Opening Remarks by OSC AA
Jill Vaughan
ACC/TSA Security Capabilities Day
June 16, 2015
Agenda

- OSC Organization
- TSA Organizational Goals
- Current Landscape
- Transportation Security Acquisition Reform Act Overview
- Five-Year Plan Approach
- Emerging Themes and Trends
  - System of Systems
  - IT Security
  - Collaboration and Transparency
  - Improved Test and Evaluation
- Next Steps
The Office of Security Capabilities safeguards our Nation’s transportation systems through the qualification and delivery of innovative security capabilities and solutions.
1. Risk-Based Approach to Operations

Expanded from Risk-Based Security to drive more risk-informed analysis and risk-based decision-making outside of security operations.

2. Engagement

Added a focus on external engagement to reflect the importance of sharing information and obtaining feedback from stakeholders.

3. Organizational Efficiency

Included new objectives that focus on developing outcome-based measures and policies and building an optimal workforce for effective operations.

From TSA Strategic Plan, FY15-FY18
Current OSC Landscape

- **Dynamic threat environment**: A dynamic adversary targets known security vulnerabilities and constantly challenges the capabilities of the security industry with new and evolving threats. As an example, TSA has seen a significant increase in electronics being in stream of commerce carry-on bags posing a challenge at checkpoints.

- **Reduced program budgets**: From FY11-FY15, the OSC budget has been reduced by 48%, necessitating prioritization across the enterprise and reduced program spending.

- **Industry Vitality and Support**: To continue to improve technology capability, TSA must rely on strong partnerships with current vendor community to leverage corporate knowledge to the maximum extent possible. At the same time, TSA must explore all avenues to solicit and implement ideas for innovative solutions in response to TSA challenges.

The Transportation Security Acquisition Reform Act encourages accountability and stakeholder involvement in the technology acquisition process.

A key requirement of the Act is the **Five-Year Technology Investment Plan**.

The Plan aims to achieve a shared vision among Congressional, industry, DHS, and TSA stakeholders to address capability needs, deploy cutting-edge capabilities to the field, and increase security effectiveness and passenger safety in American aviation security.

The Plan is due 180 days after enactment and details planned purchases and program and operations information to meet 27 specific requirements. It will be updated every two years.

The Plan is currently in the DHS clearance process.
TSA took the following approach to gather and evaluate content with stakeholders:

- Analyzed 27 Act requirements to identify existing resources and gaps and developed themes and outline
- Partnered with WHSR and SMC to engage industry. As a result, TSA:
  - Met with TSA offices and divisions to gather inputs and confirm appropriate levels of detail
  - Analyzed RFI, industry meeting, and SME inputs
  - Reviewed, refined, and produced draft Plan for TSA and DHS Review
  - Held Industry Debrief to review key themes and plan for future engagement
  - Prepared for final Plan submission to Congress by June 2015
TSA is pursuing an open architecture framework and a system of systems perspective in order to proactively identify capability gaps and define targeted screening capabilities by enabling an integrated and modularized security screening system.

**Industry Input**
Based on RFI and Working Group trends

“Incentivize industry to establish open architecture and standards requirements and promote interoperability.”

**Expected Outcomes**
Results of TSA’s efforts

- Enhanced interoperability
- Improved acquisition planning
- More open business model
- Increased participation of small and disadvantaged companies
As TSA continues to move towards a network-connected screening environment, many IT security challenges need to be addressed to ensure the security of the deployed TSE fleet and TSA’s network.

**Industry Input**
Based on RFI and Working Group trends

“Ensure TSE are secured against physical and cyber vulnerabilities.”

**Expected Outcomes**
Results of TSA’s efforts

- Proactively mitigated risks
- Mandated vendor IT security requirements
- Enhanced protection against physical and cyber vulnerabilities
TSA is establishing a regular cadence of engagement with industry stakeholders to increase the opportunities for businesses of all sizes to compete and help advance the mission of TSA.

**Industry Input**
Based on RFI and Working Group trends

“Increase transparency and allow TSA to rapidly respond to emerging threats by collaborating with industry throughout the acquisition lifecycle.”

**Expected Outcomes**
Results of TSA’s efforts

- Increased industry engagement
- Better defined requirements
- Increased participation of small and disadvantaged companies
- Enhanced predictability and clarity to business of all sizes
TSA is working with the National Institute of Standards and Technology and vetting the Third-Party Testing strategy with industry to simplify T&E procedures and deliver capabilities to the field faster.

**Industry Input**
Based on RFI and Working Group trends

“Explore testing enhancements like incremental feedback, increased predictability, realistic developmental test beds, red teams, and improvements to third party testing.”

**Expected Outcomes**
Results of TSA’s efforts

- More clearly defined third party strategy
- Reduced programmatic, financial, schedule, and performance risks
- Reduced time-to-deploy
- Reduced cost of test and evaluation
Next Steps

Five-Year Investment Plan Next Steps:

• Report in final DHS/OMB review for summer release to Congress
• To be released to Industry following approval
• Additional industry engagement opportunities will be initiated over the next year
• Plan updated at a minimum every two years

TSA Point of Contact:

Keith Goll, OSC Senior Technical Advisor
Keith.goll@tsa.dhs.gov