-4: To aid in the recruitment process federal agencies are able "To recruit and retain personnel with the critical skills needed to accomplish their missions, federal agencies can offer incentives, such as recruitment, relocation, and retention incentive payments; student loan repayments; annual leave enhancements; and scholarships" (Marinos, 2017).

Challenge 3

The FAA faces a future wave of retirements in its cybersecurity workforce.

Finding 2-2: A growing proportion of the cybersecurity workforce of the FAA is reaching retirement eligibility and, as a result, the agency is vulnerable to losing a significant portion of its cybersecurity workforce to retirement.

Challenge 4

To achieve greater diversity within the cybersecurity workforce and meet its future needs, the agency must make better use of existing programs that promote workforce diversity.

Finding 2-1: The FAA can expand representation of both women and minorities in their cybersecurity workforce. The agency is better than average with diversity workforce trends for women but may lag behind global percentages for underrepresented minorities in the cybersecurity workforce. Additional information on the racial composition of the FAA cybersecurity workforce is required to accurately describe the current state.

Finding 4-3: Institutional partnerships with Minority-Serving Institutions (MSIs) can both expand the talent pool for high-demand positions and ensure diversity in the workforce for the long term.

Challenge 5

The FAA's current recruitment capabilities are not robust enough to meet future demand in an increasingly competitive environment.

Finding 3-9: The FAA has not partnered with the Scholarship for Service program to effectively recruit cyber talent to the organization.

Finding 3-10: The FAA has not partnered with universities to shape cybersecurity programs and curricula.

Finding 3-13: The FAA does not take advantage of programs that other agencies use to recruit cybersecurity professionals.

Opportunity 1

Leverage FAA's compelling mission as a recruitment tool.

Finding 3-3: Organizational reputation and positioning is a critical component of recruitment and talent attraction efforts.

Finding 3-7: Many individuals presently in the FAA report an early interest in aviation.

Opportunity 2

Broaden the talent pipeline by building sustainable relationships with educational and industry partners and enhancing college recruitment.

Recommendation 3-1: The FAA should evaluate the use of existing and future internship programs as valuable tools to create a more diverse cybersecurity workforce.

Continued on next page

Opportunity 2

Broaden the talent pipeline by building sustainable relationships with educational and industry partners and enhancing college recruitment.

Recommendation 3-3: The FAA would benefit from engaging more robustly with recruitment fairs and college programs to bolster the hiring pipeline for cybersecurity positions. Moreover, long-term university partnerships using such activities as scholars-in-residence from the FAA might enhance the FAA's ability to recruit talented recent college graduates. The FAA should organize and expand its reach and partnerships with universities around cybersecurity preparation efforts in academic and research areas to assist in the development of a talented cybersecurity workforce. Among these partnerships, the FAA should explore opportunities to develop meaningful and sustainable relationships with Minority Serving Institutions to access up-coming cybersecurity graduates via internships and employment opportunities.

Continued on next page

Opportunity 2

Broaden the talent pipeline by building sustainable relationships with educational and industry partners and enhancing college recruitment.

Conclusion 3-5: The committee concludes that the use of numerical targets, such as number of SFS program graduates recruited and/or hired to internships and permanent employment, would be a useful mechanism for engaging additional interns with this program.

Opportunity 3

Enhance diversity by leveraging existing best practices.

Recommendation 3-3: The FAA would benefit from engaging more robustly with recruitment fairs and college programs to bolster the hiring pipeline for cybersecurity positions. Moreover, long-term university partnerships using such activities as scholars-in-residence from the FAA might enhance the FAA's ability to recruit talented recent college graduates. The FAA should organize and expand its reach and partnerships with universities around cybersecurity preparation efforts in academic and research areas to assist in the development of a talented cybersecurity workforce. Among these partnerships, the FAA should explore opportunities to develop meaningful and sustainable relationships with Minority Serving Institutions to access up-coming cybersecurity graduates via internships and employment opportunities.

Recommendation 3-7: The FAA should train its cyber leadership on best practices in building a diverse and inclusive organizational culture and should customize these best practices to implement a more contemporary model.

Opportunity 4

Leverage federal hiring programs, non-salary financial incentives, and flexibilities to attract and retain talent.

Recommendation 2-4: The FAA should compare and contrast flexibility with other federal programs in terms of hiring, to identify other agency flexibilities and practices that could be incorporated into FAA hiring.

Opportunity 5

Promote and invest in training and reskilling.

Recommendation 3-5: Reskilling the existing workforce can be an important component of developing the needed future cybersecurity workforce for the FAA and over time reskilling should grow beyond technical skills to include managerial and operational skills.

Opportunity 6

Anticipate the coming wave of retirements.

Recommendation 2-1: The cybersecurity workforce within the FAA is generally satisfied and dedicated to the agency's mission. The FAA's high employee retention rate in cybersecurity has helped it maintain the needed workforce capacity and capability, but with a growing proportion of the cybersecurity workforce of the FAA reaching retirement eligibility, the agency is vulnerable to losing a significant portion of its cybersecurity workforce to retirement. However, in the event of widespread retirement, the FAA will likely find it very challenging to restore/rebuild its workforce given its current challenges with recruitment. And thus, the FAA should implement cybersecurity workforce planning strategies that will protect the agency against the potential for sudden and mass retirements.

Recommendation 4-2: The FAA should provide professional development opportunities to refresh skill sets of current cybersecurity employees and ensure sharing of key institutional and mission-specific knowledge with newer cybersecurity staff.

Opportunity 7

Ensure that the FAA's chief information security officer (CISO) has sufficient authority and access to agency leadership.

Recommendation 4-3: The FAA cybersecurity employees and the cybersecurity program as a whole will benefit from a CISO that can develop a comprehensive cybersecurity strategy that crosses multiple complex domains in the FAA. The CISO's reporting structure needs to support a strong governance model, which ensures that the CISO has both the independence and the access required to effectively manage the FAA's cyber risk posture. In support of such leadership responsibility, the FAA should position the CISO role at the most senior level of the non-political appointees within the organization. Given the scarcity of qualified people, the FAA should consider variances from current pay-scale limitations in order to be a competitive employer.

Additional Recommendations

Chapter 2

Recommendation 2-2: Workforce diversity also strengthens the performance of cybersecurity efforts. The FAA should expand recruitment efforts to include potential hires from different science, technology, engineering and mathematics backgrounds and careers.

Recommendation 2-3: The FAA's ability to hire cybersecurity workers is constrained by citizenship and security clearance requirements. Moreover, the FAA is currently under-utilizing flexibilities in personnel management and hiring authority, such as direct-hire authority The FAA should compare and contrast flexibility with other federal programs in terms of hiring, to identify other agency flexibilities and practices that could be incorporated into FAA hiring.

Chapter 3

Recommendation 3-2: At the organizational level, promoting and marketing the agency as an attractive/fulfilling/rewarding place for cybersecurity would facilitate recruiting. However, there is a lack of clarity on what the FAA's current marketing strategy and branding are for cybersecurity. While any FAA marketing approach needs to conform with the larger context of the brand of the federal government, actions to develop a strong FAA-specific marketing presence in cybersecurity should be implemented. To do so, the FAA should identify priority targets for recruitment (and identify their characteristics) and tailor their marketing to reach those targets effectively.

Recommendation 3-4: Hiring employees with the right skillset and then growing them as the job requirements change is optimal. This is possible through programs like the Scholarship for Service (SFS) program or reskilling current employees, which are two options for improving the cyber workforce. So far, the FAA has not partnered with the SFS program to effectively recruit cyber talent to the organization; this offers an opportunity in waiting and a partnership should be pursued. In this and other ways, the FAA should explore a wide range of options for meeting future reskilling needs, including internal, outside commercial, industry conference workshops, and outside rotations in agencies and industry.

Recommendation 3-6: The FAA should continue to use the NICE tool to develop work roles that fit into a larger, well-designed organizational structure.

Continued on next page

Chapter 3

Recommendation 3-8: When comparing non-salary monetary incentives, FAA cannot compete with industry pay scales. The FAA should leverage non-salary monetary incentives (career development reimbursements, performance bonuses, etc.).

Recommendation 3-9: "Early interest" in cybersecurity and in aviation by young students is a notion that can be identified and then leveraged in FAA recruitment. Two targeted actions are recommended here to foster and capitalize on FAA related "early interest":

- The FAA should review its past experience with effective fellowship and internship programs and also look to other federal agencies for proven models, such as the DoD SMART scholarship program.
- The FAA should sponsor and leverage postsecondary-level cyber competitions.

Chapter 4

Recommendation 4-1: The FAA should monitor, and revise if necessary, its personnel practices to support the development of the necessary skills to meet the ever-changing demand in the current and future cybersecurity workforce.

Recommendation 4-5: The FAA should enable the success of the cybersecurity program and the CISO by designing a hybrid organizational model leveraging private sector best practices such as blending core and edge (vertically integrated) functions as well as the plan, build, operate model.

Path Forward

- Dissemination to additional FAA staff and congressional staff.
- FAA will report back to Congress within 180 days of report release (June 21, 2021).

Questions

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

CONSENSUS STUDY REPORT

Looking Ahead at the **Cybersecurity Workforce** at the **Federal Aviation Administration**

Backup Slides

Conclusions

Chapter 2

Conclusion 2-1: The cybersecurity labor market is not only tight today, but highly dynamic and expected to get much tighter in the future.

Conclusion 2-2: The cyber landscape of the FAA is continuously evolving. Accordingly, the future FAA cybersecurity workforce will need to adapt in order to simultaneously support traditional enterprise infrastructure and security operation center needs, as well as provide subject matter expertise and program oversight of cybersecurity integration into all aspects of FAA's missions.

Chapter 3

Conclusion 3-1: The FAA would benefit from engaging more robustly with recruitment fairs and college programs to bolster the hiring pipeline for cybersecurity positions.

Conclusion 3-2: "Early interest" is a notion that can be identified and then leveraged in recruitment. In the case of the FAA, this includes not just an early interest in aviation, but also an early interest in cyber.

Conclusion 3-3: Long-term university partnerships using such activities as scholars-in-residence and fellowships from the FAA might enhance the agency's ability to recruit talented recent college graduates.

Conclusion 3-4: In the case of the FAA, there is a lack of clarity around what the marketing and branding are for promoting cybersecurity occupations; and there is a need for further identifying what the FAA could do to promote itself as an attractive/fulfilling/rewarding place for cybersecurity work.

Conclusion 3-5: The committee concludes that the use of numerical targets, such as number of SFS program graduates recruited and/or hired to internships and permanent employment, would be a useful mechanism for engaging additional interns with this program.

Conclusion 3-6: An optimal way of improving the cyber workforce involves hiring employees with the right skillset and then reskilling them as the job requirements change. Two promising options for improving the cyber workforce in this way include programs like the Scholarship for Service program or reskilling current employees.

Chapter 4

Conclusion 4-1: It is critical that the FAA develop strategies to ensure that specialized knowledge related to the FAA mission and operation is captured and transferred effectively to new employees.

Recommendations

Chapter 2

Recommendation 2-1: The cybersecurity workforce within the FAA is generally satisfied and dedicated to the agency's mission. The FAA's high employee retention rate in cybersecurity has helped it maintain the needed workforce capacity and capability, but with a growing proportion of the cybersecurity workforce of the FAA reaching retirement eligibility, the agency is vulnerable to losing a significant portion of its cybersecurity workforce to retirement. However, in the event of widespread retirement, the FAA will likely find it very challenging to restore/rebuild its workforce given its current challenges with recruitment. And thus, the FAA should implement cybersecurity workforce planning strategies that will protect the agency against the potential for sudden and mass retirements.

Recommendation 2-2: Workforce diversity also strengthens the performance of cybersecurity efforts. The FAA should expand recruitment efforts to include potential hires from different science, technology, engineering and mathematics backgrounds and careers.

Recommendation 2-3: The FAA's ability to hire cybersecurity workers is constrained by citizenship and security clearance requirements. Moreover, the FAA is currently under-utilizing flexibilities in personnel management and hiring authority, such as direct-hire authority The FAA should compare and contrast flexibility with other federal programs in terms of hiring, to identify other agency flexibilities and practices that could be incorporated into FAA hiring.

Recommendation 2-4: The FAA should compare flexibility with other federal programs in terms of hiring, to identify other agency flexibilities and practices that could be incorporated into FAA hiring.

Chapter 3

Recommendation 3-1: The FAA should evaluate the use of existing and future internship programs as valuable tools to create a more diverse cybersecurity workforce.

Recommendation 3-2: At the organizational level, promoting and marketing the agency as an attractive/fulfilling/rewarding place for cybersecurity would facilitate recruiting. However, there is a lack of clarity on what the FAA's current marketing strategy and branding are for cybersecurity. While any FAA marketing approach needs to conform with the larger context of the brand of the federal government, actions to develop a strong FAA-specific marketing presence in cybersecurity should be implemented. To do so, the FAA should identify priority targets for recruitment (and identify their characteristics) and tailor their marketing to reach those targets effectively.

Recommendation 3-3: The FAA would benefit from engaging more robustly with recruitment fairs and college programs to bolster the hiring pipeline for cybersecurity positions. Moreover, long-term university partnerships using such activities as scholars-in-residence from the FAA might enhance the FAA's ability to recruit talented recent college graduates. The FAA should organize and expand its reach and partnerships with universities around cybersecurity preparation efforts in academic and research areas to assist in the development of a talented cybersecurity workforce. Among these partnerships, the FAA should explore opportunities to develop meaningful and sustainable relationships with Minority Serving Institutions to access up-coming cybersecurity graduates via internships and employment opportunities.

Continued on next page

Chapter 3

Recommendation 3-4: Hiring employees with the right skillset and then growing them as the job requirements change is optimal. This is possible through programs like the Scholarship for Service (SFS) program or reskilling current employees, which are two approaches for improving the cyber workforce. So far, the FAA has not partnered with the SFS program to effectively recruit cyber talent to the organization; this is a missed opportunity and a partnership should be pursued. In this and other ways, the FAA should explore a wide range of options for meeting future reskilling needs, including internal, outside commercial, industry conference workshops, and outside rotations in agencies and industry.

Recommendation 3-5: Reskilling the existing workforce can be an important component of developing the needed future cybersecurity workforce for the FAA and over time worker reskilling should grow beyond technical skills to include managerial and operational skills.

Recommendation 3-6: The FAA should continue to use the NICE tool to develop work roles that fit into a larger, well-designed organizational structure.

Recommendation 3-7: The FAA should train its cyber leadership on best practices in building a diverse and inclusive organizational culture and should customize these best practices to implement a more contemporary culture.

Continued on next page

Chapter 3

Recommendation 3-8: When comparing non-salary monetary incentives, the FAA cannot compete with industry pay scales. The FAA should leverage non-salary monetary incentives (career development reimbursements, performance bonuses, etc.) as part of the overall compensation package.

Recommendation 3-9: “Early interest” in cybersecurity and in aviation by young students is a notion that can be identified and then leveraged in FAA recruitment. Two targeted actions are recommended here to foster and capitalize on FAA related “early interest”:

- The FAA should review its past experience with effective fellowship and internship programs and also look to other federal agencies for proven models, such as the DoD SMART scholarship program.
- The FAA should sponsor and leverage postsecondary-level cyber competitions.

Chapter 4

Recommendation 4-1: The FAA should monitor, and revise if necessary, its personnel practices to support the development of the necessary skills to meet the ever-changing demand in the current and future cybersecurity workforce.

Recommendation 4-2: The FAA should provide professional development opportunities to refresh skill sets of current cybersecurity employees and ensure sharing of key institutional and mission-specific knowledge with newer cybersecurity staff.

Recommendation 4-3: The FAA cybersecurity employees and the cybersecurity program as a whole will benefit from a CISO that can develop a comprehensive cybersecurity strategy that crosses multiple complex domains in the FAA. The CISO's reporting structure needs to support a strong governance model, which ensures that the CISO has both the independence and the access required to effectively manage the FAA's cyber risk posture. In support of such leadership responsibility, the FAA should position the CISO role at the most senior level of the non-political appointees within the organization. Given the scarcity of qualified people, the FAA should consider variances from current pay-scale limitations in order to be a competitive employer.

Continued on next page

Chapter 4

Recommendation 4-4: Employee retirement, at the end of the lifecycle model, offers organizations the opportunity to rethink organizational needs and required skillsets, which in turn helps refocus talent recruitment and the next iteration of the employee lifecycle. The FAA should ensure that all efforts to upskill and evolve the cyber workforce include the agency's risk management, cybersecurity compliance, and independent assurance capabilities alike.

Recommendation 4-5: The FAA should enable the success of the cybersecurity program and the CISO by designing a hybrid organizational model leveraging private sector best practices such as blending core and edge (vertically integrated) functions as well as the plan, build, operate model.