Key Problems Facing Stakeholders

Simon Bedford, TeleSecurity Sciences

Established Vendors

- Long and difficult to plan for acquisition cycles, lengthy qualification processes and inflexible standards, cost-centric procurement - all stifle innovation
- Value of open architecture & standards understood by customers and regulators, maintain proprietary systems solutions or support more open systems?

TSA/government regulator

- Adversaries actions are potentially flexible and innovative with a far shorter planning and implementation time
- Airport operators, airlines, cargo companies strongly influence adoption of new processes and technology, high commercial influence, e.g. strong focus on traveler experience, can be pro or con for security

Academia

- Need to publish & work openly versus security restrictions & the requirement of sponsoring private entities to retain IP & competitive advantage - limits effective engagement with Industry
- Without direct access to data from technology platforms or the field it's difficult to contribute to development close to commercial / operational impact, longer term general research efforts only (opportunity missed?)

Airports, Airlines, Freight Forwarders

- Standardize on limited number of vendors/platforms (easier to manage/integrate, cost goes up), or adopt open architectures & standards (more difficult to manage/integrate, operational and cost benefits)
- Need for at least standardized TSE GUIs across platforms and applications for streamlined training and operation - high operational cost benefit
- Need for networked screening systems and TSEs with remote inspection, system monitoring/health, centralized user management & standardized (but still flexible) cyber security - up to and including on a national basis