To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides high-level TSA policy for the development, external coordination, and issuance of standard security programs (SSPs), SSP changes, security program amendments, security directives (SDs), and emergency amendments (EAs). This directive serves to formalize the practices currently used in the issuance of SSPs, SSP changes, security program amendments, SDs, and EAs. This is designed to maximize consultation with, and flexibility for, regulated parties and others, consistent with security needs. This directive also describes the roles and responsibilities individual TSA offices have when developing policy.

2. **SCOPE:** This directive applies to all TSA offices that direct, conduct, or participate in the development, coordination, and issuance of SSPs, SSP changes, security program amendments, SDs, or EAs. Procedures are addressed in Section 7 of the directive. This directive does not apply to the development, coordination, and issuance of Federal Security Director approved local Airport Security Program (ASP) amendments.[1]

3. **AUTHORITIES:**

   A. Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, 115 Stat. 597, November 19, 2001

   B. Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135, November 25, 2002

   C. 49 USC Sections 114, 40113(a), 44903, and 46101

   D. 49 CFR Parts 1542, 1544, 1546, 1548, 1549, 1550, and 1562

4. **DEFINITIONS:**

   A. Airport Security Program (ASP): A security program approved by TSA under 49 CFR 1542.101.

   B. Alternative/Alternate Procedure: A TSA-approved or TSA accepted alternative/alternate measure, used in place of an existing measure required by an SD for U.S. regulated parties or an EA for foreign air carriers, that provides the required level of security.

[1] As described in TSA Delegation of Authority 400.1, Federal Security Directors have the authority to approve and amend an ASP and ensure that the ASP complies with applicable guidance and national policy regarding the FSD's roles and authorities for day-to-day airport security incidents, coordination of air piracy security responses, law enforcement responses to security incidents, and transportation security planning.

C. Emergency Amendment (EA): A security program amendment issued when an emergency requires immediate action that makes the security program amendment process contrary to the public interest. EAs are issued under applicable 49 CFR Parts.

D. EA for Foreign Air Carriers: Since 49 CFR Part 1546 contains no rule requiring foreign air carriers to comply with TSA-issued SDs, TSA must issue an EA rather than an SD to foreign air carriers when additional security measures are necessary to respond to a threat assessment or to a specific threat to civil aviation.

E. Regulated Party: For purposes of this directive, a party operating under an SSP, security program, SD, or EA, approved, accepted, or issued by TSA that is responsible for compliance under TSA regulations or the terms of the SD. For example, an airport operator is a regulated party under 49 CFR Part 1542.

F. Security Directive (SD) (Aviation): A TSA directive setting forth mandatory security measures to a regulated party in the aviation mode issued under applicable 49 CFR Parts, when additional security measures are necessary to respond to a threat assessment or to a specific threat to civil aviation.

G. Security Directive (SD) (Statutory): An order setting forth mandatory measures to an affected party in a transportation mode in accordance with 49 USC Section 114(l)(2). Non-aviation SDs were created in ATSA in 2001. The authority is codified at 49 USC Section 114(l) (2). ATSA did not remove TSA's authority to issue aviation SDs. While TSA has authority to issue SDs under this statute to any entity in the transportation sector, TSA has other tools to use for most aviation purposes and thus refers to SDs under the statute as "statutory" SDs.

H. Security Program: A set of security measures approved or accepted by TSA for a regulated party required to operate under a security program by 49 CFR.

I. Security Program Amendment: An amendment revises the TSA approved or accepted security program of a regulated party or parties to include alternative/alternate or additional security measures. Except for Emergency Amendments, prior notice to and comment by affected regulated parties is required under applicable 49 CFR Parts.

J. Sensitive Security Information (SSI): As described in 49 CFR Part 1520.5, and in general, information about transportation security activities that, if publicly released, would be detrimental to transportation security.

K. Standard Security Program (SSP): TSA provided standard security measures that may serve as the baseline for a particular type of security program required under 49 CFR. A regulated party's security program typically consists of the appropriate standard security program, any alternative/alternate procedures approved by TSA, and any amendments to that party's security program approved by TSA.[2]

[2] In the case of foreign air carriers regulated under 49 CFR Part 1546, TSA "accepts" rather than "approves" the carrier's SSP together with any amendments and alternative procedures to the security program.

L. SSP Change: A change or revision to the contents of a particular SSP.

5. RESPONSIBILITIES:

A. The Office of Security Policy and Industry Engagement (OSPIE) has primary responsibility for developing, coordinating, and issuing security policy documents covered by this MD. All TSA offices and individuals involved in developing, coordinating, issuing, or otherwise supporting SSPs, SSP changes, security program amendments, SDs, and EAs are responsible for ensuring that these activities are conducted in accordance with this directive, and other applicable laws, regulations, and policies.

B. OSPIE is responsible for:

(1) Coordinating with OGS, to determine the appropriate security requirements that should be included in SSPs, SSP changes, security program amendments, SDs, and EAs;

(2) Conducting the necessary stakeholder outreach with affected domestic regulated parties, and as appropriate their associations, to ensure proper communication, consultation and coordination in the development and implementation of SSPs, SSP changes, security program amendments, SDs, and EAs;

(3) Participating in stakeholder outreach, in cooperation with Office of Global Strategies (OGS), with affected foreign regulated parties, and as appropriate their associations, when developing SSPs, SSP changes, security program amendments, and EAs affecting domestic operations;

(4) Coordinating OGS participation in stakeholder outreach with affected domestic regulated parties, and as appropriate their associations, when developing SSPs, SSP changes, security program amendments, and SDs affecting international operations;

(5) Coordinating with OGS, to draft SSPs, SSP changes, security program amendments, SDs, and EAs and determining timelines for their implementation; and

(6) Coordinating and tracking the review process through all responsible Assistant Administrator offices and the TSA Administrator for all SSPs, SSP changes, security program amendments, SDs, and EAs.

C. Office of Global Strategies (OGS) is responsible for:

(1) In cooperation with OSPIE, determining the appropriate security requirements that should be included in SSPs, SSP changes, security program amendments, SDs, and EAs;

(2) Conducting the necessary stakeholder outreach with affected international regulated parties, and as appropriate their associations, and foreign governments and international organizations, to ensure proper communication, consultation, and coordination in the development and implementation of SSPs, SSP changes, security program amendments, SDs, and EAs;

(3) Participating in stakeholder outreach, in cooperation with OSPIE, with affected domestic regulated parties, and as appropriate their associations, when developing SSPs, SSP changes, security program amendments, and SDs affecting international operations;

(4) Coordinating OSPIE participation in stakeholder outreach with affected foreign regulated parties, and as appropriate their associations, when developing security program amendments, SSP changes, and EAs affecting domestic operations;

(5) In cooperation with OSPIE, drafting SSPs, SSP changes, security program amendments, SDs, and EAs and determining timelines for their implementation; and

(6) Communicating the requirements described in SSPs, SSP changes, security program amendments, SDs, and EAs with an international impact to international inspectors within OGS to implement effective compliance and inspection oversight overseas.

D. Office of Security Operations (OSO) is responsible for:

(1) Ensuring that operational impact on domestic field operations is evaluated during the drafting/creation phase of SSPs, SSP changes, security program amendments, SDs, or, EAs.

(2) Ensuring that requirements in SSPs, SSP changes, security program amendments, SDs, or EAs are clearly delineated during the drafting/creation phase, so that field inspectors can provide effective compliance and inspection oversight.

(3) Communicating the requirements described in SSPs, SSP changes, security program amendments, SDs, and EAs with an operational impact on domestic operations, so that field inspectors can provide effective compliance and inspection oversight.

E. Office of Chief Counsel (OCC) is responsible for reviewing SSPs, SSP changes, security program amendments, SDs, and EAs and the procedures used to issue them, to ensure legal sufficiency and enforceability, and to identify and provide counsel on legal risks.

F. Office of Intelligence and Analysis (OIA) is responsible for providing information and guidance in the identification of current threats and other intelligence that may form the basis for SSPs, SSP changes, security program amendments, SDs, or EAs.

G. Office of Security Capabilities (OSC) is responsible for providing risk analysis to assist other TSA offices involved in making determinations on implementation of SSPs, SSP changes, security program amendments, SDs, or EAs.

H. Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) is responsible for providing information and guidance as appropriate on applicable TSA security programs that may form the basis for SSPs, SSP changes, security program amendments, SDs, or EAs.

I. Office of Policy Coordination and Intergovernmental Affairs (OPCIA) is responsible for:

(1) Reviewing final SSP, SSP change, security program amendment, SD, and EA packages that require Administrator signature and driving items, initiatives, and issues of interest to the Administrator and Deputy Administrator.

(2) Representing the Administrator in coordination of significant policy changes issued via SSPs, SSP changes, security program amendments, SDs, or EAs, with DHS Headquarters, other DHS Components as necessary, National Security Staff, and interagency partners.

6. POLICY:

A. In developing SSPs, SSP changes, security program amendments, SDs, and EAs, TSA will consult with affected parties or regulated parties, including their associations, to the extent practicable and appropriate. The consultation process allows TSA, the affected parties, and their associations to share information and address concerns before TSA issues regulatory documents.

B. TSA may approve an SSP change, security program amendment, or a change to an SD or EA if the agency determines that safety and the public interest require these revised measures and the proposed amendment provides the level of security required in the SSP, security program, SD, or EA.

C. TSA may initiate an SSP, SSP change, or an amendment to a security program if the agency determines that safety and the public interest require it.

D. TSA may issue an EA to any security program if the agency determines that there is an emergency requiring immediate action that makes notice and comment procedures contrary to safety and the public interest.

E. TSA may issue an EA for foreign air carriers if the agency determines that additional security measures are necessary to respond to threat assessments or a specific threat to civil aviation. The EA sets forth mandatory measures. When TSA issues an EA to foreign air carriers, it may at the same time issue an SD to U.S. aircraft operators.

F. TSA may issue an SD (Aviation) to airport operators, U.S. aircraft operators, indirect air carriers, or certified cargo screening facilities, in accordance with TSA regulations, if the agency determines that additional security measures are necessary to respond to a threat assessment or a specific threat to civil aviation. The SD sets forth mandatory measures. When TSA issues an SD to U.S. aircraft operators, it may, at the same time, issue an EA to foreign air carriers. SDs and EAs are not to be used to mitigate routine security concerns or vulnerabilities.

G. TSA may issue an SD (Statutory) in accordance with 49 USC Section 114(l)(2) if TSA "determines that a … security directive must be issued immediately in order to protect transportation security." The SD sets forth mandatory measures. TSA may issue an SD "without providing notice or an opportunity for comment and without prior approval of the Secretary [of the Department of Homeland Security.]" In accordance with 49 USC Section 114(l)(2), any SD (Statutory) issued under that paragraph shall remain effective for a period not

to exceed 90 calendar days unless ratified or disapproved by the Transportation Security Oversight Board or rescinded by the Administrator.

H. During the creation of all SDs and EAs, two duration dates will be assigned. The first date will be the expiration date. This date will be part of the document and will be shared with external entities who receive the SD or EA. The second date will be the Sunset Date. This date will be kept internal to TSA and will serve as the date where a decision will be made by the agency to either cancel the SD or EA or convert it into a security program change. Factors for this decision will include a comprehensive intelligence review, assessment of risk based relevance and operator performance/compliance. This lifecycle analysis will ensure that SDs and EAs are not permanent in nature and that the security program change process is routinely used as the vehicle for long term regulatory requirements.

7. PROCEDURES: TSA offices and individuals involved in developing, coordinating, issuing, or otherwise supporting SSPs, SSP changes, security program amendments, SDs, or EAs will do so in accordance with procedures contained in any TSA Standard Operating Procedures (SOPs) issued for such purpose. TSA offices will work together to prepare these SOPs within 90 days of the issuance of this MD. These SOPs will be presented to the Administrator for review and approval.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature, unless otherwise specified.

APPROVAL

Signed March 15, 2012

_____ _____

John S. Pistole Date
Administrator

EFFECTIVE

_____

Date

Distribution: Offices of Chief Counsel, Global Strategies, Intelligence and Analysis, Security Operations, Law Enforcement/Federal Air Marshals Service, Security Capabilities, Policy Coordination and Intergovernmental Affairs, and Security Policy and Industry Engagement

Point-of-Contact: Office of Security Policy and Industry Engagement