SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

"Nomination of Mr. David P. Pekoske, to be Administrator of the Transportation Security Administration, Department of Homeland Security"

10:00 AM, July 13, 2022

MINORITY QFRs

Questions for the Record from by Ranking Member Wicker To Administrator Pekoske

Question 1*: Senator Fischer and I introduced the TSA Security Threat Assessment Application Modernization Act, which would streamline the enrollment process for those working in freight transportation that are seeking a combination of the TWIC, HME and/or PreCheck credential, which each use the same Security Threat Assessment. Will you work with me on this legislation to help streamline that process for key freight transportation stakeholders?*

Answer: Yes. TSA supports the intent of S. 4298, "TSA Security Threat Assessment Application Modernization Act," which is to streamline the enrollment and renewal process for individuals requiring more than one TSA Security Threat Assessment (STA) and welcomes the opportunity to work with you and your staffs to achieve that goal.

TSA has implemented and plans to continue deploying new capabilities aligned to the draft legislation's objective that will reduce the cost and time burden on drivers and transportation workers. For instance, HME and TWIC holders eligible for the TSA PreCheck® Application Program may obtain expedited security screening using the identification number on their CDL or TWIC in the appropriate Known Traveler Number field in making their airline reservations. Additionally, applicants requiring both a TWIC and HME are encouraged to enroll for the TWIC and then use the TWIC to get a free or reduced cost HME. Currently, states have the authority to provide the HME on a state-issued CDL using a valid TWIC at no additional cost, but not all states are currently using this authority. Finally, TSA offers applicants a fully online enrollment capability to obtain a reduced cost HME, if they have undergone a comparable STA, such as the one performed for TWIC. Some states do not support this capability as they do not use TSA's enrollment provider or it requires development to allow the state to align expiration dates.

TSA will provide recommendations to improve HME and TWIC comparability and reciprocity for applicants in all states. The recommendations will include requirements for states to validate the TWIC for HME issuance as well as the sharing of biometric information to reduce the burden of issuing TWIC to applicants in states that do not use TSA's enrollment provider.

Questions for the Record from Senator Blackburn to Administrator Pekoske

Question 1: *In 2018, Congress passed the TSA Modernization Act, which required TSA to expand the PreCheck program to provide either secure end-to-end mobile enrollment or a biographic vetting enrollment alternative to in-person fingerprints. Why, in 2020, did TSA enter into agreements that did not include secure mobile end-to-end enrollment?*

Answer: TSA included the requirement for companies to have a start-to-finish secure online or mobile enrollment capability in the Other Transaction Agreement (OTA) Statement of Work (SOW) that defines TSA's requirements of the enrollment providers. In the SOW, TSA defined mobile enrollment as "the ability to enroll with equipment that is portable and can be moved to meet customer demand and location preferences (e.g., tablets, kiosks, etc.)." This definition is consistent with how both the FBI and NIST define mobile fingerprint capture devices (e.g., mobile devices on the FBI Certified Products List are able to be easily moved from place to place). All new providers plan to offer mobile enrollment options (e.g., tablets, kiosks etc.).

In addition, following feedback from Congress, TSA has worked closely with the FBI and NIST to find a path forward for a start-to-finish secure remote enrollment capability that would allow customers to complete the entire enrollment process from the comfort of their home using contactless fingerprint capture. As of today, both NIST and the FBI have identified significant technical challenges which must be overcome before considering the use of contactless fingerprints captured on currently available contactless fingerprint technology. Additionally, the FBI stated remote biometric collection, without in-person verification and monitoring, introduces unnecessary risk into the American aviation transportation system and the FBI's national criminal history fingerprint repository. The National Crime Prevention and Privacy Compact Council similarly voiced concerns noting the security of remote contactless fingerprinting goes against the Council's guidance for agencies and contractors to develop polices, practices, and procedures for identity verification prior to submitting fingerprints for noncriminal justice purposes.

Regarding vetting of an applicant by means other than biometrics, as required by Section 1937 of the TSA Modernization Act, TSA conducted a thorough analysis of private sector solutions. TSA published a Request for Capabilities to determine if any existing solution could overcome known shortcomings regarding biographic-based vetting. TSA determined that all proposed solutions did not meet the Section 1937 requirement that the vetting be "as effective as a fingerprint-based criminal history records check conducted through the Federal Bureau of Investigation."

Question 2: *With the OTA PreCheck Enrollment Providers expected to soon begin enrolling operations, how does TSA plan to protect the privacy of its customers and ensure their personal data is not sold or made available to third parties for unauthorized uses?*

Answer: As mandated by the TSA Modernization Act of 2018, each enrollment provider's OTA and its Statement of Work (SOW) require the protection of privacy and

data, including any personally identifiable information, in a manner consistent with Privacy Act of 1974 and TSA's regulations. Additionally, the OTA and OTA's SOW applies this requirement to any design, development, or operation of any system of records on individuals covered by the OTA to include a Privacy Act notification in the enrollment provider's OTA and any subcontract.
The SOW, which all vendors must adhere to, specifies that enrollment providers are not permitted to use applicant data for any purpose other than submission to TSA unless the enrollment provider obtains express permission from TSA, as well as from each individual applicant after completion of the TSA PreCheck enrollment process.

All concepts that require using applicant data for purposes outside of submission to TSA require written approval from TSA. TSA will prohibit enrollment providers from establishing partnerships that include selling any data of individuals obtained during the application process. Additionally, the enrollment provider must segregate TSA data from other data used to provide additional purposes/benefits to the applicant.

Additionally, the SOW specifically states, "In the event of violations of the Privacy Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Offeror is considered to be an employee of the agency." As such, if the enrollment providers violate the Privacy Act, criminal penalties may be imposed.

In addition, TSA is protecting applicant data from cybersecurity threats by requiring that enrollment providers' systems meet a FIPS 199 level of High/High/High. FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing information systems. Systems are rated based on confidentiality, integrity, and availability. The enrollment provider systems must meet the highest standards of confidentiality, integrity, and availability before TSA will allow the enrollment providers to begin enrollment operations.

Question 3: *Current law allows for the immediate termination of employees that intentionally allow guns, knives, or explosives through a checkpoint. Under Title 5, could that employee remain on the TSA payroll?*

Answer: Title 5 provides procedures for employee discipline, including terminations. Moving under Title 5 will not impact TSA's ability to address misconduct and implement appropriate administrative action.

Question 4: *Right now, TSA has the flexibility to move screeners between checkpoints to alleviate long lines and ensure security. Could Title 5 restrict that flexibility?*

Answer: Under Title 5 issues regarding the movement of Transportation Security Officers (TSOs) between checkpoints could be subject to collective bargaining and part of an agreement negotiated between TSA and the union representing TSOs.

Questions for the Record from Senator Young to Administrator Pekoske

Question: *TSA Precheck is already offered to active duty, reserves, and National Guard service members at no cost. The Veterans Expedited TSA Screening (VETS) Safe Travel Act will expand this program to include veterans who are amputees, paralyzed, or blind. There are approximately 70,000 amputee veterans, 100,000 paralyzed, and 130,000 blind veterans in the United States currently. Do you support the VETS Safe Travel Act and will you commit to swift implementation if it is signed into law?*

Answer: As a veteran of the United States Coast Guard and an ardent supporter of our nation's armed forces, I strongly support efforts to provide enhanced passenger experiences to disabled veterans. I welcome your effort to provide TSA PreCheck status to qualify disabled veterans at no-cost and look forward to working with you to ensure that TSA can swiftly implement this effort if passed into law.

At TSA, we have sought to ease the travel of disabled veterans through domestic airports by vetting these individuals as part of the TSA PreCheck Application Program. TSA has coordinated with the Department of Veterans Affairs to ensure that TSA can identify these individuals so that they can enroll in TSA PreCheck at no cost. Currently, TSA offers two services for travelers with disabilities and medical conditions. First, TSA Cares is a helpline that provides travelers with disabilities, medical conditions, and other special circumstances additional assistance during the security screening process. Travelers may request assistance through the TSA screening checkpoint by calling (855) 787-2227 or completing the form at https://www.tsa.gov/contact-center/form/cares. Travelers should contact TSA Cares 72 hours prior to traveling with questions about screening policies, procedures, and what to expect at the security checkpoint.

Second, the Passenger Support Specialist (PSS) Program, which consists of experienced TSOs who receive additional training to assist and screen travelers with disabilities and medical conditions. PSSs offer real-time, on-the-spot support to travelers at the checkpoints. As of April 1, 2022, 7500 TSOs have taken the updated training to be certified as a PSS.

Finally, TSA currently provides TSA PreCheck to all active military, reserve, and National Guard at no cost. Similarly, all Department of Defense federal employees can opt-in to receive TSA PreCheck at no cost. TSA relies on ongoing background checks conducted by the Department of Defense to ensure these individuals are low-risk and therefore eligible for TSA PreCheck screening. When service members or federal employees retire, Department of Defense no longer conducts ongoing background checks on these individuals. As such, TSA would require veterans to enroll in our TSA PreCheck Application Program to undergo a security threat assessment.

Questions for the Record from Senator Lee to Administrator Pekoske

Question 1: *On June 16, 2022, President Biden signed the Ocean Shipping Reform Act (OSRA) into law. I authored Section 23 of OSRA, which requires the TSA and Coast Guard to jointly prioritize and expedite the consideration of applications for a Transportation Worker Identification Credential that are to provide direct assistance to a United States Port. Could you provide me with an update on what specific steps the TSA is taking to work with the Coast Guard to implement this newly enacted provision?*

Answer: TSA appreciates the Ocean Shipping Reform Act's objective to strengthen the U.S. maritime supply chain and recognizes the importance of transportation workers to U.S. critical infrastructure and supply chain operations. The Transportation Worker Identification Credential (TWIC®) is required for all individuals who need unescorted access to secure areas of U.S. ports regulated under the Maritime Transportation Security Act (MTSA) of 2002. TSA requires all TWIC applicants to acknowledge, during the enrollment process, that they are required to have such unescorted access to ports and vessels.

TSA is prioritizing the adjudication and credential issuance for eligible TWIC applicants. For example, TSA is adjudicating applications for the TWIC Program ahead of applicants for traveler programs, such as the TSA PreCheck® Application Program, and has expanded the days and hours of operation for its card production services to reduce the time required to produce and ship the physical TWIC card to approved applicants. TSA recognizes that some ports may require expanded enrollment services to facilitate increased demand for TWIC and is working with them to better understand and meet their TWIC requirements. For instance, in fiscal year 2022, TSA successfully hosted two temporary TWIC enrollment events at the Port of Long Beach, California.

Question 2: *Since 2014 the DHS Office of Inspector General (OIG) has covertly audited and inspected the security related aspects of TSA several times. The OIG's findings have historically revealed some very alarming fail rates due to both human and technology-based failures. In February 2019, during your tenure, the OIG again found "vulnerabilities with various airport access control points and associated access control procedures."*[1]

When I last questioned TSA in Fall 2019, the six recommendations made by the IG were still open. Since this time have those recommendations been closed?

Answer: Five of the six recommendations from OIG-19-21 Covert Testing of Access Controls to Airport Secure Areas are closed. One recommendation, which involves training for airport workers and Transportation Security Officers (TSOs), remains open with an expected closure date of October 31, 2023.

[1] February 13, 2019, DHS OIG Highlights: Covert Testing of Access Controls to Airport Secure Areas, Unclassified Summary; https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-21-Feb19.pdf

Has the TSA or the OIG conducted any covert audits and inspections of the security related aspects of TSA since the beginning of the COVID-19 pandemic in March 2020 to ensure continued progress in closing vulnerabilities? If not, why not?

Answer: OIG's current Covert Testing Audit on the effectiveness of TSA's Checked Baggage Screening was announced in March 2020, but postponed due to COVID-19. OIG conducted this audit between June 2021 thru July 2022. The draft report was issued on July 1, 2022 and contains three recommendations for TSA to revise the standard operation procedures (SOPS), increase testing, and accelerate the development of a test kit which was also recommended in a 2014 OIG report. TSA plans to concur with those recommendations and is preparing a formal agency response, which is due to OIG by August 4, 2022.

Additionally, TSA re-initiated covert testing during the pandemic (August 2020), which included checkpoint screening, checked baggage, identity management, and airport employee access control, among other areas. The findings from that testing were used to drive improvements to training, procedures, and technology.

For many years, we've had alarming reports from the OIG's security related audits. How during your tenure have you sought to reverse this negative trajectory? And what is your current overall strategy for the TSA to improve these outcomes should you be reconfirmed to your position?

Answer: TSA's Inspection function, which executes its own covert testing program, works closely with the OIG on covert testing. While TSA uses insights from the OIG to identify needed areas of improvement, I have also expanded TSA efforts during my tenure to conduct covert testing to measure the TSA screening effectiveness over time in order to better understand how improvements in technology, process and training impact security (Index) outcomes. I have also expanded the program to test with our international partners both to support one-stop security agreements and to improve overall aviation security globally. For instance, during July 2022 alone we are conducting joint testing with the Republic of Korea, Israeli Aviation Security, the German Federal Police, the United Kingdom, and providing covert testing instruction to the Kenyan aviation security authority.

Questions 3: *The TSA Modernization Act made several updates to the Screening Partnership Program (SPP) – a program which allows passenger screening to be carried out by qualified private screening companies. One update was to require TSA to encourage participating SPP airports to recommend innovative ideas to TSA on screening approaches, technological ideas, etc.*

Since the adoption of the TSA Modernization Act, how has TSA encouraged innovation from SPP airports? Has TSA implemented any ideas presented by an SPP airport?

Answer: SPP Contractors have always been welcome to discuss innovation ideas with the SPP Program Office and/or Federal Security Director. Additional avenues to present suggestions for innovations include:

- Section H.7 of the SPP IDIQ contract provides information regarding how contractors through the Idea Factory can submit and share ideas and solutions that may result in the creation of programs or initiatives, or changes to security screening procedures.
- Annual SPP Vendor Forums provide contractors an opportunity to discuss innovations that would enhance the TSA security screening operation.

At this time, the SPP Program has not received any innovation suggestions or ideas from SPP airports that have been implemented.

Question 4: *As you know, since 2016, new TSOs now receive centralized training at the TSA Academy located at the Federal Law Enforcement Training Center in Georgia. During your nomination hearing you mentioned that the current two-week training would soon be extended to three weeks.*

What benefits does the TSA seek with centralizing TSO training in Georgia?

Answer: TSO training at the TSA Academy results in operational efficiency through the centralization and standardization of coursework. Students receive uniform content, delivered consistently by the agency's best instructors in a setting with access to the newest technology and state-of-the-art training labs. Training quality is constantly monitored, evaluated, and improved, and the content can be quickly adjusted in response to threats or shifts in operational priority.

Since TSA centralized its basic training in Georgia, has that increased or decreased the expenses associated with TSO training?

Answer: TSA initially centralized basic training in 2016 and a cost study performed in 2018 showed an increase in overall costs by 14%. However, the benefits of a consistent, centralized basic training and initial federal service indoctrination for new employees far exceed the additional marginal costs. Since the centralization of new hire training, associated per student costs have generally remained static.

A 2018 GAO report noted that TSA had not identified performance goals or measures to assess the benefits of the TSO Basic Program.[2] *Since the report was issued, has TSA taken steps to identify the metrics to assess the program's effectiveness? If so, which metrics have been employed and has TSA published any conclusions on the effectiveness of this training model?*

Answer: TSA has taken a number of steps to assess the benefits of the TSO Basic Training Program (TSO-BTP). TSA developed a comprehensive Training Evaluation Plan that identifies reporting timeframes for instruments and areas of comparison throughout the TSO-BTP process. This information will provide TSA Management and

[2] July 2018, Aviation Security: Basic Training Program for Transportation Security Officers Would Benefit from Performance Goals and Measures, Government Accountability Office; https://www.gao.gov/assets/gao-18-552.pdf

Course Managers with data regarding the effectiveness of the training as well as areas for improvement and requiring updates. The plan uses the industry-standard Kirkpatrick Method that identifies the Level 1, 2, and 3 measurement instruments for TSO-BTP at and beyond TSA-A.

Kirkpatrick Level-1 surveys gather data on student reactions to the training. This evaluation gathers information to determine if students understood the learning objectives, if the delivery format was effective, and if it made them feel confident and prepared to perform their tasks on-the-job. In 2018, TSA updated the Level 1 evaluation survey to include questions on TSO morale. Results show an overall 94% satisfaction rating for students attending the in-person TSO-BTP course at the TSA Academy.

The TSO Basic Program also includes Kirkpatrick Level-2 Evaluations, for determining to what degree students have acquired the intended skills and knowledge. They receive an X-Ray Image Interpretation Test (IIT) and a Job Knowledge Test (JKT) that they must pass to successfully complete the program.

Finally, a Level-3 Evaluation is administered several months after the students return to their airport, to determine how effective the skills and knowledge they learned in the TSO-BTP were applied on the job.

The table below summarizes the actions taken in response to GAO's recommendations and their associated implementation dates:

Measure	Implementation Date
Require IIT First-Time Pass Rate of XX% (rate data SSI and can be provided separately if required)	September 2018
TSO Morale Indicator implemented in Level 1 survey	October 2018
Implement Pat-down Practical Observation Laboratory for 100% of students	October 2018
FY18 Q1/Q2 Level 3 Course Evaluation	September 2018
Require JKT First-time Pass Rate of XX% (rate data SSI and can be provided separately if required)	September 2018
Complete and implement TSO-BTP Level 1, 2, and 3 Training Evaluation Plan	October 2018

Question 5: *On September 22, 2021, the OIG reported that TSA has not implemented all requirements in both the 9/11 and the TSA Modernization Acts. The OIG reported because TSA*

has not implemented all such requirements, "it may be missing opportunities to address vulnerabilities and strengthen the security of the Nation's transportation systems."[3]
Have you taken corrective action to concur with the OIG's findings? And how are you addressing concerns that you may have missed opportunities to address vulnerabilities within our transportation systems?

Answer: In the five years as Administrator, my experience has been that oversight from Congress, the Government Accountability Office (GAO), the DHS OIG and other watchdog groups help to strengthen TSA's performance by identifying areas for improvement and providing recommendations for addressing any shortcomings.

With respect to this specific recommendation in OIG 21-68, TSA did not concur with the OIG, as we have in place an effective system overseeing the implementation of the *TSA Modernization Act*. TSA established this this system informally, and we believe that it should be memorialized. In December 2021, TSA issued TSA Management Directive No. 100.11, *Oversight and Monitoring of Implementation of Enacted Authorization Legislation*, which established organizational roles and responsibilities and delineated processes for monitoring enacted authorization legislation, and OIG closed the recommendation in February 2022.

Question 6: *On April 25, 2022, the Biden Administration released the "Domestic Counter-Unmanned Aircraft Systems National Action Plan."*[4] *Prior to this, the last federal guidance on use of counter-UAS mitigation equipment was issued jointly by DOJ, DOT, FCC, and DHS in August 2020. Within that guidance it notes that Congress has only authorized DOD, DOE, DOJ, and DHS to engage in counter-UAS activities, which certainly seems to tie airports' hands in protecting from security threats.*

Would you agree that airport personnel and state/local law enforcement should be able to have the authorities to detecting, identifying, and mitigating drone threats at airports? If not, why not?

Answer: TSA strongly supports the expansion of authority for detection activities (that is the detection, tracking, identification and monitoring of UAS) to critical infrastructure owner/operators, including airports, and to State, Local, Tribal, and Territorial (SLTT) law enforcement, as outlined in the Administration's National Action Plan (NAP) and legislative proposal. As detailed in that proposal, this authority would be conditioned on using authorized equipment from a government list. To qualify for this list, the equipment would be tested and evaluated by DHS or DOJ and approved by the Federal Aviation Administration (FAA), the Federal Communications Commission (FCC), and the National Telecommunications and Information Administration (NTIA). The

[3] September 22, 2021, DHS Office of Inspector General, TSA Has Not Implemented All Requirements of the 9/11 Act and the TSA Modernization Act; https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-68-Sep21.pdf
[4] April 25, 2022, The White House Briefing Room, FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan; https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/

activities would be governed by the privacy requirements in the Act and guidance from DOJ and DHS, coordinated with the FAA.

TSA also supports the legislative proposal authorizing a temporary pilot program under which a limited number of approved SLTT law enforcement entities could engage in authorized UAS detection and mitigation activities following federal safeguards. This pilot program takes an interim, temporary step that would let Congress, the Executive Branch, and the SLTT agencies evaluate the costs and benefits associated with a possible future expansion of the authority. The proposal is a first step to address the problem that the departments do not have the equipment and personnel needed to deploy counter-UAS measures to the many events and locations that may be subject to dangerous UAS activity, especially as the number of UAS in the airspace proliferates. Today, the departments must turn down many requests to protect significant events, including requests from state governors.

TSA, however, does not support non-law enforcement conducting C-UAS mitigation activities. For any law enforcement other than Federal Law Enforcement using these authorities, TSA believes that they should be subject to strong federal oversight, ensure privacy and civil rights/civil liberties protections are in accordance with federal standards, and fully coordinate all deployments with the FAA.

The use of radio frequency jamming can be a swift, effective mechanism to mitigate drone threats without any serious damage to property, but it can also have unintended consequences for communications. As we consider legislation to grant further counter-UAS activities at airports, how should we balance these competing interests?

Answer: Any system used to mitigate drone threats must pass extensive testing to ensure it does not interfere with or affect communications, flight control systems of authorized aircraft, and other critical elements. All technologies should be coordinated with FAA and FCC to ensure that they have no unintended consequences impacting the National Air Space.

Existing 124n authorities, as well as the draft proposed legislation, require coordination with the FAA prior to using any technology to detect or mitigate a drone threat. Notably, in the past 3 ½ years with these controls in place, there have been no negative impacts on the National Air Space during operational deployments in the United States.

Specific to the additional detection-only authority in the draft proposal, authorized users of "detection-only" authority may only use technology that has been tested by the DOJ or DHS and approved for inclusion on the list maintained by DHS. Placement on that list occurs only after the FCC/NTIA and FAA determine there will be no adverse impacts on the radio-frequency spectrum and the NAS, respectively.

TSA is sensitive to concerns about unintended consequences of all C-UAS mitigation technologies. Reflective of such, TSA has established two C-UAS test beds in operational airport environments to continuously assess the effectiveness and suitability

of systems that could potentially be deployed as part of the airport's approach to detect, track, identify, and mitigate UAS.

I am in the process of drafting legislation to extend C-UAS activities, including at airports. Would you commit to working with me and my staff on this important issue?

Answer: Absolutely. My staff and I will work with you to build on the existing C-UAS authorities.