Transportation Security Administration, Requirements and Capabilities Analysis, Innovation Task Force

TSA

Requirements and Capabilities Analysis

Innovation Task Force

Accelerating smart solutions for secure and seamless travel

Mobile Staffing, Scheduling, Time and Attendance (SSTA) Optimization Evaluation Criteria

September 2023

Overview

Mobile Staffing, Scheduling, Time, and Attendance (SSTA) Optimization is TSA's approach to modernize screening resource allocations, leverage data to inform decisions, and realize efficiencies. Mobile SSTA Optimization will be comprised of three separate but integrated solutions: 1.) Bring Your Own Device (BYOD): A mobile solution for TSA employees to access TSA approved applications; 2.) Big Data Platform/Data Lake: A solution capable of ingesting and parsing data from a variety of sources and in varying formats; and 3.) Plan of Day (PoD): In a three phased approach, implement a solution capable of ingesting and visualizing massive amounts of data, there-by enabling screening leadership to draft operational plans in earlier phases and system generated (prescriptive) plans in later phases. All three solutions must be able to integrate and communicate with each other as well as other pre-existing TSA systems. The logic and business rules the system will utilize to flag operational inefficiencies will be provided by TSA.

1. Bring Your Own Device (BYOD) Capability

- A standardized process of enrolling and registering BYOD to ensure operation within a zero-trust security environment.
- Automated / Over-the-air (OTA) device enrollment and provisioning mechanism to reduce enrollment related service requests.
- Standard initialization and configuration of BYOD device (software download, install, health scan)
- Integration with existing identity and access management systems (e.g., Azure AD) for user authentication including but not limited to PIV authentication.
- Capacity to implement derived credentialing on BYOD
- Compatibility with iOS, Android, MacOS, and Windows operating systems.
- Two-factor user authentication to access all workplace apps on BYOD.
- IT capacity to audit and monitor BYOD device to ensure data and user compliance (as pertains to government applications on device)
- Secure containerization and firewall to ensure the safekeeping of government data on device
- Secure containerization and firewall to ensure the safe transit of government data to/from device
- TSA IT possesses remote application control and configuration capabilities on BYOD, in order to enforce security policies
- IT capacity to install security patches and in-house application updates on BYOD
- IT capacity to remotely lock, wipe and retire device (e.g., for end of service or lost devices)
- Capacity to authenticate and monitor user identity in order to safeguard access to secure networks and applications
- Capacity for IT/Security Office to create user and usage reports for auditing purposes.
- Capacity for IT/Security Office to monitor security breaches on BYOD device (e.g., malicious software, unauthorized user behavior, etc.).
- Capacity for administrators and IT/Security Office to maintain/manage underlying data/rules/attributes of BYOD applications (e.g., the cost of business solutions may change over time and the users need an ability to update costs).
- User self-service portal for remote troubleshooting, ticketing and issue reporting.

- Scalable to support expanded usage of BYOD adoption across TSA.
- If a long-term contract is awarded, must be able to obtain a FED-RAMP High certification within one year of award

2. Big Data Platform/Data Lake

- Capable of ingesting, parsing, and configurable visualization (e.g. dash boarding and/or reporting capabilities) of massive amounts of data from a variety of sources and varying formats near real-time
- Must provide a data management plan and data access which aligns to TSA's Enterprise Performance Management Platform (EPMP) as well as other Enterprise Architecture info/data (i.e., the TSA Enterprise Conceptual Data Model (ECDM)) referenced in the TSA Data Artifacts Guidance document.
- Integration with existing identity and access management systems (e.g., Azure AD) for user authentication including but not limited to PIV authentication.
- If a long-term contract is awarded, must be able to obtain a FED-RAMP High certification within one year of award

3. Plan of Day (PoD) Capability

- **General**
  - Leverages permission settings to limit a user's access to data within their AOR
  - Integration with existing identity and access management systems (e.g., Azure AD) for user authentication including but not limited to PIV authentication.
  - Solution must be supported on a TSA approved cloud based platform (behind the TSA firewall)
  - Must have a change management plan to include training end users, system owners and system administrators
  - Must adhere to established privacy regulations, laws and TSA policy and TSA collective bargaining agreement
  - Must provide a data management plan which aligns to TSA's Enterprise Performance Management Platform (EPMP) and the DHS Enterprise Conceptual Data Model (ECDM)
  - If a long-term contract is awarded, must be able to obtain a FED-RAMP High certification within one year of award
- **Phase 1: Informative**
  - Capable of ingesting data massive amounts of data in 15-minute (real-time = objective metric) increments
  - Can ingest and track TSA resources including but not limited to: employee rosters and schedules to include individual shifts, training and leave schedules (only finalized schedules should be integrated into PoD), employee equipment certifications, employee gender, gender balance at checkpoints and baggage locations, individual equipment status (e.g. x-ray machines, body scanner, ETD machines, and CAT/BPS machines), and anticipated equipment repair times (when applicable)
  - Can ingest and track passenger information such as passenger vetting status (e.g. Standard vs. PreCheck), airline name, flight number, destination, and departure time
  - Can create placeholders for information that would be useful but TSA does not have the direct ability to gather yet (CT data etc.)

  - Can ingest and track abstract data sets that could improve predictive demand such as weather (e.g. extreme thunderstorms in various areas could lead to flight delays, shifting passenger loads from one terminal to another as passengers adjust travel plans to navigate departure delays), and traffic events which could impact screening operations (e.g. a car accident outside of airport entrance could lead to an operational lull in passenger load, followed by a drastic spike as the route is cleared).
  - Can ingest and track airline information such as flight statuses, departure and arrival times, flight numbers, passenger capacity of each flight, and passenger checked baggage and accessible property count
  - Can visualize data (in 15-minute increments) which is easy for non-IT professionals to understand and digest
  - Enables users to build custom and/or configurable dashboards based on available data
  - Can implement key performance indicators to flag inefficiencies in a screening operation
- **Phase 2: Interactive**
  - PoD must flag operationally inefficient processes from available information and enable TSA management to interact with current resource allocations to design optimization strategies.
  - Capable of forecasting wait times for incoming passengers, operational load, and resources available to meet the long-term goal
  - Capable of evaluating wait-times at each screening location in 15-minute increments. Wait times longer than 20 minutes should be flagged for action.
  - Can create indicators to denote surpluses or deficiencies in resources.
- **Phase 3: Prescriptive**
  - PoD must notify TSA management when resource allocation inefficiencies are identified and provide recommend actions for recourse.
  - Enable notifications to pre-existing TSA mobile solution to inform impacted TSA employee(s) when scheduled shift(s) and/or training(s) are adjusted to meet operational demand. Notifications must provide the impacted employee with date, time, and location of the new duty station.