



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 TSA policy and procedures for required security measures regarding the TSA Instant Messaging System (IMS) and TSA Instant Messaging (IM).
2. **SCOPE:** This directive applies to all TSA employees and contract personnel and other authorized users of the TSA IM System.
3. **AUTHORITIES:**
 - A. *The Electronic Communications Privacy Act of 1986*, Public Law 99-508, October 21, 1986, as amended (codified in Title 18, United States Code)
 - B. OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*
4. **DEFINITIONS:**
 - A. Chief Information Security Officer (CISO): The Department of Homeland Security (DHS) official with agency responsibility for information security on all DHS networks.
 - B. Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.
 - C. Critical Infrastructure Information (CII): According to 6 C.F.R. Part 29, CII is information not customarily in the public domain and related to the security of critical infrastructure or protected systems.
 - D. Federal Record: According to 44 U.S.C. 3301, this term includes all materials regardless of physical form (including IMs) that are made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.
 - E. Federated Security: For purposes of this MD, federated security is a process whereby a security relationship has been formed between two discrete IM systems that provides for minimum levels of acceptable security.
 - F. Information System Security Manager (ISSM): DHS appointee with responsibility for information security on all TSA networks.

- G. Information System Security Officer (ISSO): TSA individual responsible for information security on an assigned set of systems or locations.
- H. Instant Message (IM): Information created or received on an electronic message system (i.e., an instant messaging system), including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents that may be transmitted with the message.
- I. Instant Messaging System (IMS): A computer application used to create, receive and transmit messages and other documents in near real-time, excluding file transfer utilities (software that transmits files between users but does not retain any transmission data), and data systems used to collect and process data that have been organized into data files or data bases on computers.
- J. Permanent IMs: IMs that contain content that is appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal or fiscal purpose.
- K. Record Retention Schedule: A document providing mandatory instructions for what to do with Federal records (and non-record materials) is no longer needed for current government business, with provisions of authority for the final disposition of recurring or nonrecurring Federal records. Includes the SF 115, the General Records Schedules, and the agency records schedule, which when completed becomes a comprehensive records schedule that also contains agency disposition instructions for non-record materials. All Federal records schedules must be approved by NARA.
- L. Sensitive Security Information (SSI): SSI is defined in 49 C.F.R. Part 1520.5 as information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.
- M. Sensitive But Unclassified/For Official Use Only (SBU/FOUO): The term used to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information impacting the National Security of the United States and classified Confidential, Secret or Top Secret under Executive Order 12958 is not to be considered SBU/FOUO. SBU/FOUO is not considered classified information.
- N. System Security Plan (SSP): The SSP defines the environment within which a system will operate and the protective measures which are to be applied. The SSP includes sections on access control, authentication, accountability, audit, object reuse, communications security, integrity, availability, and security administration. For each section, the environmental measures that are needed to provide the required level of protection are documented together with the security requirements to be implemented in the system.

- O. Temporary IMs: Temporary IMs are IMs that contain content that is approved for either immediate disposal, or for disposal after a specified period of time or an event, in accordance with the appropriate NARA records retention schedule.
- P. TSA Users: Individuals authorized to use TSA IMS as part of their assigned official duties, including TSA employees, contractor personnel, and authorized guests using TSA supplied resources.

5. RESPONSIBILITIES:

- A. Assistant Administrator for Operational Process and Technology/Chief Information Officer (CIO) is responsible for:
 - (1) Approving non-standard IM implementations.
 - (2) Advising the DHS CISO on methods for securing IMSs.
 - (3) Enforcing DHS/TSA IM security policies.
 - (4) Approving TSA IMS changes.
 - (5) Ensuring IMS security controls are in place and functioning as intended.
 - (6) Ensuring IMS security controls provide the security features outlined in applicable TSA system documents and the System Security Plan.
 - (7) Ensuring an appropriate disaster recovery plan is in place.
- B. Certifying Officials are responsible for certifying that adequate security controls are in place for IMSs.
- C. Designated Accrediting Authority (DAA) is responsible for:
 - (1) Ensuring adequate IM security controls are in place prior to accreditation of the system.
 - (2) Accepting the risk and authorizing operation of IMSs
- D. ISSM is responsible for:
 - (1) Reporting TSA information security matters directly to the DHS CISO.
 - (2) Providing TSA management and program oversight to TSA ISSOs on matters related to information security.
- E. IM Users are responsible for:
 - (1) Using and protecting personal IM accounts in accordance with established policies and procedures.

- (2) Entering appropriate information into the IMS to properly ensure and safeguard system security, appropriateness, and TSA records.
- (3) Saving and disposing of IMs as appropriate pursuant to the applicable records retention schedule.

F. System/Network/IM Administrators are responsible for:

- (1) Ensuring IM security controls are in place and functioning as intended.
- (2) Ensuring IMS security controls provide the security features outlined in applicable TSA system documents and the System Security Plan.
- (3) Testing and applying system patches in a timely manner.
- (4) Removing or disabling unnecessary services and applications from IM servers.
- (5) Configuring IMS user authentications.
- (6) Reviewing and analyzing log files.
- (7) Backing up data as required by the System Security Plan.
- (8) Protecting IMS code protection controls.

G. System Owner is responsible for:

- (1) Operating and maintaining IMS security and operations in accordance with applicable policies and operational needs.
- (2) Defining usage, controls and access requirements.

H. ISSO is responsible for:

- (1) Ensuring a disaster recovery plan is in place.
- (2) Ensuring IMS security controls provide the security features outlined in applicable TSA system documents and the System Security Plan.
- (3) Conducting periodic IMS scans using appropriate vulnerability assessment tools.

6. POLICY:

- A. All TSA IM communications shall utilize only TSA approved IM Server(s) and IM client products.
- B. Direct access to Commercial IM services (e.g., Yahoo®, Microsoft®, AIM®) is prohibited.

NOTE: TSA approved external IM services may be accessed via the TSA Intranet or Extranet IM gateways.

- C. All IMs sent and/or received by the IM system become the property of TSA, and TSA reserves the right to monitor and/or log all IM communications without notice.
- D. TSA users will not perform or advise others to perform actions to bypass IM screening tools (e.g., renaming file extensions, etc).
- E. All IM messages sent by an IM system user will be identified by their TSA domain user ID, approved email ID, or other officially approved alias only. Users are prohibited from using any user assigned or unofficial alias for any IM communications.
- F. TSA users shall not utilize IMs to communicate sensitive information, including, but not limited to: classified information, SSI, personally identifiable information (PII), and CII either in the text of an IM message or in an attached document unless protected as specified in directives covering these categories of information.
- G. IM use is permitted for communications between TSA internal users and between internal users and TSA authorized extranet users. All TSA internal users and authorized extranet users shall have individually identifiable accounts on the TSA/DHS network.
- H. IM use is not allowed for external communication with users that are outside of the TSA internal network, Extranet, or DHS federated network except through approved gateways.

NOTE: External communication is defined as communication between an individual with an account on the TSA network and an individual who does not have an account on the TSA/DHS network.

- I. IMS usage shall comply with [TSA Information Technology Security Policy \(ITSP\) Handbook](#), Chapter 3, Section 6, *Privacy and Acceptable Use*, and [TSA MD 1100.73-5, Employee Responsibilities and Conduct](#).
- J. TSA IMS may be used for messages that meet the criteria of Permanent, Temporary and Transitory as defined in [DHS Document 550, DHS Records Management Handbook](#), and each user is responsible for identifying and preserving IMs that constitute a record pursuant to applicable records statutes, regulations and policies.
- K. IMs containing active links to unofficial Internet web sites are prohibited; however, active links to approved TSA internal sites, DHS sites, and other official Government sites are permitted.
- L. All IM traffic will be processed through a TSA-approved and managed IM server that supports logging. Logs shall be retained as specified by TSA records retention schedules.
- M. Deviations and/or waivers to any part of this directive must have approval in accordance with [TSA ITSP Handbook](#), Chapter 3, Section 27, Security Policy Waivers and Deviations.

7. PROCEDURES:

- A. All IM communications that traverse the Internet shall be cryptographically protected from unauthorized disclosure or modification, and shall provide non-repudiation with proof of message origin when technically and operationally feasible.

- B. All IMs and attachments will be scanned for viruses, spyware, malware, and inappropriate content using TSA approved IA products. All quarantined IMs will be cleansed and delivered if possible, or deleted if cleansing is not possible, and users will be notified of any actions taken on incoming IMs.
 - C. When the origin of an IM is in question, IMS Users will take sufficient additional steps to authenticate the source through alternative communications media before opening any attached documents or performing official actions based solely on the IMs content.
 - D. Measures will be taken to provide anti-SPIM (i.e., Spam Instant Message) protection to monitor all Intranet and Extranet IM traffic.
8. **EFFECTIVE DATE AND IMPLEMENTATION:** This policy is effective immediately upon signature.

APPROVAL

Signed
Michael Golden, Assistant Administrator for Operational
Process and Technology/Chief Information Officer

8/10/2007
Date

Filing Instructions: File 200.1.1
Effective Date: Date of Signature
Review Date: Two years from Effective Date
Distribution: TSA employees, contract personnel and authorized users
Point-of-Contact: OPT BMO Communications, OPTBMOCcommunications@dhs.gov