

Transportation Security Administration

3300 – PREPAREDNESS AND RESPONSE

Background: Under the Aviation and Transportation Security Act (ATSA), the Transportation Security Administration (TSA) is responsible for security in all modes of transportation. TSA's Transportation Security Operations Center (TSOC) correlates and fuses real-time intelligence and operational information across all modes of transportation, and coordinates within DHS and with other Federal, state and local homeland security agencies for prevention of, and response to, transportation-security related incidents.

Supporting Authorities: Homeland Security Presidential Directive (HSPD) – 5, ATSA (P.L. 107-71), 49 CFR 1540 – 107, 40 USC 44901

WebEOC System: Web-based Emergency Operation Coordination (WebEOC) is a web-based system used by TSA to perform incident management, coordination, and situation awareness functions for all modes of transportation. TSA uses information in WebEOC to provide an operational response as it allows analysts to draw links and patterns to assist with security incident trends. WebEOC collects personally identifiable information (PII) used to facilitate an operational response to suspicious activity of individuals who violate, or are suspected of violating, TSA security regulations, policies and/or procedures. Information is captured on individuals based on 1) individuals who violate, or are suspected of violating, transportation security laws, regulations, policies or procedures; 2) individuals whose behavior or suspicious activity result in referrals by Travel Document Checkers (TDC) to a Behavior Detection Officer (BDO) or a Law Enforcement Officer (LEO) for interview; 3) individuals whose identity must be verified or checked against Federal Watch Lists; and 4) information received from the general public, agency employees, and transportation sector employees to determine if threats, security violations and vulnerabilities, criminal activity and/or non-threat, security-related issues exist.

Item 1a. ~~System Inputs: (GRS 20)~~

Disposition: **Temporary.** ~~Cut off upon successful completion of entry and verification of information. **Destroy/delete** immediately after cutoff.~~

Transportation Security Administration

Item 1b. **Master File:** WebEOC system stores security incident related information such as, but not limited to, the individual's first, middle, and last names; aliases and nicknames; home and business addresses; telephone numbers, employer information; Social Security numbers; other available identification numbers such as drivers license number or passport number; date of birth; languages spoken; nationality; age, sex and race; height and weight; eye color; hair color, style and length; and facial hair, scars, tattoos and piercings, clothing (including colors and patterns) and eyewear. Vehicle information, including make, model, year, color, license plate, state of registry, Vehicle Identification Number (VIN), as well as registration information may also be collected.

The system also collects and compiles logs, and reports from Federal, state, local, tribal, or private sector security officials related to incidents that may pose a threat to transportation or national security. It also stores final incident related documents as related to TSA's Critical Incident Management Group (CIMG). The system stores final CIMG documents such as, but not limited to, on duty rosters, DHS documents/reports, incident maps, other agency reports, press releases, TSA battle rhythm, TSA Briefings, TSA Incident Action Plans, and TSA SITREPs (Situational Reports),.

Disposition: **Temporary.** Cut off at end of calendar year. **Destroy/delete** 10 years after cutoff.

Item 1c. **System Outputs:** (GRS 20)

Disposition: **Temporary.**

Item 1d. **System Documentation:** (GRS 20)

Disposition: **Temporary.**