MAD is a forward-looking technical division that aims to focus on adjacent and transformational investments at TSA. MAD is transitioning from providing *ad hoc* support as needed to leading and directing a cohesive, strategic future state at TSA.

**What is MAD’s Vision?**

Increased Integration

Proactive

Enhanced Capabilities

Reactive

Current MAD Focus

Planned MAD Focus
Through architecture, risk, engineering, and human factors, MAD impacts many critical TSA and DHS functions, from policy and mission-critical acquisitions to strategy and R&D. MAD works with a number of partners both internal and external to TSA.

**Internal Partners**

- Office of Chief Risk Officer (OCRO)
- Office of Inspection (OOI)
- Office of Intelligence and Analysis (OIA)
- Office of Information Technology (OIT)
- Office of Security Operations (OSO)
- Office of Global Security (OGS)
- Checkpoint Solutions and Integration Division (CSI)
- Checked Baggage Technology Division (CBTD)
- Testing and Evaluation (T&E)
- Office of Training and Workforce Engagement (OTWE)

**External Partners**

- Defense Advanced Research Projects Agency (DARPA)
- Joint Improvised Explosive Device Defeat Organization (JIEDDO)
- Department of Homeland Security Science and Technology Directorate (DHS S&T)
- National Labs
- Industry
- Academia
- In-Q-Tel (IQT)
- R2A
MAD Organizational Overview

**Mission Analysis Division**

MAD performs quantitative and qualitative systems analyses to facilitate risk- and operationally-informed decision-making across TSA.

**MAD Roles:**
- Identify threats, vulnerabilities, and capability gaps
- Conduct risk, systems, and operational analyses to inform future courses of action
- Develop engineering requirements and support OSC programs in the acquisitions lifecycle

**MAD Branches**

- **Systems & Risk Analysis**
  Branch Manager
  Rich Kraske
  Conducts systems and risk analyses to determine the impact security capabilities or procedures have on the aviation system.

- **Systems Optimization Support**
  Branch Manager
  Mike Benedetti
  Provides technical oversight for checked baggage design reviews and resolves existing checked baggage issues.

- **Requirements & Systems Engineering**
  Branch Manager
  Mark Bernatowicz
  Provides system level engineering to identify capability gaps, establish system requirements, and drive TSA's future security architecture.
Systems and Risk Analysis (SRAB)

Core Mission Objectives

• Provide risk and systems analytical support to TSA working groups and decision makers, including analyses of alternatives, cost benefit analyses, allocation analyses, and qualitative risk assessments
• Conduct systems analyses to identify threats, opportunities, and to drive continued improvement
• Perform capability gap analysis and portfolio planning to inform future development

Past / Current Initiatives

• Case Studies
  • RBS Pre✓™ Decision Memo
  • Managed Inclusion Risk Analysis
  • AIT Redeployment Allocation Analysis
  • Behavior Detection Officer Return on Investment
  • RTSPA
  • RMAT Pre✓™ Analyses
• Analytical Capability Development
  • Systems Field Evaluation
  • Adversary Threat Portfolio
  • RMAT Data Refresh

Future Initiatives

• Case Studies
  • Expedited Screening
  • Trusted Traveler Population Assessments
  • Systems of Systems Cost Benefit Analysis
  • RMAT Pre✓™ Analyses
• Analytical Capability Development
  • TSALT
  • TSCAP Support – data and analysis
SRAB conducts risk and systems analyses to determine the impact that security capabilities or procedures have on the overall aviation system and to proactively identify threats and opportunities. Types of case study questions include:

- **What is the best checkpoint configuration for a particular countermeasure?**
  
  Analysis of Alternatives recommends optimal ConOps based on Security Effectiveness and other trade-off considerations.

- **How can scarce resources be best distributed?**
  
  Allocation Analysis recommends countermeasure distributions across airport categories, based on Threat and Vulnerability assessments.

- **Should a countermeasure be acquired? Does it justify the cost?**
  
  Return on Investment analysis finds the equilibrium between security value and program cost, identified as a break even point.

- **What are the impacts of implementing a population-specific RBS procedure?**
  
  Population Analysis provides risk-driven assessments and recommendations for population-specific ConOps.

**Risk and Systems case studies inform TSA’s risk-based decision-making by quantifying and structuring potential benefits and tradeoffs associated with new policies.**
Requirements and Systems Engineering (RSEB)

Core Mission Objectives

- Provides system level engineering to define capability needs, establish holistic system requirements, and drive TSA’s future security architecture.
- Develops and maintains detection requirements and coordinates with DHS S&T to characterize threats.
- Performs human factors analysis and provides human factors expertise to ensure system and task parameters are designed to optimize performance.

Past / Current Initiatives

- Common Graphical User Interface for EDS
- High Resolution OSARP for EDS
- Design Interaction Cog Gauge & ScreenADAPT (DHS S&T)
- Pat-down Accuracy Training Tool (PATT)
- Sandia Cognitive Effects of Lane Switching
- SOP Communication Effectiveness Improvement
- CEA FFRDC
- HME Characterization
- TSCAP Prototype

Future Initiatives

- TSCAP Option Year 1
- TSIC Targeted BAA
- TSE Systems Architecture
- Human Factors BPA
- Systems Field Evaluations for TSMs
RSEB: Scope of Work

RSEB has the tools and capabilities to develop technical requirements based on operational needs, assess human factors impacts of proposed security alternatives, and support the testing and acquisitions of new technologies.

**How do we translate user needs to technical requirements?**

TRMH/TSCAP ensures that user needs are accurately captured as technical requirements.

**How can we improve operator efficiency?**

Human Factors Engineering recommends interface and process modifications that are designed to improve operator efficiency and accuracy.

**Can we detect the current threats?**

HME Characterization leverages relationships with DHS S&T and TSL to fully characterize threats and test systems.

**How do we identify and implement new technologies?**

Broad Agency Announcements allow TSA to solicit and pursue new technologies in an effective manner.

MAD RSEB utilizes established engineering methodologies and strategic relationships to promote operational and security efficiency.
Core Mission Objectives

• Provide systems-level engineering subject matter expertise
• Electronic Baggage Screening Program (EBSP) Baggage Handling System (BHS) Design Reviews
• Primary POCs to provide project oversight, direction, and guidance and interface with airports and design teams
• Conducts SOS Team Assessments – Checked Baggage Inspection System (CBIS) issue resolution

Initiatives

• Provides CBIS technical expertise for maintaining checked baggage design guidelines and standards (ex., PGDS)
• Addresses security and safety concerns, issues, or problems related to inline systems
• Performs cost validations for inline system designs
• Performs BASE Team field optimization visits in support of TSA operations
• Leading systems integration effort for EBSP RBS as related to BHS and EDS communications
• Leading coordination efforts with IATA baggage working group to determine data format to be transmitted from Secure Flight
SOS Initiatives

The SOS branch seeks to mitigate existing checked baggage issues while also supporting the expansion of RBS to the checked baggage space.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Current Related Efforts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BASE Team</strong></td>
<td></td>
</tr>
<tr>
<td>• The operations of the BASE team are important for solving key CBIS integration challenges related to security, safety and efficiency.</td>
<td>• Supporting EWR, JFK, LAX, LIT, MIA, and PVD.</td>
</tr>
<tr>
<td></td>
<td>• JFK and PHL both are experiencing CBRA sizing challenges only a few years into operation</td>
</tr>
<tr>
<td></td>
<td>• EWR is experiencing “bag ID” swaps.</td>
</tr>
<tr>
<td><strong>Design Reviews</strong></td>
<td></td>
</tr>
<tr>
<td>• Design reviews ensure that new or modified checked baggage systems meet requirements outlined in the PGDS.</td>
<td>• In-house design reviews at TPA, HOU, KOA, JAX, OMH, BOI, DEN, SEA, ANC, HPN, MHT, LAS, JFK T4 West CBRA, MSY.</td>
</tr>
<tr>
<td></td>
<td>• Sites such as MSY require in-depth support due to inefficiencies of a “dual-mainline” design.</td>
</tr>
<tr>
<td><strong>Checked Baggage Innovation</strong></td>
<td></td>
</tr>
<tr>
<td>• RBS principles are mostly focused at checkpoint operations, but checked baggage systems could also realize gains from implementing RBS.</td>
<td>• RBS: Pilot at FLL with new IATA standards in place.</td>
</tr>
<tr>
<td>• Beumer Tray System: Installed at the TSIF</td>
<td>• Beumer: New technology for CBIS</td>
</tr>
<tr>
<td>• DAC-II: Camera system</td>
<td>• DAC-II: Positive exterior bag matching capabilities</td>
</tr>
<tr>
<td><strong>Planning Guidelines &amp; Design Standards (PGDS)</strong></td>
<td></td>
</tr>
<tr>
<td>• A comprehensive document that provide baseline requirements and a list of best practices for the industry to follow when designing inline screening systems.</td>
<td>• Support in transitioning the ownership to the Planning Branch.</td>
</tr>
<tr>
<td></td>
<td>• Key role is now to provide technical content.</td>
</tr>
</tbody>
</table>
International Collaboration

The Senior Technical Advisor (STA) is working with our international partners to mitigate credible threats to transportation, streamline technology priorities, and align detection standards and testing methodologies.

**Core Mission Objectives**

- Expand International Knowledge Base through collaboration and information sharing
- Increase screening capability at LPDs (detection of smaller threat masses, breadth of threats, detection within complex concealments (i.e., Laptops, Liquids, etc.))
- Instill consistency in threat characterizations (i.e., density, threat mass), testing methodologies (process, confidence levels, quality control), and next generation (mass spectrometry, x-ray diffraction) technology assessments in response to evolving aviation threats
- Ultimately, instill reciprocity to deliver enhanced capability to the US market sooner

**Collateral Responsibilities**

- **Detection Standards** – Establish, maintain, and update detection standards in close collaboration with the Intel Community, Checkpoint and Checked Baggage Programs, and Testing entities
- **ICAO** – Represent TSA as the co-chair on the aviation technology working group
- **QUAD** (US, Canada, Europe and Australia) – Represent TSA on the Technology Working Group
- **Bi-lateral Information Exchange** – Partner with OGS by participating in numerous technical discussions with international partners
- **Collaboration with DHS S&T and Industry** – Assist DHS S&T to align testing process with international partners, provide foreign OEMs feedback on investment roadmaps, and provide status updates to international associations (i.e., ACI Europe)
TSCAP Overview
TSA’s Operational Environment

Significant Challenges:

- TSA screens 640 million passengers and 1.5 billion bags annually.
- TSA oversees a transportation network with over 751 million bus passengers and 10 billion mass transit passenger trips annually.

Security capabilities have historically been developed, acquired, and deployed discretely. Usually in response to recent events or information regarding emerging threats and risks.
What is TSCAP?

Transportation Security Capability Analysis Process (TSCAP)

TSCAP identifies TSA’s needs, supports better decision making, and recommends security solutions for aviation security. This process justifies TSA’s investments by weighing the value of those solutions in a structured, repeatable manner.
TSCAP

Transportation Security Capability Analysis Process (TSCAP) is an integrated, decision support process that improves TSA’s development of security capability operational requirements.

**What is the value of TSCAP?**

TSCAP combines the relevant drivers for requirements into a structured method and uses a suite of tools that allow for analytic rigor and smarter decision-making. This process leads to:

- Stronger connection between strategic objectives and requirements
- Improved requirements for industry to meet
- Clearer understanding of system functionality and the impact of one piece not working correctly

TSCAP’s outputs generate new value for OSC:

**Holistic (Agency Level)**
Conducted annually, across OSC and in conjunction with industry, to identify and prioritize gaps across the entire system and to determine requirements to close gaps

**Program Level**
Conducted in response to gaps or a specific driver to determine requirements for specific gaps

**Specific Questions**
Targeted analysis using TSCAP tools and data
How Does TSCAP Address TSA’s Issues?

- **Produce Smart Investment Decisions**
  - Uses a disciplined systems analysis approach to identify TSA’s risk posture and security gaps
  - Establishes a customer-based forum designed to identify prioritized functional capability needs to address security gaps
  - Aligns R&D investments with TSA capability needs to drive technical solutions

- **Develop Better Requirements**
  - Delivers preliminary operational requirement documents that support the capability gaps
  - Expand engagement opportunities to generate ideas early in the Needs Phase (part of the AD-102 Acquisition Lifecycle Framework) to drive innovative technology solutions
How TSCAP Supports Decision-Making at TSA

**Holistic (Agency Level)**
Conducted annually to identify and prioritize gaps across the entire system and to determine requirements to close gaps.

**Example:**
An annual refresh of the entire TSCAP process is performed. Capability gaps are identified, prioritized, and then recommendations are given to project offices. Both SOP and technology options are to be recommended.

**Program Level**
Conducted in response to gaps or a specific driver to determine requirements for specific gaps.

**Example:**
Based on the identified gaps, a Program Management Office explores possible options with industry that are analysed by decision makers using TSCAP’s architecture and visualization tools and prioritized using TSCAP’s decision making tools.

**Specific Questions**
Targeted analysis using TSCAP tools and data.

**Example:**
An IPT wished to address the high rate of resolution pat downs (RPDs) resulting from the increased alarm rate of Advanced Imaging Technology (AIT) Tier II Automated Target Resolution (ATR) systems.
TSCAP High-Level Phases

- Establish TSCAP Baseline
- Identify and Prioritize Capability Gaps
- Generate Alternatives
- Analyze and Select Alternative
- Document Operational Requirements
- Handoff to Project Office

As-needed Analyses
(e.g., Unexpected Changes or Emerging Threats)
TSCAP Detailed View

Establish the TSCAP Baseline

Step 1: Update Goals and Objectives, Threats, Countermeasures and Configurations

Identify and Prioritize Capability Gaps

Step 3: Perform Security Capability Gap Analysis

Generate Alternatives

Step 5: Identify Mitigation Options by Collaborating with Stakeholders

Analyze and Select Alternatives

Step 8: Share and Vet Results with Stakeholders

Document Operational Requirements

Step 10: Develop p-ORDs and p-CONOPS

Handoff to Project Office

Step 11: Handoff

Execute Program To Deliver Capability

Step 2: Update Trade Space Performance Baselines

Step 4: Select Security Gaps to Address and prepare p-MNS

Step 6: Select Mitigation Concepts to Analyze

Step 7: Conduct Analysis

Step 9: Conduct a p-AoA and Formulate Recommendations

Document Operational Requirements

Step 10: Develop p-ORDs and p-CONOPS

Handoff to Project Office

Step 11: Handoff

Execute Program To Deliver Capability
What’s Next?

• TSCAP is currently being implemented more broadly across OSC:

  • Validate and prioritize gaps, and define measures of success for the gaps

  • Defines the need and early requirements for next generation capabilities

  • Conducting analysis from the prioritized mitigation options resulting in a pAoA, p-ORDs and p-CONOPS
Questions?