December 3, 2021

The Honorable Maria Cantwell
Chair
Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC  20510

Dear Chair Cantwell:

This letter accompanies the Federal Aviation Administration’s (FAA) report to Congress on the progress in meeting the requirements of Section 549 of the FAA Reauthorization Act of 2018, Public Law 115-254 (the Act).

Section 549 of the Act directs FAA to submit a report describing the results of a study performed by the National Academy of Sciences, Study on Cybersecurity Workforce of FAA. The study focused on the cybersecurity workforce at FAA to make recommendations to increase the size, quality, and diversity of the cybersecurity workforce.

Safety is the foundation of our mission at the Department of Transportation (DOT) and this Administration has recognized the growing importance of cybersecurity in maintaining and increasing the safety our nation’s infrastructure, including the national airspace system. DOT and FAA remain committed to increasing diversity across our workforce. The FAA will use all of its federal recruiting, hiring and retention capabilities to continue building and retaining the FAA cybersecurity workforce.

A similar response has been sent to the Ranking Member of the Senate Committee on Commerce, Science, and Transportation and the Chair and Ranking Member of the House Committee on Transportation and Infrastructure.

Sincerely,

Steve Dickson
Administrator

Enclosure
December 3, 2021

The Honorable Roger F. Wicker
Ranking Member
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC  20510

Dear Ranking Member Wicker:

This letter accompanies the Federal Aviation Administration’s (FAA) report to Congress on the progress in meeting the requirements of Section 549 of the FAA Reauthorization Act of 2018, Public Law 115-254 (the Act).

Section 549 of the Act directs FAA to submit a report describing the results of a study performed by the National Academy of Sciences, Study on Cybersecurity Workforce of FAA. The study focused on the cybersecurity workforce at FAA to make recommendations to increase the size, quality, and diversity of the cybersecurity workforce.

Safety is the foundation of our mission at the Department of Transportation (DOT) and this Administration has recognized the growing importance of cybersecurity in maintaining and increasing the safety our nation’s infrastructure, including the national airspace system. DOT and FAA remain committed to increasing diversity across our workforce. The FAA will use all of its federal recruiting, hiring and retention capabilities to continue building and retaining the FAA cybersecurity workforce.

A similar response has been sent to the Chair of the Senate Committee on Commerce, Science, and Transportation and the Chair and Ranking Member of the House Committee on Transportation and Infrastructure.

Sincerely,

Steve Dickson
Administrator

Enclosure
December 3, 2021

The Honorable Peter A. DeFazio  
Chair  
Committee on Transportation and Infrastructure  
House of Representatives  
Washington, DC  20515

Dear Chair DeFazio:

This letter accompanies the Federal Aviation Administration’s (FAA) report to Congress on the progress in meeting the requirements of Section 549 of the FAA Reauthorization Act of 2018, Public Law 115-254 (the Act).

Section 549 of the Act directs FAA to submit a report describing the results of a study performed by the National Academy of Sciences, Study on Cybersecurity Workforce of FAA. The study focused on the cybersecurity workforce at FAA to make recommendations to increase the size, quality, and diversity of the cybersecurity workforce.

Safety is the foundation of our mission at the Department of Transportation (DOT) and this Administration has recognized the growing importance of cybersecurity in maintaining and increasing the safety our nation’s infrastructure, including the national airspace system. DOT and FAA remain committed to increasing diversity across our workforce. The FAA will use all of its federal recruiting, hiring and retention capabilities to continue building and retaining the FAA cybersecurity workforce.

A similar response has been sent to the Ranking Member of the House Committee on Transportation and Infrastructure and the Chair and Ranking Member of the Senate Committee on Commerce, Science, and Transportation.

Sincerely,

Steve Dickson  
Administrator

Enclosure
December 3, 2021

The Honorable Sam Graves  
Ranking Member  
Committee on Transportation and Infrastructure  
House of Representatives  
Washington, DC  20515

Dear Ranking Member Graves:

This letter accompanies the Federal Aviation Administration’s (FAA) report to Congress on the progress in meeting the requirements of Section 549 of the FAA Reauthorization Act of 2018, Public Law 115-254 (the Act).

Section 549 of the Act directs FAA to submit a report describing the results of a study performed by the National Academy of Sciences, Study on Cybersecurity Workforce of FAA. The study focused on the cybersecurity workforce at FAA to make recommendations to increase the size, quality, and diversity of the cybersecurity workforce.

Safety is the foundation of our mission at the Department of Transportation (DOT) and this Administration has recognized the growing importance of cybersecurity in maintaining and increasing the safety our nation’s infrastructure, including the national airspace system. DOT and FAA remain committed to increasing diversity across our workforce. The FAA will use all of its federal recruiting, hiring and retention capabilities to continue building and retaining the FAA cybersecurity workforce.

A similar response has been sent to the Chair of the House Committee on Transportation and Infrastructure and the Chair and Ranking Member of the Senate Committee on Commerce, Science, and Transportation.

Sincerely,

Steve Dickson  
Administrator

Enclosure
REPORT TO CONGRESS:

The FAA’s Report Regarding the Results of a Study by the National Academy of Sciences: “Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration”

Federal Aviation Administration Reauthorization Act of 2018, PL 115-254, SEC. 549
Introduction

Section 549 of the FAA Reauthorization Act of 2018, Public Law 115-254 (the Act) required the Federal Aviation Administration (FAA) Administrator to enter into an agreement with the National Academy of Sciences (NAS) to conduct a study on FAA’s cybersecurity workforce. The Act directed the investigation to culminate in recommendations to increase the cybersecurity workforce’s size, quality, and diversity, including cybersecurity researchers and specialists. Additionally, within 180 days of the completion of the study, the FAA Administrator is required to submit a report to the appropriate congressional committees summarizing the study results.

The FAA received the pre-publication copy of the NAS study on June 7, 2021. The NAS organization made the report available for public consumption two weeks later on June 21, 2021. The complete study is accessible online at the National Academies website.

The Study

In September 2019, the FAA entered into a contractual agreement with the NAS. The Statement of Tasks further refines the scope of the study and subsequent recommendations. Of note, a committee of experts sanctioned by the NAS (the Committee) would review:

- The current and future cybersecurity landscape for the FAA;
- Statutory, regulatory, and other institutional constraints on recruitment flexibilities, hiring, retention, and compensation of cybersecurity workers; and
- The U.S. labor market in cybersecurity expertise and competition for qualified candidates.

Representatives from across the agency participated in the study, including the FAA’s Cybersecurity Steering Committee, FAA’s Office of Human Resources, and FAA’s Office of Information and Technology. The Committee held several public sessions which FAA representatives attended and, in many cases, provided presentations to the Committee. After the study, additional FAA offices engaged to review the results and assist in developing the FAA’s strategy and response. Critical stakeholders in the post-publication review include the FAA’s Office of Communications and the FAA’s Office of the Chief Counsel.

The FAA’s Efforts Related to NAS Recommendations

The NAS study, titled "Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration," culminated in several recommendations made by the Committee. The study also provided a comprehensive list of findings, conclusions, agency challenges, and agency opportunities to further develop the cybersecurity workforce.

---

2 https://www.nationalacademies.org/our-work/cybersecurity-workforce-of-the-federal-aviation-administration#sectionCommittee
The NAS study's recommendations to address challenges, include meeting the requirement of new cybersecurity skills and capabilities to secure new and emerging technologies in an ever-evolving threat landscape, addressing the challenges of recruiting and retaining diverse cybersecurity talent in a highly competitive global labor market, and the need to ensure cybersecurity is continuously represented in the enterprise.

FAA then used the NAS study's recommendations to form the basis for six strategic outcomes. To achieve these outcomes, the FAA will leverage the opportunities identified in the NAS study to strengthen its cyber workforce by enhancing recruiting and the talent pipeline, increasing diversity, ensuring the cybersecurity organization is designed for effectiveness, and preparing for a retirement wave in the FAA's current cyber workforce.

The FAA has extended its agreement with NAS through the second quarter of the Fiscal Year 2022 to ensure continued guidance and gain clarity where appropriate and applicable.

**Outcome 1: Develop or expand partnerships to foster opportunities for details, rotational assignments, or "exchange programs" to expose potential, new, and existing talent to multiple cybersecurity functions at the FAA.**

The FAA has an existing set of leadership development programs that enable staff growth and development, including detailed assignments across the agency. The FAA will continue to leverage these programs for leadership development, including the Aspiring Managers Program (formerly - Program for Emerging Leaders), Emerging Enterprise Leaders Program (formerly - Senior Leadership Development Program), FAA Leadership and Learning Institute, and numerous Line of Business / Staff Office leadership development programs. In addition, the FAA regularly engages employees at all levels, in detailed assignments to other parts of the agency and even outside the agency. The FAA will continue to expand these internal rotational assignments or details within FAA and across the U.S. Department of Transportation (DOT) to provide employees with increased exposure to new roles and functions. Based on the study's recommendations, the FAA is considering several new initiatives to develop and create opportunities to expose employees to different cybersecurity functions. These efforts focus on cultivating and expanding industry and inter-agency relationships to provide additional exposure to novel cyber approaches applied in other agencies or industries. The FAA is also considering implementation of training initiatives providing current staff with opportunities to pursue additional cyber-focused training and education. Additionally, the FAA is reviewing its authorities to provide potential new staff with recruitment incentives. These efforts will provide FAA with effective recruitment and retention tools.
Outcome 2: Identify and promote opportunities for training and knowledge sharing - including best practices and lessons learned - to enhance the effectiveness of the cybersecurity workforce throughout the employee lifecycle.

Knowledge sharing is a crucial element to a successful cybersecurity workforce. The NAS study's recommendations and findings reinforced this concept. The FAA has already embarked on initiatives to increase information sharing through peer engagement and more formalized training platforms. The FAA will continue its engagement with Information Sharing and Analysis Centers for peer information exchange and collaboration and will look to enhance these engagements with the addition of cyber research presentations from academia, industry, and federally-funded research and development centers.

The FAA will internally promote its existing partnership with a third-party provider deploying a cyber-specific training platform. This platform provides FAA personnel access to training courses, virtual labs, assessments, and practice tests for cyber-related certifications.

The FAA has also identified potential new undertakings based on the study's findings. One area under consideration is establishing a formal cybersecurity mentor program that will bring employees together on a paired or small group basis to provide an environment conducive to formal and informal knowledge sharing. In addition, the FAA will explore establishing standard inter-agency and intra-agency site visits for cyber employees to increase exposure to new and different ideas, approaches, and areas of cybersecurity. These engagements would foster the exchange of information from other organizations and diverse internal teams.

Outcome 3: Develop and implement a "One-FAA" approach for cybersecurity workforce development.

The FAA has embraced the National Initiative for Cybersecurity Education (NICE) framework as a cornerstone element of its cyber workforce strategic planning and development. This is an essential step in creating a consistent agency-wide "One-FAA" approach for cybersecurity workforce development. It also helps the FAA identify the key cybersecurity knowledge, skills, and abilities that the current workforce has, and areas where opportunities for improvement exist to meet the cybersecurity needs of today and the challenges of tomorrow. The FAA will continue to leverage the NICE framework, and complimentary cybersecurity job codes from the U.S. Office of Personnel Management (OPM), in its cybersecurity workforce strategic planning.

Identifying the capabilities needed to meet future cyber challenges will be a key component to developing the FAA’s plan to attract, design, and retain its cyber workforce. In support of this need, the FAA recognizes the value of exploring initiatives that will support this effort across the agency. The FAA will explore opportunities to develop cybersecurity "career maps" that incorporate necessary skillsets, training, certifications, etc. The "career maps" will provide both a consistent mechanism for the placement of new employees and a growth path for existing employees. The information provided in these documents would serve as reference only and not necessarily guarantee an employee's promotion or placement in the agency. The FAA agrees that cybersecurity awareness and skill sets are not limited to front-line employees – executives and acquisitions personnel may need to be included in cyber workforce development activities as well.
Outcome 4: Review hiring and personnel management authorities afforded to cybersecurity recruits and employees, reduce or remove barriers for adoption, and educate employees and supervisors on the critical components of each available source.

The FAA faces a challenging cybersecurity labor market, similar to many other organizations seeking to hire and retain cyber personnel. As the study noted, there are many programs in place in the federal government to accelerate and simplify the cybersecurity hiring process. The FAA currently leverages some federal hiring and personnel management authorities afforded to cyber-specific employees, such as on-the-spot hiring. As the study recommended, the FAA will look to expand this practice and identify additional programs that may currently be underutilized.

The FAA will look at potential changes to current practices to create additional agility to recruit and retain cyber employees. One such approach the FAA may consider is the potential designation of cybersecurity positions as mission-critical. This could enable changes in geographic location limitations or requirements, phased retirement policies, and pay scales. The FAA also will consider reviewing authorities to reward employees for obtaining and maintaining relevant cybersecurity certifications or holding memberships in industry associations. The FAA will ensure managers and employees are aware of the available programs.

Outcome 5: Develop and expand FAA recruitment efforts and programs to attract qualified cybersecurity experts.

The FAA recognizes the importance of recruiting efforts to attract a diverse pool of qualified employees. The agency’s current initiatives include cybersecurity as part of a broader aviation-focused engagement. In the FAA’s Science, Technology, Engineering, and Math (STEM) Aviation and Space Education program, youth from diverse backgrounds are inspired to pursue aerospace careers. The program seeks to create a consistent pipeline of aerospace professionals for the workforce of the future. The FAA will look to expand the presence of cybersecurity specialties within this program. Engagement with older students, closer to entering the workforce, is accomplished through several internship programs. One example is the Gateways Internship Program, which primarily focuses on STEM field internships, including cybersecurity-related positions. Cybersecurity leadership has leveraged these programs to recruit cyber personnel in the past, and they offer ample opportunity to expand the cyber talent pipeline in the future. Participants receive both planned training and on-job training during their internship and usually progress to higher-level positions.

Another critical part of recruiting is establishing "brand awareness," to this end, the FAA regularly participates in industry-sponsored cybersecurity training and awareness events, such as Black Hat³ and DEF CON⁴. The agency’s participation promotes awareness of the FAA’s unique mission, and the FAA will continue these types of marketing efforts to further increase awareness of FAA cybersecurity career opportunities.

³ https://www.blackhat.com/
⁴ https://defcon.org/
The FAA agrees with the NAS study's recommendations around capitalizing on the unique mission and marketing the agency as a cybersecurity career destination. The FAA will explore further engagement with OPM to identify additional incentives and flexibility programs that may strengthen cybersecurity recruiting efforts at all levels. The FAA will also consider developing a cybersecurity "roadshow" to actively recruit for cyber positions within FAA. The agency will also evaluate the potential to sponsor cyber competitions with an aviation cyber focus, helping to build awareness of the FAA as a cyber-employer, expose cyber experts to the aviation context, and ignite interest in an aviation cyber-focused career.

**Outcome 6: Ensure the most effective organizational design, structure, and influence for the cybersecurity organization.**

The study highlighted the importance of a well-designed, properly positioned, and influential cybersecurity organization structure. The FAA has taken several steps to position cybersecurity in the enterprise and establish the strategic importance of the cybersecurity workforce. In 2014, the FAA chartered the Cybersecurity Steering Committee (CSC) to create an executive-level governance body that promotes an enterprise cybersecurity approach. Soon after, the FAA created the Cybersecurity Strategy, which is updated regularly by FAA Leadership. One goal within FAA’s Cybersecurity Strategy focuses exclusively on building and maintaining the cybersecurity workforce at the agency. The FAA has also leveraged the NICE framework and identified and classified cybersecurity roles across the agency with plans to explore potential enhancements to the process to enable continuous updates and handle changes from an employee's initial assignment.

The study noted, and reflected in its recommendations, that the cybersecurity organization is being elevated in many organizations. This reflects the increasing importance of cybersecurity as a mission enabler for nearly all entities across the private and public sectors. The FAA has elevated cybersecurity at executive and leadership levels and has cross-agency representation on the CSC. The FAA will engage with appropriate industry experts to ensure best practices in terms of organizational design.

**Summary**

The FAA recognizes that even the near future holds many challenges for the cybersecurity workforce, including a tight global labor market. The increasing digital footprint of the FAA increases the need for robust cybersecurity. Workforce diversity and recruitment must be increased to meet this need and compensate for a future wave of retirements in the current workforce. The challenges identified in the study, along with opportunities and recommendations, have validated existing FAA cyber workforce initiatives and inspired potential new initiatives. Through the six strategic outcomes, continued investment in existing initiatives, and promoting new programs developed as a result of this study, the FAA will strengthen its cybersecurity workforce today and in the future. The FAA thanks the NAS Committee for its comprehensive analysis, identification of challenges, opportunities, and compelling recommendations reflected in the study.