Michael C. Mullen
Executive Director
Express Association of America

TESTIMONY OF THE
EXPRESS ASSOCIATION OF AMERICA
TO THE SUBCOMMITTEE ON
TRANSPORTATION AND PROTECTIVE SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON: AIR CARGO SECURITY
July 25, 2017

This testimony is provided by the Express Association of America (EAA) on behalf of EAA members DHL, FedEx Express and UPS, the three largest express delivery service providers in the world, providing fast and reliable service to the U.S. and more than 200 other countries and territories. These three companies have estimated annual revenues in excess of $200 billion, employ more than 1.1 million people, utilize more than 1700 aircraft, and deliver more than 30 million packages each day.

EAA will focus its testimony on the contribution of the Air Cargo Advance Screening (ACAS) project to air cargo security. In October 2010, the all-cargo aircraft industry and larger supply chain was a target of a terrorist attack out of Yemen. The ACAS pilot was created as a response to this incident and has demonstrated that a close partnership with industry across government agency jurisdictions in development and execution of new security measures can improve the safety and security of global networks while minimizing negative operational and economic impacts. First developed with express carriers in late 2010, ACAS has expanded to include passenger air carriers, all-cargo carriers, and freight forwarders, and now includes 20 fully operational members, covering 80% of the air cargo shipments entering the United States. The ACAS project has been highly successful and has screened over 440 million shipments without detecting any imminent threats to aviation. Several key lessons have been learned during the pilot, and any rulemaking effort to formalize ACAS through regulation should consider these lessons, as follows:

- **INDUSTRY AND GOVERNMENT WORKING TOGETHER AS PARTNERS:**
  Seeking industry input before proposed rulemakings are drafted allows for broader operational impacts to be considered in order to improve effectiveness. This further minimizes the defensive posture or even anxiety as the private sector faces a government "mandate." The absence of penalties during the ACAS pilot phase further reduced "threshold anxiety" as a barrier to participation. Additionally, the coordination between TSA and CBP enabled industry to accept that the U.S. government had a unified approach and industry would not be subjected to differing rules and requirements.

  - **GOING FORWARD –**

- Penalties should only be imposed in cases of gross negligence or willful circumvention of the rules, and not for the timeliness or accuracy of information (for reasons outlined immediately below). Similar to the move from transaction-based to account-based management of trade parties found in other customs' spheres, the overall compliance level of the ACAS transmitter should be a key factor in the penalty scheme that is developed. This would be consistent with the spirit of trusted partnership that has been the core of the success of the ACAS effort.

- Further, CBP and TSA must ***both*** be included in ACAS discussions with industry in order to ensure the unity of effort across the U.S. government and avoid duplicative and even contradictory approaches.

- **7+1 DATA IS EFFECTIVE TO TARGET RISK:** Separation of shipment and transport data was a necessary precondition to providing information earlier in the supply chain. The information on the shipment transmitted for ACAS (seven data elements plus the bill number – called "7+1 data") is available much earlier than other data required for customs clearance, and "Risk Based Targeting" against this 7+1 data set has proven effective with risk assessment sufficient to identify a shipment of interest. Mandating additional transport data such as master airway bill routings or flight numbers, full automated manifest system information, harmonized tariff system (HTS) numbers or any other commercial data as part of the advanced security filing not only fails to significantly improve targeting, but would also challenge the operational feasibility to provide data in a timely manner. Further, the pilot has shown:

    1. Data provided for ACAS can be "raw data" where typographical or other clerical errors do not substantially affect the targeting capabilities.

    2. The 7+1 data set is sufficient to determine whether or not a shipment is a potential threat to aviation security. Upon analysis of the 7+1 data set, if a particular shipment is of concern, then additional data can be requested on a shipment-specific basis or additional screening can be required. This screening can be conducted early in the supply chain due to the submission timeline for ACAS data. In the majority of cases, shipments already have been screened as a result of standard security program and other requirements, and the results of that screening can satisfy the ACAS referral.

    3. The centralized approach to targeting, risk assessment, selection and referrals for additional screening can be successfully run through joint CBP/TSA teams coordinating all aspects of this process from a single location. This coordination and information sharing between the agencies could be strengthened.

    4. ACAS pilot participants can manage the requests for data and physical screening successfully from a central, corporate inspection system, without requiring requests to be filed with field office locations, thereby improving timeliness, consistency, and accuracy of response.

5. The private sector parties can complete the necessary actions in the event of a referral at an operationally optimum point in the supply chain, thereby reducing the commercial impacts in terms of cost and delays. If the Government has a question about the ACAS data or the data is incomplete, the shipment keeps moving while the additional data is being provided and/or the question is being answered.

6. Any expansion of the ACAS data set beyond the 7+1 elements would be inconsistent with the WTO SAFE Framework on air cargo security.

- **GOING FORWARD –** Future initiatives looking at advanced cargo data should:

  - Recognize that raw, 7+1 shipment data can effectively target risk without requiring data elements needed for other customs functions.

  - Specify the last point of departure of the flight that delivers the shipment to the United States as the deadline for submission of the data. Choosing any other deadline for data submission will add unnecessary complexity and is likely to affect operational feasibility, as shipment routing is often not known at origin.

  - Accept that shipment-specific data is sufficiently accurate to determine any potential threat by the shipment, and shipper-based approaches associated with a shipper's volume are often not feasible in the advanced data context due to the timeliness of information and the need of the carriers to segregate shipments based on the shipper before building the pallets or other unit load devices (ULD). Further, shipper-based determinations are often redundant, and the shipment has already been singled out for screening prior to the shipper-based determination.

  - Express carriers have a centralized database for tracking the results of shipment screening, that includes screening caused by ACAS referrals, which could be made available to TSA for auditing purposes. Based on this information, TSA could provide exemptions to standard security program screening requirements for some ACAS participants.

- **<u>ACAS ANALYSIS IS LIMITED TO SECURITY:</u>** While it is tempting to use advanced data for other purposes, the success of ACAS has been in part driven by the common goal to prevent a bomb from entering the network. This singular focus of utilizing air cargo advanced data for security risk assessment remains the top priority among private and public sector participants. Regulatory risk assessment to interdict IPR violations, illegal drugs or other controlled substance trafficking, or other trade functions can and should be the focus of CBP officers upon arrival in the U.S. Any attempt to expand the ACAS scope to achieve the simultaneous completion of both security and regulatory risk assessments pre-departure would undermine achieving the primary goal of protecting the supply chain against terrorist attacks.

- **GOING FORWARD-** This singular focus on security must be maintained for ACAS.

- **<u>FLEXIBILITY IS CRITICAL FOR EFFECTIVENESS: Three distinct types of flexibility needed:</u>**

1. ***IT Systems Can And Should Be Flexible:***

   - ACAS has demonstrated that data can be transmitted via multiple types of IT systems and in various formats. This flexibility in the interface reduces the barrier to participation and avoids unnecessary costs and time delays associated with updating a company's IT system. Furthermore, the flexibility reduces the risk of competitive disadvantages arising from existing differences in the functionality and capacity of corporate IT systems.

   - Where a "dual filing" approach is taken with a separate ACAS filer and carrier, a rapid confirmation for the carrier of ACAS submission and the shipment's security status is important. The timeliness of verification across systems is most difficult with time definite shipments, yet this is also the most essential.

   - The differing business models of express/integrated and non-express/conventional will require that the IT system provide different functionality for these, in particular with regard to security status messaging.

   - **GOING FORWARD -** The final IT filing system developed for ACAS must remain flexible. It should continue to accommodate multiple data submission formats and provide for the return messaging options required by some business models of the entities utilizing the system.

2. ***Screening Methods and Locations Need to Adapt to Country and Operational Limitations:*** The screening is being conducted outside U.S. borders, often well before the U.S. jurisdiction to control and mandate screening. This provides a screening and security level far greater than the U.S. could ***<u>mandate</u>*** and helps ensure the security of cargo movements throughout the entire supply chain, not just from the last point of departure. However, this also understands that there may be challenges to screening with a particular method at ***<u>every</u>*** point globally.

   - The screening method available at a particular country early in the supply chain may not offer AT X-ray, and the shipment should be allowed to be physically screened by other appropriate methods as approved at that location or allowed to move to the next point at which the cargo could be screened.

- When there is a U.S. government recognized National Cargo Screening Program (NCSP) of another government's cargo security program, the NCSP recognized screening methods can be effectively applied to mitigate risk. The NCSP methods were – by definition – already accepted by TSA as offering a level of security commensurate with the U.S., and local screeners cannot be trained to apply differing screening standards whether it is getting a U.S.-ACAS based screening referral or a locally-based screening referral.

  - **GOING FORWARD-** The U.S. should continue to allow cargo selected for ACAS referral screening to be screened at the most operationally feasible location and allow the local screening standards to be applied for a screening referral when the cargo is in an NCSP recognized country. These National Cargo Security Program recognitions have become a critical facilitator of seamless cargo movement through major transit hubs.

3. ***Operational Requirements Need To Be Flexible Based On Different Business Models:*** The air cargo industry is not one-size-fits-all; the regulations and programs should not be either. Challenges and opportunities differ between business models, and the system can be flexible regarding who transmits the data and when. While the jointly held overriding goal is to intercept a high-risk shipment as early as possible, data can be transmitted by multiple partners, depending on who may be in possession of the shipment data. No specific time limit is necessary, as long as data can be transmitted in raw form as soon as available. Further, government targeters have the ability to prioritize shipment reviews based on the urgency/timeliness of the shipment itself, thereby helping to address concerns for last-minute shipments in the just-in-time supply chain.

   - **GOING FORWARD-** The government must continue to recognize the different components and business models in the larger air cargo industry and avoid putting burdens on all segments that are not appropriate for individual segments. This includes ensuring that the screening referral goes to the party who filed the ACAS data – even if that party is a forwarder and not a carrier – in order to ensure the timely interception of a suspect shipment.

- **INFORMATION SHARING REMAINS KEY:** The private sector is providing shipment level data to the government. At the same time, any government held intelligence of concern regarding a specific shipment must be shared with the private sector ACAS participants when appropriate. When a screening referral has been issued, CBP/TSA have been able to provide specific intelligence as to why that shipment is targeted and what screeners should look for on that specific shipment if there is a specific threat. Although there has been some hesitance to provide broader intelligence sharing with the private sector, use of other government bodies, such as the Office of the Director of National Intelligence (ODNI), could be utilized more effectively to include both domestic and international parties involved in the ACAS system.

- **GOING FORWARD-** Information sharing should include:

  - ACAS participants should be provided with specific concerns for that shipment, thereby improving their detection capability on a targeted shipment.

  - For a shipment that rises to the level of a DNL, the carrier in possession of the shipment must be given all information to quickly identify and isolate both that shipment and others in the network that may be similar.

  - Other ACAS participants must also be made privy to the full information – for them to identify and isolate similar high-risk shipments.

  - Finally, a secure means to provide broader threat information to the appropriately selected security staff within the ACAS carrier is needed. It would improve internal risk targeting prior to a shipment ever entering the network. This type of "bridge line" conference call can and should be tested with industry more effectively.

- **THE AIR CARGO NETWORK IS HIGHLY SECURE:** Air cargo operators are highly motivated to ensure their systems are not targeted by a terrorist weapon and have made major investments in creating a secure aviation network based on multiple layers both from government regulations and additional corporate security measures. Of the hundreds of millions of shipments screened through ACAS over a period of nearly seven years, less than one-half of one percent has required additional measures to verify the contents, and no terrorist threats have been detected. This indicates that existing measures are working effectively to deter attempts to exploit the network for terrorist purposes.

  - **GOING FORWARD-** Before any new regulations are proposed to improve the security of what is already a very secure air cargo system, government agencies should conduct a cost/benefit appraisal, consider the operational impacts and weigh those against the marginal increase in security. This is the backbone of "Risk-Based Security."

- **INTERNATIONAL HARMONIZATION IS CRITICAL FOR LONG TERM EFFECTIVENESS:** Most of the industry partners involved in the ACAS pilot are operating on a global scale. There are several initiatives similar to ACAS being discussed in multiple countries. It is vital that the U.S. Government seek early alignment with international organizations and other partners/countries to develop internationally-recognized standards, procedures and processes for advanced shipment data provision to minimize the level of variability of systems and requirements and avoid duplication of data submission and security risk assessment where possible.

  - **GOING FORWARD-** It is vital to develop a common global solution that recognizes and supports the different air cargo business models and to achieve mutual recognition of security programs and risk assessment results. The global solution should harmonize

data requirements and eliminate duplication by ensuring shipment data is only submitted to one country for a single security risk assessment that is accepted by partners with whom that country has a mutual recognition agreement. This will allow international trade partners to share information globally and quickly, both reducing unnecessary cost and complexity while improving governments' risk assessment capabilities.