Transportation Security Administration

OFFICE OF INFORMATION TECHNOLOGY

TSA MANAGEMENT DIRECTIVE No. 1400.21
TSA INFORMATION BOARDS MANAGEMENT

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

REVISION: This revised directive supersedes TSA MD 1300.3, *Watchlists WebBoard Management*, dated August 9, 2010.

1. **PURPOSE:** This directive provides TSA policy and procedures for user and system management of the TSA Information Boards (TSA infoBoards).

2. **SCOPE:** This directive applies to all TSA employees, contractors, vendors, detailees, others working on behalf of TSA, and non-TSA employees authorized to access TSA infoBoards.

3. **AUTHORITIES:**

   A. DHS/ALL/PIA-027(c) Watchlist Service (WLS) Privacy Impact Assessment (PIA) Update, August 11, 2014

   B. DHS MD 11042.1, Safeguarding Sensitive but Unclassified Information

   C. DHS MD 11052, Internal Security Program

   D. DHS MD 4400.1, DHS Web (Internet, Intranet, and Extranet Information) and Information Systems

   E. DHS Sensitive Systems Policy Directive (PD) 4300A

   F. DHS Sensitive Systems Policy Handbook 4300A

   G. DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

   H. NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

   I. TSA MD 100.0-2, Office of Inspection Roles and Responsibilities

   J. TSA MD 300.8, Acquisition Program Review and Reporting

   K. TSA MD 300.12, Program Requirements Review and Approval

   L. TSA MD 1100.75-3, Addressing Unacceptable Performance and Conduct

   M. TSA MD 1100.73-5, Employee Responsibilities and Code of Conduct

   N. TSA MD 1400.3, Information Security

   O. TSA MD 2800.15, Foreign Visitor Management

P. TSA MD 2810.1, SSI Program

Q. TSA MD 3700.4, Handling Sensitive Personally Identifiable Information

R. TSA Information Assurance Handbook

S. TSA SSI Policies and Procedures Handbook

4. **DEFINITIONS:** See the *TSA Information Assurance Handbook* for additional definitions.

A. Community of Interest (COI): A gathering of people assembled around a topic of common interest. Each COI's users are active on one or more boards/sites.

B. COI Sponsor: At HSIN, a COI Sponsor has authoritative responsibility over that COI's users, which includes managing the existence of that COI's boards.

C. Foreign National: An individual who is a citizen of a country other than the United States.

D. Homeland Security Information Network (HSIN): An information-sharing "network of trust" service designed to meet the sensitive but unclassified (SBU) information sharing requirements of the homeland security enterprise.

E. Information Technology: Any equipment or interconnected system(s) or subsystem(s) of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.

F. Nominator: A TSA employee who recommends new users for HSIN accounts. The same individual may act as Nominator and Validator to update a TSA infoBoards' user account, if the user has been previously vetted.

G. Primary COI Sponsor: The TSA employee who has authoritative responsibility over all users accessing TSA infoBoards, which includes managing the existence of all TSA infoBoards. The entire collection of boards is the primary COI managed under this directive.

H. Security Coordinator: The individual at the requestor's organization who is permitted by policy and regulation to validate completion of COI-appropriate training by their employee prior to obtaining access to TSA infoBoards.

I. TSA Information Boards (TSA infoBoards): The HSIN or TSA IT system that hosts a single TSA infoBoards environment. The HSIN IT system is considered the gathering place for a single COI, known as "TSA infoBoards" and contains all TSA infoBoards' boards/sites located on that system. Each board/site on each IT system (and within the COI on the HSIN IT system) shall be sponsored by only one TSA office.

J. TSA infoBoards Board Administrator: Any TSA employee who is designated to administer an individual board/site on behalf of the Executive Council Member (or TSA AA) who sponsored the board/site. A Board Administrator shall belong to the same TSA office as the sponsoring Executive Council Member. One primary Board Administrator shall be appointed for each board/site, although alternate(s) may be designated.

K. TSA infoBoards Executive Council: A governance board and decision-making body for TSA coordination, collaboration, and information sharing on TSA infoBoards. The TSA infoBoards Executive Council shall consist of the following standing, voting members:

(1) Chair: OIT Assistant Administrator (AA)/Chief Information Officer (CIO);

(2) Vice Chair: Assumes the responsibilities of the Executive Council Chair in the Chair's absence. It is a rotational position assigned on an annual basis among members of the Executive Council; and

(3) Member: Assistant Administrator from each TSA office sponsoring a board/site.

L. TSA infoBoards System Owner: The TSA employee who is responsible for the overall procurement, development, integration, modification, and/or operation and maintenance of all TSA infoBoards. There shall be only one TSA infoBoards System Owner, although an alternate may be designated. Note: There is also a DHS employee who acts as the HSIN System Owner for all matters relevant to HSIN, including TSA infoBoards.

M. TSA infoBoards User: TSA employees, TSA contractors, vendors, detailees, others working on behalf of TSA, other government employees, and commercial employees who regularly access TSA infoBoards. (a) Each TSA infoBoards user shall be associated with at least one TSA infoBoards board/site. (b) Each non-TSA user (e.g., other government employee or commercial employee) shall be associated only with TSA infoBoards hosted at HSIN.

N. TSA Representative: Any TSA employee who is the primary point of contact (POC) for the user. May act as a TSA Sponsor or a TSA infoBoards Board Administrator. Their primary role at TSA may be such as Principal Security Inspector (PSI) or International Industry Representative (IIR).

O. TSA Sponsor: Any TSA employee permitted by guidelines, policy, and/or regulation to authorize access to TSA infoBoards.

P. Validator: Any TSA employee permitted by guidelines, policy, and/or regulation to approve new users for a HSIN account. The same individual may act as Nominator and Validator to update a TSA infoBoards' user account (especially for Watchlists access), if the user has been previously vetted by DHS.

5. RESPONSIBILITIES:

A. The DHS Office of Chief Information Officer (OCIO) is responsible for:

(1) Hosting HSIN;

(2) Ensuring all foreign nationals have been formally vetted prior to gaining access to HSIN and TSA infoBoards.

(3) Validating the identity (or "identity proofing") and creating HSIN accounts for authorized

and approved users; and

(4) Providing the communication environment and user access controls.

B. The TSA OIT is responsible for:

(1) Managing all IT systems that host the TSA infoBoards, as accessed solely by TSA employees; and

(2) Monitoring the specific content of TSA infoBoards at HSIN.

C. The TSA Chief Security Officer (CSO) Foreign National Vetting Office is responsible for coordinating applications and submitting foreign nationals for vetting prior to granting access to HSIN and TSA infoBoards.

D. The TSA infoBoards Executive Council is responsible for:

(1) Approving and overseeing the implementation of TSA infoBoards strategy and policies, including the budgets for TSA infoBoards total life cycle costs;

(2) Enhancing consistency in information sharing, policy, and procedures across TSA infoBoards with respect to operating environments;

(3) Identifying support needed by both the TSA stakeholder offices and OIT to facilitate the implementation of TSA's stakeholder collaboration strategy; and

(4) Addressing and resolving issues that arise concerning HSIN's implementation of TSA infoBoards (or "Site Collection").

E. The TSA infoBoards Executive Council Chair is responsible for:

(1) Implementing the recommendations of the TSA infoBoards Executive Council;

(2) Coordinating with HSIN (as lead) to investigate misuse and enforce penalty in the HSIN environment; and

(3) Coordinating with the TSA Office of Inspection (OOI) and Office of Chief Counsel (OCC) to investigate misuse and enforce penalty in the TSA environment.

F. Each TSA infoBoards Executive Council Member is responsible for:

(1) Approving and overseeing the implementation of TSA infoBoards strategy and policies, establishing a total life cycle estimate for fiscal year funds (budgets);

(2) Permitting all usage on all boards/sites sponsored by their office, including facilitating collaboration;

(3) Delegating responsibility to nominate and validate users, to their respective TSA

infoBoards Administrator(s), Nominator, and Validator; and

(4) Resolving security concerns.

G. Each Security Coordinator is responsible for:

(1) Validating any COI-appropriate and other TSA requirements are satisfied by their staff member prior to TSA granting access to TSA infoBoards; and

(2) Ensuring that all security requirements (e.g., data handling) are satisfied by their organization's systems.

H. Each TSA Representative is responsible for serving as the primary point of contact for TSA infoBoards users, including accepting requests for accounts.

I. Each TSA Sponsor is responsible for:

(1) Authorizing access to TSA infoBoards; and,

(2) Establishing all users' needs prior to gaining access to HSIN and TSA infoBoards.

J. Each TSA infoBoards Board Administrator is responsible for:

(1) Managing and administering the TSA infoBoards' user accounts;

(2) Nominating and validating requests for new user accounts;

(3) Ensuring that each board/site's users are appropriately validated, trained, and documented per guidelines, policy, and/or regulation; and

(4) Ensuring that each board/site's information is appropriately posted and managed per guidelines, policy, and/or regulation.

K. The TSA infoBoards System Owner is responsible for:

(1) Managing content on all TSA infoBoards' site(s)/board(s);

(2) Ensuring TSA infoBoards' content is accessible by all users; and

(3) Acting as Site Collection Administrator for matters related to HSIN.

L. TSA infoBoards Users are responsible for retrieving and implementing COI postings, including but not limited to Security Directives (SD), compliance status, and policy updates for each TSA infoBoards boards/sites.

M. The Office of Inspection (OOI) is responsible for investigating misuse of TSA infoBoards.

N. The Office of Chief Counsel (OCC) is responsible for determining and enforcing penalty and disciplinary or criminal action if a user violates the TSA infoBoards Terms of Use.

6. POLICY:

A. The TSA infoBoards is the only official means, other than the Secure Flight system, for the issuance of Special Posting Files and the dissemination of Special Posting Files and No Fly, Selectee, and Cleared Lists to applicable regulated parties.

B. A TSA infoBoards user shall be at least a Site Visitor (responsible for viewing items only) but may also be a Site Member (responsible for adding content) of a site/board. Authorized representatives of regulated entities may only become Site Visitors, not Site Members.

C. All TSA infoBoards users shall be compliant with DHS 4300A Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook, TSA MD 1400.3 Information Technology Security Policy, and the TSA Information Assurance Handbook.

(1) Users shall be required to complete IT Security Awareness and Sensitive Security Information (SSI) training within 60 days of receiving access to TSA infoBoards. Refresher training must be completed annually thereafter. User accounts and access privileges shall be disabled for those TSA infoBoards users who have not completed annual refresher training in a timely manner.

(2) Remote access connection to DHS/TSA networks shall be considered a privileged arrangement to conduct sanctioned TSA business. Therefore, remote access rights shall be expressly granted, in writing, by the TSA Information Assurance and Cyber Security Division (IAD).

i. Regulated entities shall maintain proof of eligibility to access TSA.

ii. Authorized representatives of regulated entities shall renew proof of eligibility at least annually (via submitting a copy of a binding agreement with a current TSA infoBoards User who is a regulated entity containing terms and conditions).

(3) The user's remote access connection to DHS/TSA networks may be terminated for unauthorized use, at the sole discretion of DHS/TSA.

(4) The user shall satisfy requirements to work with and safeguard SSI, and Personally Identifiable Information (PII). All users shall understand and rigorously follow DHS and TSA requirements, policies, and procedures for safeguarding SSI and PII. Users shall be required to complete annual online training for SSI, Informational Security, and TSA Privacy training.

(5) The user shall be responsible for the security of TSA data otherwise stored or processed by the user regardless of who owns or controls the underlying systems while that data is under the user's control. All TSA data, including but not limited to PII, SSI, and sensitive but unclassified (SBU) shall be protected according to DHS and TSA security policies and mandates.

(6) Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing DHS/TSA IT assets are expected to actively apply the practices specified in the TSA Information Assurance Handbook and applicable IT Security Technical Standards, including not co-mingling with non-TSA data and proper destruction when necessary.

(7) The user shall comply with Sensitive PII disposition requirements stated in the TSA Information Assurance Handbook, applicable Technical Standards and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*.

D. All users of TSA infoBoards shall complete TSA Form 1403, Computer and Personal Electronic Device (PED) Access Agreement and DHS Form 11000-6, Non-Disclosure Agreement (NDA) prior to receiving a HSIN account and access to TSA infoBoards.

E. The user shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA IAD and management, as directed by the TSA infoBoards Board Administrator.

F. TSA shall ensure that only individuals meeting the trustworthiness requirements associated with sensitive security and/or critical data are allowed to access TSA official information.

G. Third party agreements that directly, or indirectly, impact DHS/TSA IT assets or information are required and shall include explicit coverage of all relevant personnel security requirements including security roles and responsibilities for third-party personnel. This includes agreements involving accessing DHS/TSA IT assets by authorized representatives of regulated entities.

H. Only U.S. Citizens are allowed access to DHS systems and networks; however, at times a need exists to grant access to foreign nationals. Foreign nationals shall be vetted by DHS prior to receiving a HSIN account and access to TSA infoBoards.

I. If misuse of TSA infoBoards is identified, the TSA infoBoards System Owner or TSA Board Administrator(s) will immediately report the incident to the TSA infoBoards Executive Council Chair and the OOI. The OOI will investigate the incident and provide recommendations (e.g., corrective, disciplinary) to the Executive Council Chair. The Executive Council Chair and OCC will determine if user access will be revoked and disciplinary actions enforced.

J. TSA infoBoards users are prohibited from allowing anyone else (including other TSA infoBoards users) to use their TSA infoBoards user login information to access the HSIN environment.

7. **PROCEDURES:** Reference HSIN and TSA applicable guides, manuals, Standard Operating Instructions (SOIs) and Standard Operating Procedures (SOPs), and other process directions relevant to and specific to the program and functions identified in this directive. Direct programmatic inquires to the appropriate subordinate program office point-of-contact.

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

APPROVAL

Signed February 25, 2016

______________________________________ _______________
Stephen Rice Date
Assistant Administrator
Chief Information Officer
Office of Information Technology

EFFECTIVE

____
Date

Distribution: Assistant Administrators and equivalents, Business Management Office Directors
Point of Contact: TSA-infoBoards@tsa.dhs.gov