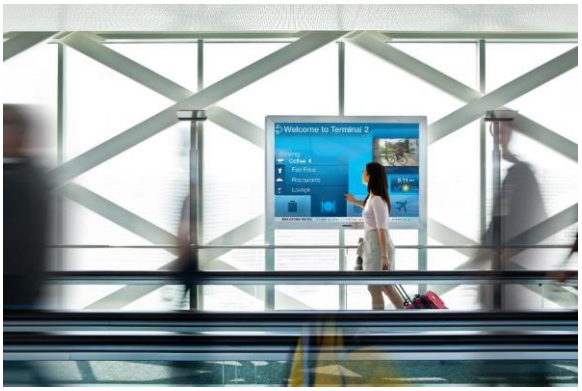
Cisco Connected, Safe and Secure Aviation

Safe and Secure Airport Checkpoint Operations to Transform the Travel Experience for the 21st Century Mobile Society

Section 1 – Corporate Expertise



Cisco is committed to creating secured network solutions that are smarter, thanks to built-in intelligent network services; faster, in their ability to perform at ever-increasing speeds; connected, in our drive towards standards-based solutions; and more robust, with a generational approach to an evolutionary infrastructure. More specifically, Cisco supports governments and defense agencies around the world by delivering innovative, integrated mission capabilities through thought leadership, advanced technologies, and services. The Cisco federal staff comprises a team of top experts from space, military, homeland security, and public safety from all levels of government around the world. They not only understand the unique challenges of government, but also bring years of personal experience to help solve these challenges.

Financial Strength

In high-tech industries, where change is the only constant, financial strength is the foundation of a company's staying power. Cisco has a consistent track record of financial performance that is undisputedly the best in the industry. Our balance sheet attests to this strength. When you consider current assets minus current liabilities, which is a good measure of liquidity, Cisco's position is greater than that of our major competitors combined.

R&D Investment

Cisco also uses its financial leverage to benefit customers through significant investment in R&D—approximately 14 percent of our revenue each year. In fiscal year 2013, this translated to roughly $5.9 billion (U.S. dollars). Not only do we invest more in R&D than anyone in the industry, we also focus that investment on the future.

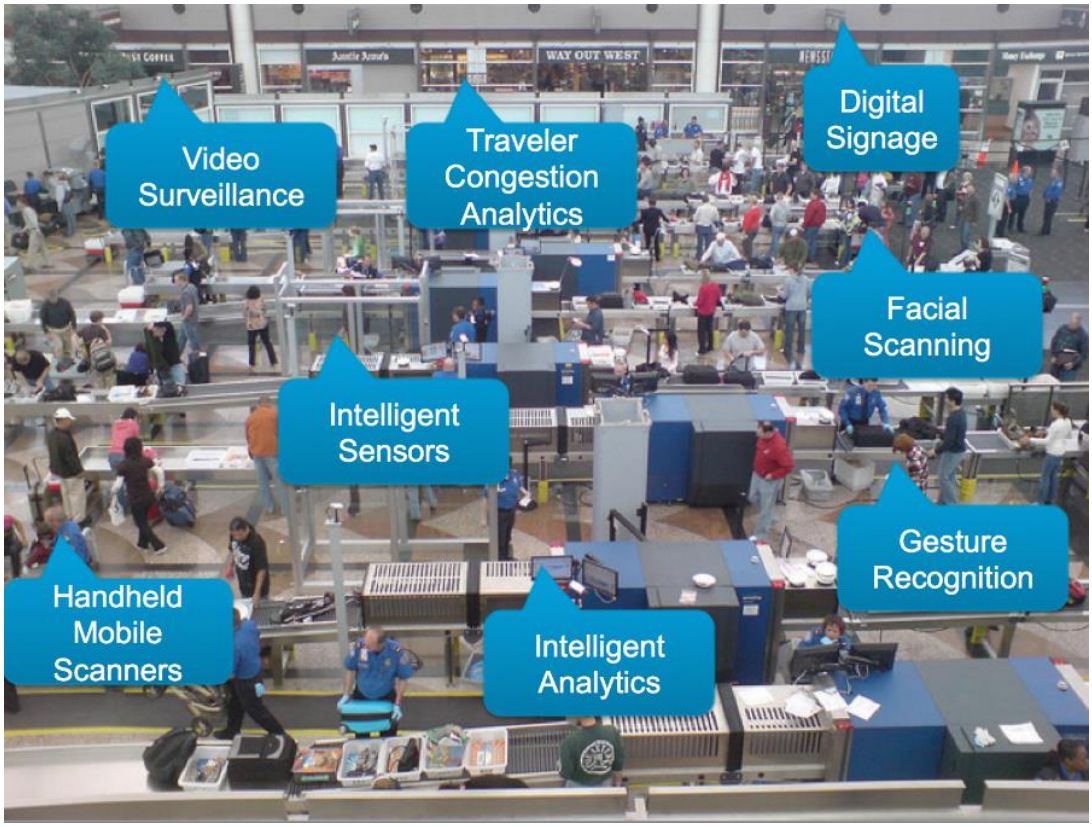
This research enables us to develop many of the innovative technologies and solutions that drive and lead the dynamic technology market. Our R&D efforts have led to some truly breakthrough solutions, such as Cisco TelePresence, Cisco Unified Computing System, and Medianet technologies, which uniquely enable next-generation services our customers are demanding.

Section 2 – Conceptual Alternatives

Executive Summary

Cisco Connected, Safe, and Secure Aviation provide capabilities for airport checkpoint operations and innovations to transform the traveler experience. Efficient and effective operations require mapping key challenges to capabilities supported by people, processes, and robust technologies. The mission-critical IP network-centric framework integrates with existing infrastructure today and supports innovation for future requirements in checkpoint technology integration and passenger screening processes including:

- Checkpoint operation efficiency (automation) and efficacy
- Innovation/integration
- Improved passenger experience
- Remote diagnostics and repair
- Real Time Threat Assessment related to behavior detection or explosives detection canine



The Cisco network platform supports requirements for secure information and communications capabilities today and supports the requirements for the future technologies for the Internet of Things (IoT). The network provides the platform to integrate the IoT for airport checkpoint security with the secure connection of machines, devices, sensors, and "things" to help people improve operations, save time, money, and even lives.

The Cisco vision for the "The Internet of Everything (IoE)" brings together people, processes, data, and things to make networked connections more relevant and valuable than ever before – turning information into actions that create new capabilities, richer experiences, and unprecedented opportunity for businesses, individuals, and countries.

Air Travel Security	*Today*	*In the Future with Internet of Everything (IoE)*
Checkpoint operation efficiency (automation) and efficacy	Need to improve operational excellent with best practices sharing across all checkpoints	Automated processes, people, data, and things for operational excellence
Innovation/Integration	Challenges meeting performance requirements for integrating advanced technologies	Flexible platform integrates new capabilities on demand
Improved passenger experience	Frustrated travelers, long lines	Efficient passenger flow and positive travel experience
Remote diagnostics and repair	Difficulty managing and monitoring multiple technologies at scale	Self-diagnosing, self-healing capabilities
Real Time Threat Assessment related to behavior detection or explosives detection canines	People-intensive processes subject to human error	Intelligent analytics identifies potential threats to improve security posture

Challenges: Airport Security More Complex; Passenger Expectations Rising

Governments around the world are seeking innovation solutions to address the requirements to ensure the safety and security of airports and passenger travel and to transform the experience in our increasingly global and mobile society.

Modern airport authorities must maintain the security of the traveling public and ensure efficient mobility of people and commerce. Threats to national and international air travel face a wide spectrum of risks including terrorism, crime, attacks on critical infrastructure, natural catastrophes, and other emergencies. Threats to aviation security continue to evolve and are becoming more sophisticated and complex with a number of challenges including:

- **Sophisticated safety and security threats**: Increasingly, terrorists take advantage of technology. Modern terrorist attacks, for example, are facilitated by advanced consumer electronics such as smartphones, Geographic Positioning System (GPS) navigators, and anonymous email accounts.

- **A need for capability-based approaches**: Airport security relies on the execution of explicit and documented policies and procedures. The challenge is that it is impossible to predict all contingencies. With capability-based planning, or putting in place a flexible architecture with capabilities that are useful in a wide range of scenarios. This provides agility to prepare unpredicted threats.
- **Unreliability of rarely used processes**: When personnel rarely use a system, they are more likely to make mistakes. They might even not notice an alert announced on the special emergency system, if they are unaccustomed to checking. What's more, maintaining separate systems for emergencies and everyday communications doubles the expense for training, administration, and upgrades.
- **Difficulty of monitoring and managing more systems**: The increase in the number and types of threats has led to a corresponding increase in the systems that airport security authorities must manage. Many agencies already have large existing investments in video surveillance cameras, radios, fire suppression systems, and more. Now they are adding new systems for cybersecurity, event correlation, and response to chemical, biological, and radiological threats. If each system is deployed on its own proprietary network, management becomes progressively more expensive.
- **Confusion resulting from disparate emergency communication systems**: Poor information flow both within and among the organizations involved in preparing for and managing airport safety and security is among the principal causes of failures. Costs can be measured in money as well as in lives. Typically, inadequate information distribution is the direct consequence of human error, interagency conflicts, political considerations, and lack of communications interoperability.
- **Organizational boundaries and public-private partnerships**: A variety of people from different organizations, not just traditional airport authority security agencies, need to share information and communications for routine procedures and be prepared for a crisis scenario. These might include airlines; local, state, and federal authorities; emergency responders; international authorities; and more. These entities ordinarily keep their information private, so they need assurance that their information will be shared only for the duration of the crisis, and on a need-to-know basis.
- **Growing dependence on privately held critical infrastructure**: Airports and travelers depend on critical infrastructure located within or nearby airports. Examples include retail, restaurants, medical clinics, public transit, parking, power plants, and utilities. This further illustrates the need for airport security architectures to support information sharing with private-sector organizations.
- **Cyber threats**: The number of cyber threat actors is increasing, the number of targets has increased, and the techniques have gotten better. Airports and critical infrastructure are subject to the same risks, potentially affecting power generation and distribution, transportation, oil and gas pipelines, water distribution, and telecommunications. Disruption of this infrastructure has significant economic consequences.

- **Misinformed general public**: While airport authorities proactively inform the traveling public and respond promptly to potential threats and crises, authorities often struggle to inform the public, especially during the busy travel seasons and when a specific threat crisis begins. The larger the scope, the more carefully the information must be conveyed. Too much information can cause confusion or even mass panic; too little can result in some travelers not finding out about the situation until it is too late.
- **Citizen and traveler privacy needs**: Airport safety and safety agencies need to collect and apply information about travelers in a responsible way.

Goal 1: Unified Operations across Multiple Airports and Checkpoints

In airport checkpoint environments, it is critical to maintain consistent procedures and best practices at all times. When threat conditions increase or incidents occur, it is critical that personnel are able to react with the appropriate response and reduce delays and potential crisis scenarios. Operation efficiency and operational excellence require consistent processes, training and communications for personnel, and flexible systems that can securely integrate information and communications from different types of sensors and different agencies, process the information to detect anomalies, present it in an easy-to- understand fashion tailored for the person's role, and enable decision makers to assign tasks to personnel. Achieving this goal requires the following capabilities:

- **Intelligence management**: The agency needs a secure network to integrate information and communications (data, voice, video) from different sources, including citizens and travelers, video cameras and sensors, and other authorities.
- **Process management**: Converting intelligence into actionable information requires tools to analyze, correlate, and consolidate data. Airport security authority operations personnel need a role-based view of the information.
- **Common Operational Picture**: All participating organizations must be able to share information from their own systems and access information as appropriate to their role. The Common Operational Picture (COP) can be monitored within and across a single airport as well as scaled across all national airports.

Goal 2: Confidentiality, Interoperability, and Information Availability

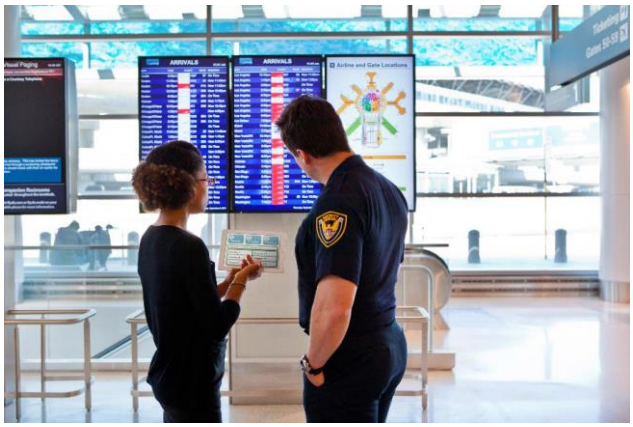
To maintain security of the traveling public across the national transportation system, airport security agencies need ubiquitous, instant, secure, and reliable access to information. That information can come from centralized databases, sensors, or first responders on the scene. Access to information should not be restricted by the user's location, type of network, or device. Rather, it should be governed by policies related to the user's role. Required capabilities to achieve this goal include:

- **Resilient infrastructure that can survive adverse conditions**: Redundancy and resiliency mechanisms help to ensure the network remains available despite partial outages of the underlying infrastructure.

- **Interoperability**: Personnel need the ability to transmit voice, video, and data, including rich-media video such as passenger traffic flow video, over wired or wireless networks. This requires communications devices and networks that support open standards with mission-critical capabilities.
- **Cyber security**: To protect sensitive information, including private citizen and traveler data, airport security agencies need to protect the network from unauthorized access and from internal and external attacks.

Goal 3: Effective Collaboration within Airports and Across the National TSA Systems

Interagency collaboration is often thwarted by incompatible communications systems. Comprehensive communications interoperability requires the following attributes:



- **Multimodal**: Airport security and background personnel need the flexibility to communicate with whatever device is appropriate and available, including analog or digital radio, cell phone, traditional phone, IP phone, or laptop.
- **Cross agency**: Airport security personnel need to be able to collaborate with people in other agencies.
- **Ad hoc**: Organizations involved in national airport security must be able to instantly join their systems into a "system of systems" for the duration of their collaboration.

Goal 4: Surveillance, Monitoring, and Incident Control

Effective procedures and processes to secure national air travel and transportation requirements and ability to respond to crisis scenarios including terrorist attacks, inclement weather, and large-scale disasters requires that personnel can rapidly access all available information as well as information including sensor data. The Internet of Things (IoT) includes machine-to-machine communications between intelligent video surveillance systems, intelligent sensors, and actuators. In addition, the Internet of Everything (IoE) includes passenger information and environmental analytics that can be integrated with airport safety and security capabilities to scale surveillance. TSA security personnel also need the ability to take action remotely, without having to rely on deployed human forces. To meet this goal requires the following capabilities:

- **Ubiquitous sensor system**: Intelligent sensor devices including video cameras, smoke detectors, and explosive sensors can help identify potential conditions leading to incidents. TSA can use this information to identify risks or reduce airport passenger congestions points to open additional security checkpoints or activate additional

resources. Similarly, passenger flow sensors could trigger intelligent passenger flow control systems to reduce waiting times. Detection systems can be placed in areas with high incident rates or in busy public areas. And video surveillance systems with intelligence collect valuable information for real-time analysis or predictive planning.

- **Handheld mobile scanners:** Innovative mobile handheld scanners can be used to quickly scan suspicious travels to determine if they are carrying explosive or other dangerous materials.
- **Distributed behavior analytics**: The network provides the platform for distributed analytics to improve real-time analysis. Video analytics software continuously scans surveillance video feeds for suspicious behavior, rather than relying on human eyes alone, filters predefined events and then takes an action, such as sending an alert, when the event is detected. It is preferable to perform video analytics in the cameras themselves instead of in centralized servers. This conserves network bandwidth and reduces hardware cost and space requirements.
- **Video soft spot surveillance**: Video surveillance monitoring and analytics can be used to identify suspicious repeat behaviors and would be a time-intensive process, but can be optimized within both planning and reviewing incidents that have occurred.
- **Asset and people tracking and tracing**: Airport security sometimes requires tracking the location of people and assets. Safety agencies can accomplish this by embedding intelligence to devices, to automate process workflows. Passenger flow can be monitored and optimized for peak conditions and incident scenarios. Critical security devices can be managed and moved across fixed and mobile networks to reduce downtime and optimize utilization of critical assets.
- **Facial scanning:** Video surveillance capabilities can match faces and personally identify signatures to a database of previously identified individuals.
- **Remote actuation**: Actuators can remotely move or control mechanisms such as airflow control vents and fire sprinklers or they can be triggered by a human or a sensor. For example, if a gas sensor detects a leak, the security supervisor can remotely shut the valve. Alternatively, the alert can trigger an action to automatically shut the valve.
- **Biometrics:** Network-based (wired, wireless) biometric identity devices can be implemented with intelligent tags and new face and iris scanners to identity travelers and optimize the traveler experience. With automated identity, the travel flow is streamlined with automation.
- **Big data mining:** Intelligence gathered from public and private sources of big data can provide capabilities.

Goal 5: Increased Presence at the Checkpoint and Beyond

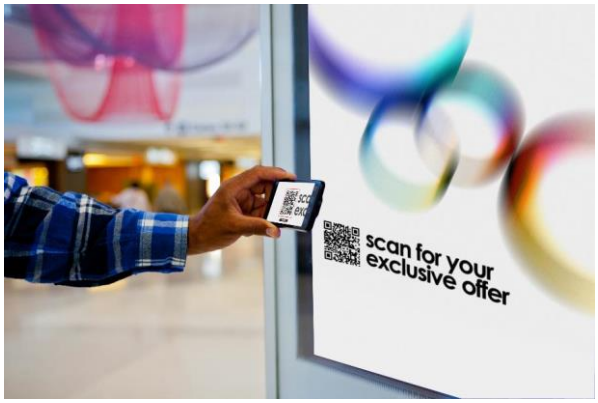
Public visibility and public communications helps improve passenger readiness for travel and can reduce delays in the process. Digital video communications at airport kiosks, via the Internet and social media channels, can help increase the awareness to the public as well as educate

travelers for security requirements in advance. In addition, these capabilities can also provide two-way communications and remote expertise between airport authorities and travelers. Travelers can receive and provide valuable information that can be utilized to improve the optimization of the passenger flow as well as provide information that could be useful to detect security threats. Achieving this goal requires the following capabilities:

- **Interactive video kiosks**: Video kiosks located throughout the airport can provide information to passengers to assist in the security clearance procedures. These kiosks can also provide 2-way capabilities with remote experts including information on flights, safety and security concerns, and language interpretation services for foreign languages.
- **Video communications to mobile devices**: More and more travelers are using mobile devices such as smart phones and tablets when travelling to access travel information, airline tickets, and other applications including real-time video, maps with satellite imagery, Global Positioning System (GPS) tracking, and global databases access via service providers and Wi-Fi. Cisco Mobile Experience (CMX) provides a platform for the airport and airport authorities to provide valuable information and applications to travelers to optimize their flow and also as a channel for communications.
- **Location-based services:** Travelers, personnel, and equipment can be equipped with intelligent tags to provide up-to-date information on their position and perhaps other conditions.
- **Incident Area Network**: If an incident occurs, the Incident Area Network (IAN) can be established for the duration to connect all personnel including local, state, and federal emergency responders at the incident scene with situational awareness and interoperable communications.

Goal 6: Enhanced Communication between Government and Citizens

TSA needs the capability to provide travelers defined ways to report security incidents and ask for help. Cisco Remote Expert provides a high-definition video capability that can be deployed at strategic locations in the airport. In addition, travelers often communicate via mobile devices and smart phones via instant messaging and social media channels and can provide intelligence including photos, information, and video. Required capabilities to meet this goal include:



- **Distributed emergency call system**: When travelers experience or notice safety and security concern or incident, such as a suspicious person, an unattended bag or package, they need a reliable way to report the incident and ask for help.
- **Public Alert Notification**: These systems quickly disseminate warning messages to specific individuals, communities, or organizations in response to an imminent or oncoming emergency or hazardous event. The message describes the event and the affected areas, and provides instructions. For instance, if toxic fumes are emanating from a chemical factory, the agency might need to inform neighboring citizens to seal their windows and doors and wait for further instructions. When confirmation of receipt of the message is required, the system can keep trying until receiving acknowledgement, or else repeat the message at regular intervals for the duration of the incident. Technologies include: Emergency Telephone Alert System (ETAS), Cell Broadcast (CB), voice alert (Public Address), digital signage, and mass media.

Section 3 – Experience

Cisco Internet of Everything: Value for Public Sector:
http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf

International Airport improves operational efficiency and public safety case study
http://www.cisco.com/en/US/prod/collateral/ps6712/ps6718/lviv_international_airport.pdf

2012 U.S. National Convention LTE-based National Security
http://www.cisco.com/en/US/prod/ps6712/new_ways.html