BY ORDER OF THE COMMANDER
AIR MOBILITY COMMAND

AIR MOBILITY COMMAND
INSTRUCTION 24-101V4

10 AUGUST 2016

Transportation

MILITARY AIRLIFT/AIR TRANSPORTATION SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: HQ AMC/A4TI

Certified by: HQ AMC/A4T
(Col Christine M. Erlewine)

Supersedes: AMCI24-101V4, 26 December 2013

Pages: 34

This publication implements Air Force Policy Directive (AFPD) 24-1, *Personnel Movement,* and AFPD 24-2, *Preparation and Movement of Air Force Material.* This volume describes automation and communication procedures for developing, operating, and managing Air Mobility Command (AMC) transportation computer systems used to control and record the movement of passengers, cargo, and mail for all AMC aerial ports and air terminals. It also provides guidance for those non-AMC organizations that are using AMC automated systems. This volume applies to Air Force Reserve Command (AFRC) units when performing air transportation duties at AMC locations and/or on AMC's behalf, but not Air National Guard (ANG) units. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct Supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, Publications and Forms Management, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier

waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. This document requires collecting and maintaining information protected by the Privacy Act of 1974, authorized by 10 USC, 8013, Secretary of the Air Force: powers and duties; delegation by, and Executive Orders 9397, 9838, 10450, and 11652. System of records notice F024 AF USTRANSCOM D DOD, Global Air Transportation Execution System (GATES) (August 3, 1999, 64 FR 42098) applies.

SUMMARY OF CHANGES

This document has been revised and must be completely reviewed. Major changes include: updated office symbols and internet links, updated WASO responsibilities, addition of physical security for DGATES servers, added additional A4TI and A6IB responsibilities, updated DGATES satellite connection billing, renamed the Deployment Processing Center (DPC) to the Remote Manifesting Resolution Center (RMRC), and updated the procedures to utilize the RMRC.

1. General.

1.1. Three separate functional community requirements are integrated into GATES: AMC and aerial port operations, United States Transportation Command (USTRANSCOM) with the Defense Courier Division (DCD), and the Surface Deployment and Distribution Command (SDDC). As a joint system, GATES is primarily managed and funded by USTRANSCOM. This instruction only applies to GATES as it pertains to AMC's aerial port operations and air transportation.

1.2. AMC must provide automation support and data capture of aerial port transportation activities to meet wartime mission requirements as well as sustain normal peacetime operations. Automation is required to support aerial port operations and AMC financial management obligations, as well as to enable In-Transit Visibility (ITV) for cargo and passengers moving on AMC airlift.

2. Responsibilities.

2.1. **Headquarters (HQ) AMC/A4T will:**

2.1.1. Provide policy guidance on aerial port operations.

2.1.2. Oversee transportation systems and development planning with HQ AMC/A4TI.

2.1.3. Oversee policy changes that affect transportation automation systems with HQ AMC/A4TI.

2.1.4. Review system metrics and identify problem areas that impact efficient operation of transportation automation systems and take appropriate action to facilitate correction.

2.1.5. Serve as a voting member on the USTRANSCOM Joint Functional Requirements Board (JFRB) for GATES.

2.2. **HQ AMC/A4TI will:**

2.2.1. Serve as the Air Functional Manager for GATES and in this capacity will:

2.2.1.1. Coordinate with both internal and external program managers of automated information systems pertaining to the exchange of information between their systems and GATES.

2.2.1.2. Develop and review concepts of operations (CONOPS) for automation systems based on user requirements, higher headquarters directives, and new capabilities resulting from improved technology.

2.2.1.3. Manage GATES access requests.

2.2.1.4. Substantiate data systems development and implementation schedules.

2.2.1.5. Develop and/or validate Baseline Change Requests (BCRs), Software Problem Reports (SPRs), and Document Problem Reports (DPRs) applicable to GATES. For instructions and templates, see **paragraph 4.3**. Gates Change Control Process within this instruction.

2.2.1.6. Maintain close liaison with the GATES Program Management Office (PMO).

2.2.1.7. Working through the GATES PMO; maintain close liaison with the GATES programming developers.

2.2.1.8. Maintain close liaison with GATES account holders and serve as their advocate to the GATES PMO and GATES developers.

2.2.1.9. Make all necessary arrangements to provide AMC GATES users for AMC GATES Customer Acceptance Testing (CAT) in the GATES Port Simulation Center (GPSC) and augment the GATES test bed.

2.2.1.10. Coordinate installation and removal of GATES/Remote GATES (RGATES)/Deployed GATES (DGATES).

2.2.1.11. Work Trouble Tickets (TT) assigned to the Functional Managers through C2 Remedy.

2.2.1.12. Maintain the HQ AMC/A4TI web pages and ensure the functional information on the web pages is current.

2.2.2. Research and integrate new technologies into AMC transportation systems.

2.2.3. Serve as the AMC functional point of contact for issues concerning non-AMC transportation systems.

2.2.4. Serve as the Chairman of the Transportation Functional Management Board (FMB).

2.2.5. Serve as a voting member on the GATES Configuration Control Board (CCB).

2.2.6. Ensure GATES requirements are included in air transportation submissions to joint strategic planning documents and the biennial planning, programming, and budgeting system.

2.2.7. Ensure the requirement for foreign national background investigations is included in all contracts for services provided at air terminals and commercial gateways in locations where foreign nationals provide the services and must have access to GATES.

2.2.8. Serve as POC for HQ AFRC and ANG Bureau functional on GATES issues/developing enterprise wide GATE solutions.

2.3. **Other HQ AMC/A4T Branches will:**

2.3.1. Notify A4TI of GATES related issues.

2.3.2. Submit and/or coordinate on BCRs, SPRs, and DPRs. For instructions and templates, see **paragraph 4.3.** Gates Change Control Process within this instruction.

2.3.3. Serve as a voting member on the Transportation FMB.

2.3.4. Work TTs assigned to them through C2 Remedy.

2.4. **HQ AMC/A4TR will:**

2.4.1. Coordinate development and implementation of GATES training programs and material with 423 MTS/MTLT.

2.4.2. Coordinate GATES training issues with A4TI and 423 MTS/MTLT.

2.5. **HQ AMC/A4TP will:**

2.5.1. Function as the approval authority for organizations requesting access to GATES for passenger bookings.

2.6. **HQ AMC/A4TC will:**

2.6.1. Serve as the authority for creating and maintaining worldwide Aerial Port Codes (APC) as needed for agencies throughout the command.

2.7. **The Chief, In-Transit Visibility and Business Systems Branch (HQ AMC/A6IB) will:**

2.7.1. Establish a GATES PMO and appoint a GATES Program Manager (PM).

2.7.2. Execute appropriate PMO responsibilities as articulated in DOD, Air Force, and AMC directives.

2.7.3. Secure funding for procurement, development, and initial/software directed implementation of hardware and software for AMC air terminals and aerial ports and non- AMC air terminals and aerial ports operated on AMC’s behalf.

2.7.4. Maintain the Sun server level (parent site) & Virtual Private Network Equipment.

2.7.5. Provide GATES equipment per the GATES Integrated Logistics Support Plan (ILSP).

2.7.6. Manage all aspects of security for GATES including Workstation Area Security Officer (WASO) management for the air side of GATES.

2.7.7. Serve as the Chairman of the GATES CCB.

2.7.8. Act as central point of contact for completion and finalizing Service Level Agreements (SLAs).

2.7.9. Secure funding for Certification and Accreditation (C&A) contractor services for GATES Central and Alternate sites as well as aerial ports.

2.7.10. Ensure appropriate documentation, technical library, and software/equipment user's manuals are current and changes are released to the field; obtain transportation policy and technical information from HQ AMC/A4T to support the sustainment of transportation systems.

2.8. **The Chief, Mission Systems Support Branch (HQ AMC/A6IS) will:**

2.8.1. Provide automated transportation systems sustainment and support services.

2.8.2. Maintain the GPSC, ensuring it is operational and stable a minimum of two weeks prior to any scheduled functional software testing.

2.9. **The Director of Global Readiness,(HQ AMC 618 AOC (TACC)/XOP) will:**

2.9.1. Task deployable units with appropriate automation systems, support elements, and trained personnel.

2.9.2. Submit and/or coordinate on BCRs, SPRs, and DPRs. For instructions and templates please see **paragraph 4.3.** Gates Change Control Process within this instruction.

2.9.3. Serve as a voting member on the Transportation FMB.

2.10. **The Director of Global Channel Operations, (HQ AMC 618 AOC (TACC)/XOG) will:**

2.10.1. Review system metrics and identify to HQ AMC/A4TI problem areas that impact efficient operation of transportation automation systems. **(T-2)**

2.10.2. Develop, submit, validate, and/or test system software BCRs, SPRs, and DPRs. For instructions and templates, please see **paragraph 4.3.** Gates Change Control Process within this instruction. **(T-2)**

2.10.3. Serve as a voting member on the Transportation FMB. **(T-2)**

2.10.4. Participate in developing future transportation automation system requirements. **(T-2)**

2.10.5. Provide routing IDs for approved passenger booking agencies. **(T-2)**

2.11. **375th Computer Support Squadron will:**

2.11.1. Coordinate with HQ AMC/A4TI in exercising technical operation direction over resources for the purposes of maintenance in support of transportation automation systems. **(T-2)**

2.11.2. Coordinate the release of system advisory notices, letters, messages, and software releases or updates with HQ AMC/A4TI. **(T-2)**

2.11.3. Identify operational trends and recommend improvements to the GATES PMO and HQ AMC/A4TI. **(T-2)**

2.11.4. Maintain a 24/7 customer support branch (help desk) for operational problems or system outages. **(T-2)**

2.11.5. Maintain working documents to track network and systems problems and make available to update GATES PMO and HQ AMC/A4TI. **(T-2)**

2.11.6. Serve as an Information Assurance Manager overseeing services provided under the Enterprise Security Support contract (providing technical services to support DoD and AF C&A activities for GATES). **(T-2)**

2.12. **Aerial port squadrons and air terminals operated on AMC's behalf will:**

2.12.1. Maintain fully qualified primary and alternate systems management personnel to oversee GATES-specific issues (C4/CSA duties not required), act as central points of contact for Automatic Identification Technology (AIT) upgrades, and serve as liaison between the unit and the HQ AMC GATES Functional Management Office, HQ AMC/A4TI. **(T-2)**

2.12.2. Develop and submit system software BCRs and DPRs. For instructions and templates, please see **paragraph 4.3.** Gates Change Control Process within this instruction. **(T-2)**

2.12.3. Participate in developing future transportation automation system requirements to include review, coordination, signatory, and adherence to established SLAs within 90 days. **(T-2)**

2.12.4. Configure and install GATES-related devices to support transportation automation in the air terminal. **(T-2)**

2.12.5. Ensure adherence to the requirements of all applicable AMCI 24-101 Volumes. **(T-2)**

2.12.6. Follow established GATES policies and operating instructions as identified in AMC instructions, the GATES Installation and Operations Documents (GIOD), GATES C&A documentation, policy memorandums, and other such guidance as promulgated by HQ AMC. **(T-2)**

2.12.7. Locally manage GATES equipment, to include maintaining accountability in accordance with applicable Air Force Instructions, according to the policy established by HQ AMC and ensure that the life cycle replacement hardware is installed in a timely manner. **(T-2)**

2.12.8. Track open TT to ensure all GATES related problems, to include AIT, are tracked, and fixed in a timely fashion. **(T-2)**

2.12.9. All WASOs or designated supervisory personnel maintain C2 remedy account and periodically check for open TT assigned to units. Request required application and instructions by emailing the 375 CSPTS/SCOC C2REMEDY-Team org box. **(T-2)**

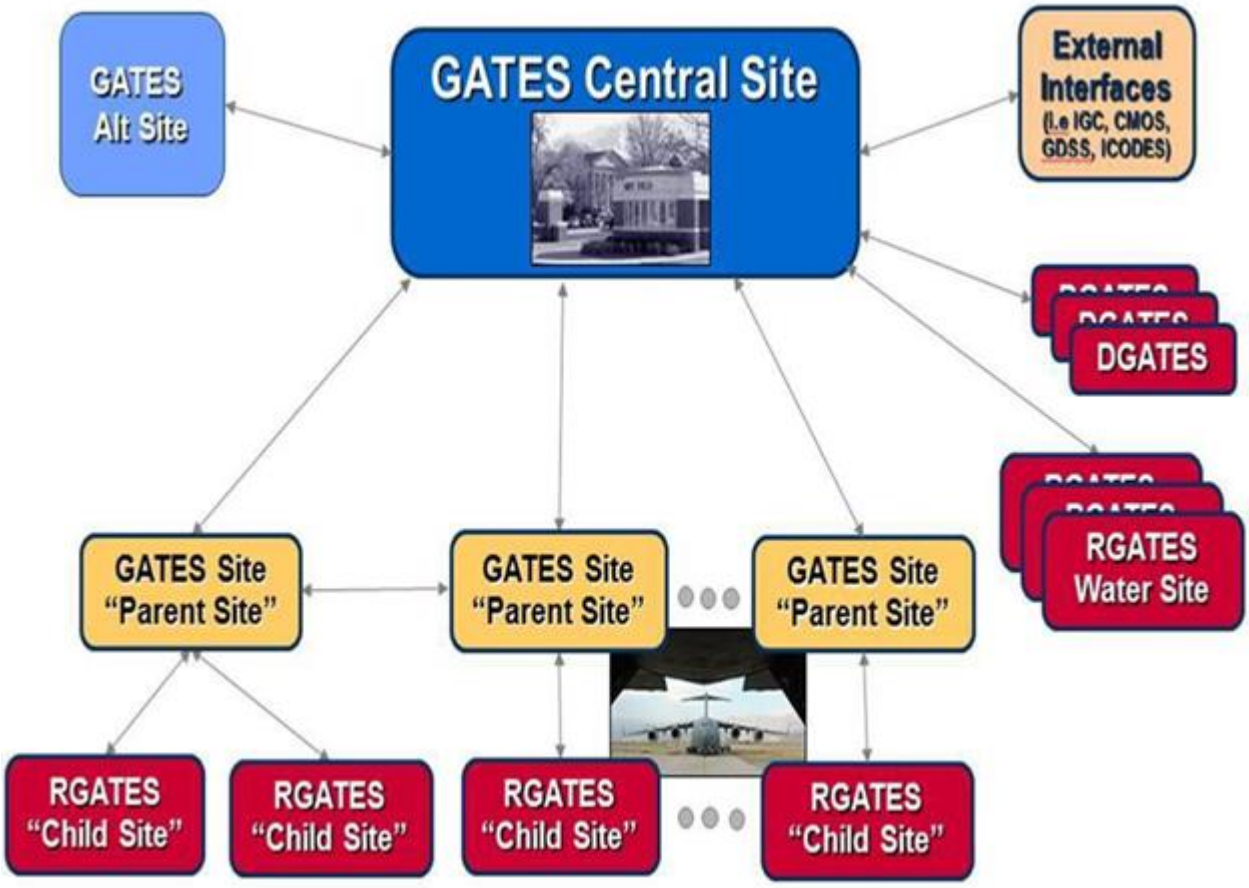
2.13. **GATES parent sites will:**

2.13.1. Assist as required with installation of RGATES servers at locations identified by HQ AMC/A4TI. **(T-2)**

3. Transportation Systems.

3.1. **GATES.** This is USTRANSCOM's automated air transportation management system. GATES access requires a valid need-to-know, background investigation (National Agency Check with Inquiries [NAC-I] or Host Nation Equivalent), and annual computer based information assurance training. This information is documented on a DD Form 2875, *System Authorized Access Request (SAAR)*. GATES issues a distinct user account when the above conditions are met. The individual's DOD issued Common Access Card (CAC) or token card, with digital certificates, are used for authentication into the GATES system. An important distinction to understand with the GATES architecture is that GATES is web-enabled and should not be considered web-based. While GATES is accessed via the Internet Explorer web browser, the connectivity to the GATES Central Servers at Scott AFB depends on the hierarchy architecture depicted in **Figure 1** Only a few GATES users connect directly to the Central Servers at Scott AFB: Transportation Offices making passenger reservations, certain Airlift Clearance Authorities (ACAs), those using cargo Track and Trace, users of the GATES Enterprise Management Service (GEMS) and those accessing GATES from Scott AFB, i.e. HQ AMC or TACC users with GATES accounts or "ad hoc" query and reporting tools using a variety of Commercial-Off-The-Shelf (COTS) business intelligence applications. GATES cannot simply be fielded at any site that desires GATES access. Installation of servers and associated equipment is required in order to process cargo and passengers. Due to the expense and complexity, expansion of GATES to new locations is carefully controlled. **Figure 1** provides an overview of the GATES connectivity architecture. Note: There are essentially seven different types of GATES configurations as follows:

Figure 1. GATES Connectivity Diagram.



3.1.1. **GATES/RGATES.** This configuration is found at the larger, fixed location aerial ports where a large amount of transportation data is generated. A GATES/RGATES server is located at the site with access to the server via PCs using the local LAN. At a GATES site, the server connects to the rest of the GATES world by connectivity back to the central servers at Scott AFB. At an RGATES site, the connectivity first goes through a parent GATES server and then back to the central servers at Scott AFB. See **Figure 1** for a diagram of the GATES/RGATES connectivity.

3.1.2. **DGATES.** This is a transportable installation of GATES used to rapidly provide ITV in a deployed environment. These installations are managed, as downward directed taskings by HQ AMC or the Director of Global Readiness, 618 AOC (TACC) /XOPM. A DGATES server is a ruggedized computer capable of working in austere environments. It connects directly back to the central servers at Scott AFB either via the site's LAN, or by satellite communications using INMARSAT/Broadband Global Area Network (BGAN). Often, a DGATES location does not generate large amounts of data, and if a LAN is not available the site can connect through the satellite to allow replication with the central servers. Charges are only accrued when data is transmitted, no longer does the BGAN charge for time connected. See **Figure 1** for a diagram of the DGATES connectivity. DGATES locations are intended to only be temporary until more stabilized operations are set in place and reliable ITV can be maintained.

3.1.3. **Track and Trace.** Track and Trace provides essentially the same tracking capability found in the GATES/RGATES configuration, but does not require installation of equipment. The user simply uses a PC with a 128-bit encryption capable browser and connects to the GATES Track and Trace web site **https://gatesea.gates.scott.af.mil**. Track and Trace is provided to personnel/organizations with a valid need to track cargo within the AMC airlift system but do not initiate manifesting or processing functions.

3.1.4. **Passenger Reservations.** Passenger Reservations, like Track and Trace, uses a web browser to connect to the GATES website **https://gatesea.gates.scott.af.mil**. The function is limited to organizations authorized to make passenger reservations on AMC organic/charter aircraft.

3.1.5. **Airlift Clearance Authority (ACA).** ACAs use a web browser to connect to the GATES website **https://gatesea.gates.scott.af.mil**. ACAs from the Air Force, Navy, Army, and Marine Corps use the ACA application to add, modify, and delete their particular service's advances within GATES.

3.1.6. **Other GATES Configurations and Equipment:**

3.1.6.1. **GATES Hand-held Operating Systems Tablet (GHOST).** GATES takes advantage of automatic identification technology, to include bar-coded military shipping labels (MSLs) and bar code scanning, by the use of the GHOST at aerial ports for various cargo and passenger processing operations. GATES uses AIT devices to improve cargo processing accuracy and efficiency by allowing air transportation specialists to perform real-time updates to the system from the same location they are working the cargo/pallets. The user can in-check, inventory, palletize, manifest surface or air, along with every action required to manage cargo (e.g., split, consolidate, frustrate) all from the device inside or outside the warehouse and other highly utilized areas. The GHOSTs utilize touch screen capability, linear and 2D bar code scanning, and real time web access via the Combat Information Transport System – Generation II (CITSGEN II) wireless capability, or Wireless Local Area Network (WLAN) interactive connectivity, to the GATES database. GHOSTs are also capable of non-interactive capability (batch mode) where CITSGEN II coverage is intermittent or not available. The software on the GHOST platform was written to mirror GATES common workstations.

3.1.6.2. **Radio Frequency Identification (RFID).** To increase transportation visibility for the Combatant Commanders (CCDRs), the DOD directed the use of active RFID tags on cargo moving to, within, and from the CCDRs area of responsibility (AOR) through the Defense Transportation System (DTS), to include port-built air transportation pallets. In response to this tasking, RFID tag write capability was added to GATES. GATES obtains any available content level detail data directly from the Defense Logistics Agency E-Business Server upon in-check of cargo at an aerial port. GATES then allows writing both Transportation Control and Movement Document (TCMD) data and content level detail data to the active RFID tag during pallet Close and Process (CAP) procedures. GATES then sends the combined data to the Radio Frequency (RF) ITV (RF-ITV) server. During surface movements, the RFID-tagged pallet passes choke-point interrogators that relay movement information to the RF-ITV server. The server matches the RFID tag ID

with the TCMD and requisition data for near-real time ITV and Total Asset Visibility (TAV) to anyone with an account for the RF-ITV server.

3.1.6.3. **GATES Enterprise Management Services (GEMS).** GEMS is a query tool that provides ports and other system users a capability to easily access both current and historical GATES data. Available as an assigned role to a regular GATES account, GEMS provides pre-formatted queries and allows for the development of additional queries based on new functional requirements. The information displayed by GEMS comes directly from either legacy databases, real time data from Central Site servers, or aerial port servers depending on what data is being requested.

3.1.6.4. **GATES Mobile Workstation (GMW).** GMWs are designed to provide mobile GATES functionality within the warehouse or ramp environment. The workstations are normally configured with a GATES capable CPU with Common Access Card (CAC) reader, keyboard, optical mouse, 19-inch monitor, military shipping label printer, pallet placard Laserjet printer, and an optional handheld imager.

3.1.6.4.1. To fully capitalize on the capabilities of the GMWs, as well as other advanced wireless capabilities, wireless connections are required. The expectation is for GATES to run on the base CITSGEN II wireless infrastructure instead of a dedicated GATES network. Units need to submit a Cyberspace Infrastructure Planning System/Work Order Management (CIPS/WOM) request with the local base communications organization requesting GATES hardware be part of the installation's wireless infrastructure. Inform HQ AMC/A4TI of any difficulty with obtaining wireless connections for GATES.

3.1.6.5. **Flight Information Display System (FIDS).** FIDS is used to provide passengers information about arriving flights, departing flights, and general information about the aerial port. All three of these components can be displayed on the same monitors in a revolving format or on separate monitors throughout the terminal and/or various base-wide locations. Refer to AMCI 24-101, Volume 14, paragraph 22 for further guidance concerning use of FIDS.

3.1.6.6. **Printers.** GATES uses a variety of printers to provide necessary output documentation. These printers include: military shipment label printers, (e.g., desktop and portable shoulder-carried), baggage tag and boarding pass printers, and standard laser printers for printing reports, manifests, placards, etc. The most common printers utilized throughout the GATES architecture are the PM4i and PD42 Intermec brand that are pre-formatted programmed specifically for GATES cargo and passenger processing functions.

3.1.6.7. **Remote Manifesting Resolution Center (RMRC) Server.** The RMRC server is a robust GATES server that allows AMC’s RMRC to view all aerial port manifest registers and input manifest data as required for any aerial port worldwide. Only RMRC personnel located within HQ AMC/A4TID at Scott AFB have access to this server. The server business rules allow manifesting data to stay active beyond the normal purge rules found on other GATES servers. This allows the RMRC to make corrections to manifest discrepancies when aerial port personnel are not able to ensure accurate data is passed on for billing actions. Additionally, this server is capable of

opening passenger flights up to eighteen hours after departure when other GATES servers are locked out at 1 hour. The RMRC server is robust enough to handle a multitude of cargo and passenger transactions.

3.1.6.7.1. **RMRC Utilization.** Should an aerial port be forced to utilize manual processing procedures, a GATES TT must be initiated. The TT must state GATES will be unavailable for 24 hours or longer and the aerial port is unable to keep pace with multiple active missions. During that time, the capability exists for the effected location to e-mail the data to the RMRC after obtaining approval from HQ AMC/A4TI, wherein the movement data can be entered into the GATES system as if from the originating APC. This provides for continuous ITV on cargo and passengers, allows processing by down line GATES stations without having to manually input the data themselves, and captures appropriate data for billing purposes. Official use of the RMRC for unit moves must be approved through the 618th AOC (TACC)/XOPM or HQ AMC/A4TI. Normal procedures call for the unit to request utilization of the RMRC through their MAJCOM to USTRANSCOM who will then contact the appropriate agency for approval/denial of RMRC involvement. AMC owned and operated terminals contact HQ AMC/A4TI. However, not all instances are approved automatically; if approved, the RMRC will contact the unit with standardized formats for the required documents they will be processing. The RMRC is a 24/7 agency that can be contacted at DSN (312)779-0045/COMM (618)229-0045 and/or **org.amca4-70@us.af.mil.**

3.2. **Additional Transportation Systems.** In addition to GATES, other automated information systems affect AMC transportation. The following systems are those that an AMC transporter is most likely to interact.

3.2.1. **Cargo Movement Operations System (CMOS).** CMOS automates and streamlines base-level cargo movement processes during peacetime and deployment passenger and cargo movements during contingencies operations. CMOS provides an integrated transportation capability in routine, deployment, and sustainment operations by employing the same DOD and Service shipment policies and procedures in peace and war. GATES provides CMOS with information about on-hand cargo that is ready for surface transportation. CMOS will provide GATES with information on the load planning and surface shipment of that cargo.

3.2.2. **The Transportation Coordinators' – Automated Information for Movements System II (TC-AIMS II).** An Army system, TC-AIMS II provides an integrated information transportation system capability for routine deployment, sustainment, and redeployment/retrograde operations. TC-AIMS II automates the processes of planning, organizing, coordinating, and controlling unit-related deployments and sustainment. It also automates the day-to-day redeployment, and retrograde operations for the Installation Transportation Officer/Transportation Management Officer in support of the DTS. TC-AIMS II provided cargo air, surface, and passenger manifest files to GATES where in turn GATES sends cargo air, surface, and passenger manifest files to TC-AIMS II for processing.

3.2.3. **Mechanized Materials Handling System (MMHS).** MMHS is a fully automated pallet storage system. It allows input commands from authorized computer terminals, attached control panels, scales, and laser scanners. The MMHS sorts and stores 463L pallets for efficient and safe retrieval. The MMHS system retrieves, rotates, and sequences pallets as directed, based on a given load plan. GATES will send a file containing one or more records with information about pallets, load plans, and/or missions to MMHS. MMHS reads that file and applies that information to its database. As pallets are stored in the MMHS, it creates files containing one or more records with information about each pallet.

3.2.4. **Integrated Computerized Deployment System (ICODES).** ICODES provides for a single, cross service, planning and execution system for aircraft, rail travel, and sea vessel load planning and stowage. It is engineered to provide users with intelligent decision/support during administrative, preposition, and humanitarian assistance operations. ICODES integrates multiple expert programs, knowledge bases, and graphical user interfaces within a computer-based distributed cooperative operational environment. GATES and ICODES utilize a two-way interface enabling a load planner to extract air eligible cargo from GATES for import into ICODES to safely and efficiently plan air movements. Once this is accomplished, ICODES then returns the cargo sequence numbers back to GATES so load planners can identify the order at which cargo will be loaded.

3.2.5. **Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence (IGC).** IGC provides DOD with an integrated set of networked, end-to-end visibility, deployment, and distribution capabilities. IGC collects and integrates transportation information from selected transportation systems. The resulting information is provided to the SECDEF, Combatant Commanders, USTRANSCOM, its component commands, and other DOD customers to support transportation planning and decision- making during peace and war. The end goal of IGC is to effectively support the Joint Force Commander's ability to make decisions based on actionable logistics information. GATES employs a one-way interface with only unclassified ITV data being output for IGC account holders to query and view.

3.2.6. **Deliberate and Crisis Action Planning and Execution Segments (DCAPES).** DCAPES supports USAF war planners and commanders in performing the tasks required to plan, source, mobilize, deploy, sustain, redeploy, and reconstitute forces for deliberate and crisis operations. DCAPES produces two files for GATES. The first file contains data for passengers to be booked on a flight. The second file contains Unit Line Number (ULN) information. These files are imported into GATES via a manual, air gap interface.

3.2.7. **Global Decision Support System (GDSS).** GDSS is an IGC interface system that provides aircraft scheduling and execution information. Additionally, it is an AMC migration system that records and displays airlift schedules, aircraft arrivals and departures, and limited aircraft status. It provides executive level decision support. GATES interfaces with GDSS to provide aircraft load data, where then GDSS delivers critical air mission information.

3.2.8. **Advanced Passenger Information System (APIS).** APIS facilitates the collection by Customs and Border Patrol (CBP) of certain information from private and commercial aircraft and vessels on all passengers and crewmembers that arrive in or depart from (and, in the case of aviation crew, fly over) the United States. CBP uses the information to identify those passengers and crew who may pose a higher risk to border, transportation or public security, may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants or warrants. GATES employs a one-way interface with APIS. Each time a passenger manifest is closed at any GATES location throughout the world, GATES immediately and automatically formats an Electronic Data Interchange for Administration, Commerce, and Trade (EDIFACT) file and sends an electronic message to the Department of Homeland Security's router, which uploads the file into APIS. This message includes all passengers manifested on a particular flight. That list of passengers is prescreened against the CBP "No Fly" list. Once vetting is complete, APIS returns an email confirmation with the status of each flight to an APIS NOTIFICATION email org box in addition to interaction with the DHS National Targeting Center (NTC) that is staffed 24/7 in preparation for possible immediate response to a "No Fly" alert.

3.2.9. **Finance Air Clearance Transportation System (FACTS).** FACTS is a Navy sponsored web-automated information system for the clearance of DoD air eligible cargo moving through the DTS and provides funds management and budgeting functions to facilitate the tracking and management of transportation funds. FACTS interfaces with GATES to provide advanced TCMD data for approval into the DTS and assists to forecast inbound cargo workload for aerial port personnel. GATES, in return, passes the movement status of the cargo back to FACTS so shippers may be informed on the status of their cargo.

3.2.10. **DEAMS Component Billing System (DCBS).** DCBS is utilized to apply business rules and rates to transportation data received from GATES and other transportation systems for the purpose of facilitating reimbursement to the Transportation Working Capital Fund (TWCF). Transportation data is then summarized and forwarded to the DEAMS accounting system where customers of the TWCF are invoiced for airlift services rendered.

3.2.11. **Defense Supply System (DSS).** DSS is the Defense Logistics Agency's (DLA) primary system to process and manage depot cargo destined for aerial ports of embarkation (APOEs). The primary focus of DSS is to provide pre-built cargo data to aerial ports prior to reception for the ability to forecast appropriate airlift in advance, hasten the processing time of building cargo at the aerial port, and provide an efficient process to streamline outbound cargo movement. DSS, like FACTS, provides advanced TCMD elements to help forecast airlift and streamline cargo processes ahead of time for aerial ports.

3.2.12. **Logistics Module (LOGMOD).** LOGMOD is an unclassified, responsive, online system providing Air Force warfighters with the ability to plan, execute, accelerate, or redirect to a higher priority location the deployment of Air Force units for accomplishing real-time combat operations anywhere in the world. LOGMOD is used by Air Force, Major Commands (MAJCOMs), and base-level logistics planners; and base-

level unit deployment managers (UDMs) to plan and execute deployment, reception, and redeployment of personnel, supplies, and equipment to meet various exercises, contingencies, and wartime tasking worldwide. LOGMOD will provide GATES with cargo data related to unit moves for deployments and exercises. The cargo data is provided as a text file that is then loaded by a GATES user accessing the LOGMOD tab of the Data Import Center.

4. GATES Procedures and Policies.

4.1. Commissioning RGATES/DGATES Servers.

4.1.1. **Procedures.** The following procedures have been developed to ensure all necessary actions are accomplished prior to an RGATES/DGATES site being commissioned. If these steps are not accomplished the server will not be deployed. Un-reconciled airlift manifests can possibly be dropped between GATES and DEAMS Component Billing Systems (DCBS) or manifest numbers may be overwritten by the deploying unit, mistakenly destroying historical data.

4.1.2. **Business Rules.**

4.1.2.1. The RGATES/DGATES deployment team must submit a TT to the GATES C2 Call Center NLT 5 days prior to departure to determine server availability and data management. The TT must request for a Remote Manifesting Resolution Center (RMRC) review of the GATESDP server or other RMRC owned servers prior to deployment (GATES Level II technical is not required to sign off on this TT). When the RMRC receives GATES TT for server review, they will determine if the RMRC or a Contingency Response Wing (CRW) owns the APC server being requested. **(T-2)**

4.1.2.2. If the requested APC is a RMRC owned server/APC. The RMRC team (DSN (312)779-0045/COMM (618)229-0045) and deployment team lead must contact each other to discuss ownership responsibilities and review server instructions. Responsibilities include:

4.1.2.2.1. The RMRC will determine if DGATES server is required based on In-transit Visibility (ITV), and RMRC work load for requested APC. DGATES servers are not normally deployed for JI only support tasking. Server is used for ITV, the RMRCs mission workload tasking for requested APC will generally be the determining factor for sever release, or non-release to the deployment team. **(T-2)**

4.1.2.2.2. Deployment teams are only responsible for working the missions specified as part of their tasking package. All other inbound or outbound missions outside the tasking package are the responsibly of the RMRC team and will be coordinated through local aerial port management. **(T-2)**

4.1.2.2.3. The deployment team must provide the RMRC team a working phone number from tasking location. It is imperative that the deployment team and RMRC have good communication to ensure manifest overwrite does not occur. **(T-2)**

4.1.2.2.4. Deployment team will coordinate with RMRC to get the latest manifest

passenger/cargo/surface register numbers and ensure these counters are adjusted on their deployed GATES server prior to team departure. **(T-2)**

4.1.2.2.5. The Deployment team will ensure all DGATES processes attributed to each mission tasking are cleared each day; complete all cargo and passengers manifests, in-check air and surface cargo, ensure missions are closed, clear cargo bay and grid reports, ensure all suspended passengers are processed, ensure manifest registers are clear of unprocessed manifests, work any TTs submitted to completion, as well as, create and file Consolidated Flight Packages (CFP) for each mission. **(T-2)**

4.1.2.3. Non-commissioned APCs: Non-commissioned APCs that are not currently assigned to any GATES/DGATES/RGATES server and are most likely available for immediate deployment. If this is the case, the deployment team lead is still required to submit a TT and must contact the RMRC team to determine DGATES instructions. RMRC team will review GATESDP server and provide cargo and passenger manifest numbers used, review/clear outstanding data and coordinate training on how to update the cargo or passenger running counters, as required. **(T-2)**

4.1.2.4. Deployment team lead will be responsible for TTs needed to replace and reset over written manifest data if the counters are not properly adjusted before deployment. CFPs will be created and filed with deployment team home aerial port. **(T-2)**

4.2. **Decommissioning RGATES/DGATES Servers.**

4.2.1. **Procedures.** The following procedures have been developed to ensure all necessary actions are accomplished when an RGATES/DGATES site is decommissioned. If these steps are not accomplished, the server will not be ready for any future deployment, and airlift manifests may remain in an un-reconciled status, thus preventing AMC from collecting airlift revenue. There are two distinct decommissioning phases that must occur. The first concerns completion of the business rules associated with decommissioning a site while the second involves the actual decommissioning of the RGATES/DGATES server and return of the server to a deployable configuration. The business rules need to be accomplished before the server itself is decommissioned.

4.2.2. **Business Rules.**

4.2.2.1. RGATES/DGATES sites must contact HQ AMC/A4TID Transportation Remote Manifesting Resolution Center (RMRC) DSN (312)779-0045/COMM (618)229-0045 or e-mail to **org.amca4-70@us.af.mil** NLT 5 days prior to decommissioning the servers/closing down locations, or as soon as possible in the case of a short notice site closure to ensure manifest registers for that location are reconciled. The following information must be provided: **(T-2)**

4.2.2.1.1. Name of the data records representative currently on station, representative's home station, representative's next station, and, if not classified, Incoming Contingency Response Group (CRG) representative or replacement unit. **(T-2)**

4.2.2.2. When a server is ready to be deactivated, on station personnel at RGATES/DGATES sites must submit a GATES TT for server deactivation request to the GATES Call Center. The TT will be forwarded to the RMRC team for DGATES server review. If the server review finds no server issues, the TT is forwarded to GATES Level II for server deactivation. If the server has unfinished data, the TT will be sent back to the deployment team for additional action. Only when the data is complete will the RMRC sign off the server review. **(T-2)**

4.2.2.3. Personnel at RGATES/DGATES sites must provide information on the last passenger/cargo manifest number/reference generated at the 5-day point and follow up with a tentative list no later than 24 hours prior to departure with the last manifest references to be created for final mission departures. This will let the RMRC know status prior to actual closure. **(T-2)**

4.2.2.4. Personnel at RGATES/DGATES sites must provide the number of over/short (O/S) shipments and the status of shipments (Tracer Action or Transportation Discrepancy Report (TDR) action in progress). **(T-2)**

4.2.2.5. Personnel at RGATES/DGATES sites must provide the RMRC with any outstanding TT numbers and situations causing TT action, if required. (NOTE: This provides the RMRC the ability and opportunity to compare what is left in the user system versus what can be seen in GATES Central Site.) **(T-2)**

4.2.2.6. Review all cargo/passenger reports and clear all manifests prior to decommissioning of the site/server. There should be minimal follow up actions for the RMRC to clear for departing units in the event processes cannot be completed due to TT action or assault departures. The RMRC retains the right to send data back to deployment teams for further quality checks and/or validation. Forward all pertinent documentation to the RMRC in these instances only. Otherwise, all documentation will be sent to the appropriate staging facility upon departure, or as soon as possible thereafter. **(T-2)**

4.2.2.7. Deployment Team Lead, WASO, or CRW will review RGATES/DGATES deployment user logins in “Security Services”, “Site User List Report”. Responsible lead will delete all user logins from their server prior to deactivation and turnover back to the RMRC. Not deleting user logins from the DGATES/RGATES server will leave delinquent user names on GATES-Central Site and will show on Delinquent User Account Report next time server is deployed. **(T-2)**

4.2.3. **Server Decommissioning.** The procedures for decommissioning a DGATES server are found in the GATES Installation and Operations Document (GIOD), Appendix V, Deployable GATES Installation, Registration, and Notification. The user should refer to the GIOD, which is available on the web at URL **https://cs3.eis.af.mil/sites/OO-LG-AM-73/default.aspx** to ensure the most current procedures are being followed. This action should only be performed if the DGATES location has completed the mission and the server needs to be cleaned and prepared for the next deployment. The server will not be decommissioned until all outstanding manifests are reconciled. **(T-2)**

4.2.3.1. If a server is no longer going to be used as a GATES server, sanitation of all data from all storage devices that contained GATES data must be accomplished IAW

AFMAN 33-282, *Computer Security (COMPUSEC).* GATES data contains sensitive government/DoD information as well as individual privacy act information and this data must be completely erased from GATES systems once a server is no longer used for GATES applications. **(T-2)**

4.3. **GATES Change Control Process.**

4.3.1. **Change Mechanisms.** Three mechanisms exist where GATES users can make changes to the system and the GATES documentation. The three mechanisms are the BCR, SPR, and the DPR processes.

4.3.1.1. **Baseline Change Requests (BCR).** BCRs are used to make enhancements to the system or to change the way the system operates due to new or changing requirements. GATES users formulate an idea on how to improve GATES functionality and complete the BCR form. The form and instructions for completing the form can be found through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html** and looking under the GATES Community of Practice (CoP) Homepage Links located in the left frame menu. When completed, the form is submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB. Since any change to the GATES software takes time and funding, and must compete with other validated requirements, a formal BCR process has been established to ensure critical changes are addressed first. This process is described below in **paragraph 4.3.2**

4.3.1.2. **Software Problem Reports (SPR).** SPRs are used to correct deficiencies in the GATES software when the system is in use but is not operating as it should. The form and instructions for completing the form can be found through the HQ AMC/A4TI website at **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html** and looking under the GATES CoP Homepage Links located in the left frame menu. It should be noted that most SPRs that result from a user reporting a problem to the help desk, and in the subsequent investigation of the TT, it is determined that a problem exists in the software code. Rarely, if ever, will a user submit an SPR directly. In most cases, the developer will document the required fix action on the SPR and submit it to configuration management.

4.3.1.3. **Document Problem Reports (DPR).** DPRs are used to correct errors in the GATES documentation, such as the GIODs or user manuals. If users find an error within the realm of GATES documentation, the DPR should be completed. The form and instructions for completing the form can be found through the HQ AMC/A4TI webpages at **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html** and looking under the GATES CoP Homepage Links located in the left frame menu. When completed, the form is submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB. The GATES Functional Managers will validate the DPR and submit to the GATES PMO for further processing.

4.3.2. **GATES Software Change Process.** The time from BCR submission until the change is fielded can take several months or years to accomplish depending on the level

of software development, coordination between the services, and depth of processes that must change accordingly. Other factors that weigh into this process are the complexity of the BCR, the priority the BCR is given, the point in the GATES release cycle that the BCR is submitted, as well as funding considerations. All these elements have an impact on the length of time it takes a change to reach the field. The following is a description of the steps in the BCR process which every request must go through.

4.3.2.1. **BCR submission.** The BCR process is initially written when a user completes a BCR form and submits it to the GATES Functional Managers within HQ AMC/A4TI for consideration. In the Project Impact section of the BCR, clearly state what will happen if the requirement is not implemented or how much time and money will be saved if the change is approved. In addition, mention if the BCR is being written due to the result of a Lean initiative or Terminal 21 (T21) event. The BCR should also contain a few words on the submitter's expectations of what the change should accomplish. This is where the user states exactly what he/she expects to see or have GATES do when the change is implemented. This helps the software developer understand the intent of the requested change. Without this information, the headquarters air transportation functional community may not adequately assess the BCR. The completed BCR can be mailed to HQ AMC/A4TI, 402 Scott Dr, Unit 2A2, Scott AFB, IL 62225-5308; e-mailed to **org.amca4-69@us.af.mil**, or as a last resort, fax to DSN (312)576-6476/COMM (618)256-6476. If at any time a user has a question concerning this process, HQ AMC/A4TI can be contacted at DSN (312)779-8174/COMM (618)229-8174.

4.3.2.2. **BCR processing.** The GATES Functional Manager(s) will review the submitted BCR, log it, and provide the other A4T branches a copy for their review and coordination. The branch which has responsibility for the BCR, e.g. A4TC will take ownership of cargo related BCRs, will ensure the BCR does not violate any established policies or business processes and perform a sanity check to ensure the BCR is a valid and necessary change. They will ensure the BCR is clearly written, and if necessary, contact the submitter for any required clarifications. Other branches will be provided a copy of the BCR to review and provide A4TI feedback as required. If the lead branch does not concur with the BCR, they will provide the GATES functional their rationale for non-concurring. From there, the GATES Functionals will notify all the branches, as well as the submitter, that the BCR will not be processed and provide the rationale. BCRs can be disapproved for a number of reasons, e.g., it is a duplicate of another BCR, the change is not necessary, the change is not possible, or the change violates established policy. If the lead branch concurs with the BCR, they will make any necessary modifications and return it to the GATES Functional to submit the BCR to configuration management where it is assigned an official number. The GATES Functional Managers will then provide all the branches, as well as the BCR submitter, a copy of the final BCR so they may track its progress through the development cycle if desired.

4.3.2.3. **BCR meets the GATES FMB.** As the GATES budget is limited, it is important to take all the BCR submissions and rank them in priority order so the most important changes can be addressed first. The GATES FMB reviews all functional requirement BCRs to prioritize those affecting the user/functional communities. First

the GATES Functional Managers analyze the BCRs prior to the FMB. An internal prioritization is accomplished and the prioritized list is then submitted to all branches within A4T. The formal FMB meets as required to discuss and finalize the priorities and this prioritized list is then submitted to the GATES CCB.

4.3.2.4. **BCR meets the GATES CCB.** The validated BCR is forwarded to the GATES CCB whose primary function is to manage all system BCRs. The CCB is made up of the PMO, System Manager (SM), the Functional Managers (FMs), Test Manager (TM), Configuration Manager (CM), and representatives such as Database Administrator (DBA), System Administrator (SA), Information/Protection/Security, Information Assurance Manager (IAM) Help Desk, and software engineers. The GATES CCB reviews and validates all new requirements and change requests to the existing GATES software and hardware baseline. The CCB works to prioritize developmental/ maintenance activity and change requests based upon system requirements and cost. In some cases, BCR implementation will be deferred because it is too late to incorporate the change into the next GATES software release or is deemed too costly to be accommodated by the GATES program budget at the present time. At the end of this process, the BCRs are allocated to a respective GATES release and given a tentative timeline for fielding. Since GATES also incorporates both surface and air requirements in addition to the Defense Courier Division, a Joint Functional Requirements Board (JFRB), chaired by the United States Transportation Command (USTRANSCOM), has been chartered to appeal and adjudicate competing functional requirements between the three functional areas within GATES.

4.3.2.5. **Develop Software/Create Release Documentation.** The GATES program manager, in coordination with the functional manager, develops the software to enable the requested change to GATES. This process usually involves several discussions between the developer and the GATES functional managers to clarify the requirement and ensure the change is effectively incorporated into the release. Documentation, such as software and user manuals, is also updated to reflect the change.

4.3.2.6. **Testing.** Once the software is developed, it is provided to the government for testing to ensure it functions securely and according to applicable DISA Security Technical Implementation Guides in addition to relative documented requirements. The software is independently tested during Formal Qualification Testing (FQT) via the Enterprise Security Support contract within the GPSC. When the software passes FQT testing, the GATES Functional Managers, supported by GATES users from the aerial ports, perform customer acceptance testing (CAT) to ensure the software functions as required. Errors are documented, sent back to the developer for corrections, and the software is tested again. Once all applications work according to the requirement, the software is accepted.

4.3.2.7. **Authorize Release for Fielding.** Following successful testing, the submitter's idea will be incorporated into a GATES release and fielded for all GATES users worldwide. In most cases, this will occur at the time of the next version release of the GATES software, which will also incorporate all other approved and newly developed BCRs.

4.4. **GATES Access Process.** The following procedures apply to air transportation access requests only. Customers requiring GATES for SDDC or DCD related missions must contact host functional communities for access. Access to Air GATES requires a legitimate need and requests must meet the criteria outlined in the following paragraphs. To request approval, the requester completes the appropriate GATES Access Request Letter Template which can be found on the A4TI web site at URL: **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html**. The following paragraphs provide specific details on obtaining access.

4.4.1. **Aerial Port GATES/RGATES.**

4.4.1.1. GATES installation at an aerial port is significantly more complicated since the GATES application is web-enabled, not web-based. This distinction requires modification to the GATES infrastructure as a GATES web server is installed at aerial port locations. The user's Internet Explorer on his or her computer connects to the local server and not directly to the central servers at Scott AFB. This architecture was chosen to allow the port personnel to continue to operate even if outside communications (internet capability from the aerial port server to Scott AFB) are cut off. Once communications are restored, the server automatically replicates data back to the central servers allowing the loss of communications to possibly go unnoticed depending on how long the lines were down. Modifications to the GATES infrastructure may require the purchase and installation of servers; therefore, these requests must be fully justified at the appropriate levels.

4.4.1.2. AFI 10-403, *Deployment Planning and Execution*, and AFI 24-114, *Small Air Terminal Operations*, requires the use of CMOS (or GATES if the specific location has GATES already) for deployment of Air Force forces except at AMC strategic aerial ports where GATES may be used instead. Strategic aerial ports are identified in Defense Transportation Regulation 4500.9-R, Part III, *Mobility*, Appendix M. CMOS is the Air Force standard system for deployment. One of the primary purposes of GATES is for Transportation Working Capital Fund (TWCF) reimbursement on channel traffic. The cost of operating GATES is recouped through TWCF, so installation of GATES at non-TWCF generating locations is approved solely on a case-by-case basis.

4.4.1.3. The request process for GATES/RGATES begins with the requester completing the appropriate GATES/RGATES Access Request Letter Template. Air Force organizations must coordinate with their Major Command's (MAJCOM) or higher headquarters' transportation division as well as HQ USAF/ILGD before submitting the letter to HQ AMC/A4TI. Without concurrence of both the MAJCOM and HQ USAF, the request will be denied. Non-Air Force organizations must work requests through their service major command and USTRANSCOM. GATES/RGATES will not be installed at non-Air Force locations without the approval of USTRANSCOM. If approved, the GATES Functional Managers will work with the GATES PMO and the affected sites to coordinate the installation of GATES/RGATES.

4.4.2. **Track and Trace.** Track and Trace request letters may be sent directly to HQ AMC/A4TI. Since IGC is the DOD approved system for ITV, requests for GATES Track

and Trace must include a statement as to why IGC will not meet the requester's needs. If approved, the requester is sent an e-mail notifying them of the approval with the WASO appointment letter template attached. The requester fills in the required information and has the letter signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, the appointed WASO sends the letter to the GATES Security Office at **208@us.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions. The new WASOs then create any additional Track and Trace accounts, to include replacement WASO accounts, required in their organization.

4.4.3. **Passenger Reservations.** Requests to gain access to GATES for Passenger Reservations must be sent to HQ AMC/A4TI for consideration. The Defense Transportation Regulation (DTR) Part I, *Passenger Movement*, states it is DOD policy that official travel providers/Transportation Officers (TOs) will make AMC channel airlift seat reservations directly in the AMC passenger seat reservation system, GATES. Access to GATES to make passenger reservations will not be approved for any organization not designated as a transportation office or official travel provider. All other organizations must work through their local/supporting transportation officer for passenger reservation support. The request letter must include the activity's routing indicator or contain a statement that a routing ID needs to be assigned. AMC in conjunction with 618th AOC (TACC) will assign a routing ID if the request is approved. AMC will staff the request within HQ AMC/A4T and, if approved, the requester is sent an e-mail notifying them of the approval with the WASO appointment letter template attached. The requester fills in the required information and has the letter signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, the appointed WASO sends the letter to the GATES SSO at **208@us.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions. The new WASOs then create any additional passenger reservations accounts, to include replacement WASO accounts, required in their organization.

4.4.4. **GATES Enterprise Management System (GEMS).** Access to GEMS is via a regular GATES account with an associated GEMS role. If the requester's organization already has GATES or GEMS users, the person requiring GEMS should contact the unit's GATES WASO to obtain a GATES account with the GEMS role. If the requester is not at a location with a request letter requesting GEMS directly to HQ AMC/A4TI. If approved, the requester is sent an e-mail notifying them of the approval with the WASO appointment letter template attached. The requester fills in the required information and has the letter signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc. This signature may be accomplished either by pen (preferred) or digitally with the CAC. A signed copy must be maintained at each site as a source document. Once signed, the appointed WASO sends the letter to the GATES SSO at **208@us.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the

WASO accounts and sends the new WASOs their login instructions. The new WASOs then create any additional GEMS accounts, to include replacement WASO accounts, required in their organization.

4.4.4.1. GEMS accounts must be placed into the appropriate GEMS group in order for the user to access the port data required and to allow sharing of reports with other members of the same GEMS group. At an aerial port, the GEMS user will normally be restricted to the data at his or her port. At other locations, e.g. Combatant Commands, MAJCOMs, Groups, Wings, etc., the GEMS user may be authorized access to more than one aerial port's data in order to retrieve data from all ports under their responsibility. When the WASO adds the GEMS role to a GATES user ID, the WASO can select the group the user ID belongs. A WASO can only add a user ID to a group they themselves belong. New GEMS locations require creation of a new group, which is accomplished in coordination with HQ AMC/A4TI during the initial request for GEMS access.

4.5. **Work Area Security Officer (WASO).** The WASO is responsible for managing GATES accounts at the site as well as ensuring GATES security issues are taken care of at his/her location. A GATES user with the "sybase_acct_mgr" role has full WASO privileges and is able to use most menu options of the GATES Security Services application. The "sybase_acct_asst" role only allows the WASO to lock, unlock, and reset user accounts. GATES will not allow "sybase_acct_mgr" and "sybase_acct_asst" to be assigned together. There is no limit to the number of WASOs allowed at a site, though, for effective account management, the "sybase_acct_mgr" role should be limited to a select few. As a rule, at least one WASO must be available to reset accounts at all times. It is very important that the WASOs keep their e-mail addresses current within the GATES system, as this is the primary method used by the GATES Functional Managers and GATES Security Office to contact them on GATES related issues. The e-mail address is easily updated using "Security Services" and the "modify account option". In depth familiarization training for WASO procedures can be accomplished via the "Security" link located on the GATES EIM A link to this site is found here **https://cs3.eis.af.mil/sites/OO-LG-AM-73/default.aspx**.

4.5.1. **WASO Appointment Process.**

4.5.1.1. **Initial WASO appointment.** WASOs must be appointed to the position. The GATES SSO creates the initial WASO accounts at a new location. Personnel at the new location must obtain the WASO Appointment Letter Template from the GATES EIM website. A link to the WASO Appointment Letter Template and processing instructions can be accessed at **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html**. Fill in the requested information and have it signed by the commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander. Signature may be accomplished either by pen and ink (preferred) or digitally with the CAC. A signed copy and DD Form 2875 must be maintained at each site as the source documents. Once signed, send the DD Form 2875(s) to the GATES SSO at **208@us.af.mil** attached to a digitally signed e-mail. The GATES SSO creates the WASO accounts and sends the new WASOs their login instructions. Any time WASOs are added or deleted, a new WASO appointment letter is required to be signed and saved to the local government file management system as a permanent

record. The DD Form 2875 is required to be updated anytime the user account is modified.

4.5.1.2. **Subsequent WASO appointments.** Once the GATES SSO has created the initial WASO accounts for a site, subsequent WASOs at the site are created and filed locally. The commander or equivalent, e.g. Division Chief, Operations Officer, Flight Commander, etc., must sign the WASO appointment letter before the WASO adds the WASO role (sybase_acct_mgr) to an existing account or creates a new user account with the WASO role. Additionally, the endorsed letter must match the system-generated letter. When existing WASOs no longer perform WASO duties, their WASO permissions/role must be removed. Only those users with the "sybase_acct_mgr" role are listed on the WASO appointment letter. Anytime WASOs are added or deleted, a new WASO appointment letter is required to be signed and saved to the local government file management system as a permanent record.

4.5.2. **User Account Management.**

4.5.2.1. The WASOs (user with "sybase_acct_mgr" role) and assistant WASOs (user with "sybase_acct_asst" role) are the only users allowed access to the GATES Security Services application. WASOs can only create, modify, delete, transfer, receive, and lock and unlock user accounts at their location, e.g. a WASO at Dover AFB cannot accomplish account management for a user at Ramstein AB. Assistant WASOs can only reset user accounts. When a user no longer requires a GATES account, the account must be deleted within 24 hours after the user no longer requires access. The WASO needs to be notified when personnel leave the unit so a deletion or transfer can take place. WASOs should be on the unit's out-processing checklist to ensure they are aware of personnel leaving the unit. GATES users ordered to a temporary duty location or to PCS who have a requirement to use GATES at the new location may have their accounts transferred to the new location. This process is fully automated within GATES for personnel with WASO roles and permissions. To transfer accounts between GATES sites, authorized WASOs activate this process in the "Security Services" Application. WASOs losing the user account must designate the gaining APC for the user's new GATES location. Once submitted, the WASO at the new location must log into GATES and initiate receiving the new account for their site. NOTE: Accounts assigned the WASO role are unable to be transferred. These accounts must be removed of the WASO capability before the transfer of the account may take place.

4.5.2.2. Login IDs are auto generated from the user's name and then given a number from 00 to 99, which ensures individual accountability. System audits and GATES transaction audits track each action accomplished in GATES. User accounts are not shared between teams or groups; users must only use their personal account to maintain accountability. To activate a new user account, the user must complete a DD Form 2875, *System Authorization Access Request (SAAR)*, with supervisor and security manager information filled out. This ensures the user is approved for GATES system access and use. Once complete, the DD Form 2875 is kept and stored within the WASO office as a record of access granted for users created under that WASO.

DD Forms 2875 must be accounted for in accordance with the disposition instructions located in Section E on the last page of that form.

4.5.2.3. To be eligible for a GATES account, an individual must have as a minimum, a favorable background investigation as well as documented Information Assurance (IA) training. Foreign nationals who require access to GATES in the performance of their duties are authorized a GATES account. They too require a favorable background investigation, i.e. National Agency Check with Inquiries (NACI) or host nation equivalent and documented information assurance training. See **paragraph 4.5.6.** for specific procedures on providing foreign national access to GATES. User roles determine user permissions to access GATES information. As a rule, WASOs should assign the minimum number of roles required for the individual to accomplish his/her job. Refer to the GATES GIOD, Appendix P for specific information concerning roles.

4.5.2.4. Every 30 days, the WASO will review account usage by printing a Delinquent User Account report from the GATES "security services" application. The WASO must contact delinquent users and determine if the user still requires GATES access. If access is no longer required, the WASO must delete the account. Any accounts showing 120 days of inactivity will be deleted automatically. If/when, the TDY indicator is checked and the account still shows no use after 1 year, the account is removed completely from the system. **(T-3)**

4.5.3. **Password Management.** Authentication to GATES for all users will be accomplished via the CAC. Those administrative users still requiring the use of a password for authentication will use special software that will allow them to reset their own passwords in the future.

4.5.4. **User Revalidation.**

4.5.4.1. GATES user accounts must be revalidated annually or more frequent intervals dictated by HQ AMC/A6IB, GATES PMO, to prevent unauthorized user access to the critical information within the system. This revalidation is a WASO responsibility and the GATES SSO will notify WASOs when the revalidation is due, normally in January. Sound security practices require user accounts to be deleted when a user no longer requires access to GATES. In many cases, the WASO is unaware of those individuals who no longer require access to GATES and the annual revalidation ensures that accounts no longer required are deleted. The WASO must contact each GATES user on the site user list report, determine if they still require GATES, verify the roles they have are the minimum required, and validate personal information, i.e. last name, first name and middle initial, rank, DSN phone #, e-mail address, type of security clearance, date of clearance, type of investigation, and citizenship. The WASO must meet each user face-to- face or if the user is geographically separated, the user must send the WASO a digitally signed e-mail containing the user's data to validate the user's identity. Accounts no longer required must be deleted. **(T-2)**

4.5.4.2. WASOs must also complete new foreign national (FN) access requests (FNAR) for any foreign nationals still requiring GATES following the procedures in **paragraph 4.5.6. (T-2)**

4.5.4.3. The WASO completes the user revalidation by selecting the User Revalidation application from the Security Services drop down window. The WASO should modify or delete accounts as required and accept those accounts that are required and up to date. The accepted accounts will then show as valid. **(T-2)**

4.5.4.4. Once all user accounts, WASO appointment letter and (if applicable) the foreign national users have been revalidated, the WASO must select the 'Send Revalidation Completion Message" from the activities drop down menu. This signals the GATES SSO to verify all actions have been completed satisfactorily. **(T-2)**

4.5.5. **RGATES and DGATES Server Patches.** Periodically, local base security auditors will scan a GATES server to determine if the server is up to date with the most recent network required security patches. If patches are missing, the site WASOs will be notified and provided a list of the patches required. It is extremely important to accomplish this as soon as possible and is a WASO responsibility to work with the local security/communications office to have the patches loaded onto the GATES server. **(T-2)**

4.5.6. **Foreign National Access Request (FNAR) to GATES.** Foreign Nationals (non-US citizens) have been authorized by the Air Mobility Command Vice-Commander to have access to GATES. The following procedures have been developed to ensure foreign nationals who access GATES have a valid need-to-know and have been approved by the local commander to access the system.

4.5.6.1. Before granting access to GATES for any foreign national, the requirements of AFI 33-200, *Air Force Cybersecurity Program Management*, AFI 31-501, *Personnel Security Program Management*, and AFMAN 33-282, *Computer Security (COMPUSEC)*, must be met. In summary, as a minimum, all foreign nationals must have a completed background investigation (NACI or host nation equivalent), completed the annual Protecting Sensitive Information training, and DOD mandated network cybersecurity awareness training. This training must never expire, or GATES access must be denied. In addition, foreign nationals will be assigned the minimum number of roles required to accomplish their mission. **(T-2)**

4.5.6.2. The FNAR process is initiated within GATES as a part of the Foreign National Approval window; however, Commanders at the GATES site (O-4 or higher) must still authorize in writing foreign national access to GATES using the GATES system generated FNAR from the Security Services Foreign National Approval application. Multiple foreign national users can be listed on the same document. This document requires signature (may be a digital signature) by the command authority (O-4 or higher) at the GATES site. When signed, the WASO must e-mail these access requests, using a digitally signed e-mail, to GATES Security at **208@scott.af.mil.** The document will require annual update and forwarding to GATES Security. WASO will be required to create the FN account, lock it, generate the FNAR, obtain the appropriate endorsement, and then send to GATES Security. These accounts remain locked until GATES Security has approved the request and notified the WASO via email. **(T-2)**

4.5.6.3. Foreign national access to GATES will be revalidated during the annual GATES User Revalidation. Commanders will re-accomplish and sign a new foreign national GATES access letter for each foreign national requiring access to GATES.

HQ AMC/A4T will periodically conduct a random audit of foreign national accounts to ensure compliance with these procedures. **(T-2)**

4.5.7. **Physical Security.** The primary purpose of physical security is to prevent unauthorized access to equipment, facilities, material, and information. Physical security includes physical barriers and control procedures. Physical security for GATES is provided by the entry control procedures of the facility where the equipment is housed and the application of standard resource protection measures. GATES equipment does not require any special physical security considerations beyond those specified in AFMAN 33-282, *Computer Security (COMPUSEC)*, for workstation security in the computing environment.

4.5.7.1. **DGATES Servers.** To ensure the safety and security of DGATES servers, these servers must always be hand carried and included into carry-on baggage while traveling. DGATES servers cannot be checked as checked baggage or shipped as freight. **(T-2)**

4.5.8. **Additional Information.** Detailed, information related to WASO responsibilities can be located on line through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html**

4.6. **GATES Training.** Air Force Air Transportation personnel receive initial GATES training at their technical training school at Ft. Lee, VA upon entering the career field. This training is an introduction to GATES only. In-depth training on GATES is provided at the aerial port via on-the-job training. As more than just Air Force Air Transportation specialists use GATES, additional training material has been developed to assist other users in becoming proficient in the use of GATES. A brief description of training material available is provided in the following paragraphs. All GATES training concerns should be addressed to HQ AMC/A4TR at DSN (312)779-4592/COMM (618)229-4592.

4.6.1. **GATES Training Videos.** AMC A6IS has developed GATES training videos to help airman become familiar with GATES functions and to accelerate their training. The videos are found under the "GATES Air" headline, and they include: Cape Forecasting, Cargo Inbound, Cargo Manifesting, Form 214 Inventory, GATES Mission, Load Planning, Pallet Processing and RFID Tag Burn, Passenger Check In and Gate Control, Passenger Reservations, Passenger Reservations for TMO, Passenger Service Center, and Shipment Unit Maintenance. These videos are available at **https://cs3.eis.af.mil/sites/24920/GATES/SitePages/Training%20Videos.aspx**. You must request access to the site and be approved before having access to the videos.

4.6.2. **Pamphlets.** Several training pamphlets are also available to provide familiarization on GATES operation and can be located on line through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html**.

4.6.3. **Continuous Learning Environment (CLE).** The CLE provides a GATES environment that is dedicated to training aerial porters to use GATES. The CLE provides

both formal classroom training and informal training capabilities. Users of the training system have the ability to simulate a selected APC during the Login process, or create a new one. The system runs the current version of GATES and will update when new versions are released.

4.6.4. **DOD CyberSecurity Awareness (IA) Training.** In accordance with Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01 all DOD military, civilian, and contractors will receive documented IA training prior to receiving access to the network. Training required to obtain a network user license is standardized in the Information Assurance Awareness Training" WBT course. Access the WBT on the current IA training site via the Air Force Portal. Successful completion of this course satisfies the Air Force training requirement for a network user license. Annual system security training is required IAW AFI 33-115, *Air Force Information Technology (IT) Service Management*. **(T-2)**

4.6.5. **Advanced Distributed Learning System (ADLS).** Due to the increased numbers of GATES users worldwide, several (WBT) modules were developed and placed on the AMC ADLS training website for easy access and to help keep GATES users trained appropriately. To access these WBTs, log onto the Air Force Portal and locate the ADLS quick-link. Once inside, locate the ADLS Gateway for access to the AMC course list where you will find various helpful GATES WBTs. Use keyword "GATES" for your search and the links to the WBTs will appear. The WBTs are an open enrollment opportunity where all users with access to the ADLS training website have access to the training modules.

4.7. **GATES Documentation.** Additional, detailed information related to GATES can be located on line through the HQ AMC/A4TI web pages at URL **https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1353610FB5E044080020E329A9/Files/a4t/a4ti/gates/hello.html**. The GATES User Manuals GUMs), GIODs, WASO instructions, and other GATES related documentation can be accessed through this link. These documents are important as they provide instruction on how your computer and/or internet browser need to be configured to work with GATES and provide guidance on how to use the system.

4.8. **GATES Help Desk.** If a user experiences any problems with GATES, their first action should be to call the C2 Call Center at DSN (312)576-4949/COMM (618)256-4949, Option 1 to reach the GATES Help Desk, or e-mail to **amctranshelpdesk@us.af.mil.** The user can set the priority of the problem as either low, medium, high or critical. If the issue is causing a work stoppage, the user should inform the help desk. The GATES Help Desk will open a TT with the customer and pass the problem off to the appropriate agency for corrective action. Once corrected, the help desk will contact the submitter to determine if the issue was satisfactorily resolved prior to closing the ticket.

STACEY T. HAWKINS, Brigadier General, USAF
Director of Logistics, Engineering,
& Force Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DTR 4500.9-R, *Defense Transportation Regulation, Part I, Passenger Movement*, November 2010

DTR 4500.9-R, *Defense Transportation Regulation, Part II, Cargo Movement*, May 2014

DTR 4500.9-R, *Defense Transportation Regulation, Part III, Mobility*, July 2011

DTR 4500.9-R, *Defense Transportation Regulation, Part IV, Personal Property*, December 2015

DTR 4500.9-R, *Defense Transportation Regulation, Part V, Department of Defense Customs and Borders Clearance Policies and Procedures*, March 2011

DTR 4500.9-R, *Defense Transportation Regulation, Part VI, Management and Control of Intermodal Containers and System 463-L Equipment*, March 2015

DTR 4500.9-R, *Defense Transportation Regulation, Part VII, Human Remains Movement*, July 2013

DOD 4515.13-R, *Air Transportation Eligibility*, 1 November 1994

CJCSM 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

AFI 33-115, *Air Force Information Technology (IT) Service Management*, 16 September 2014

AFI 33-324, *The Information Collections and Reports Management Program*, March 2013, Incorporating Change 1, 18 December 2014

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 12 January 2015

AFI 33-364, *Records Disposition-Procedures and Responsibilities*, 22 December 2006

AFI 10-403, *Deployment Planning and Execution*, 20 September 2012

AFI 24-114, *Air Transportation Operations (Non-Aerial Port)*, 04 September 2014

AFI 33-200, *Cybersecurity Program Management*, 31 August 2015

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMAN 33-282, *Computer Security (COMPUSEC)*, 24 April 2013

AFPD 33-3, *Information Management*, 08 September 2011

AFPD 24-1, *Personnel Movement*, 9 August 2012

AFPD24-2, *Preparation and Movement of Air Force Materiel*, 27 April 2011

AMCI 24-101 Vol 6, *Transportation Documentation, Data Records and Reports*, 21 March 2016

AMCI 24-101 Vol 9, *Air Terminal Operations Center*, 20 February 2013

AMCI 24-101, Vol 10, *Military Airlift Fleet Service*, 30 August 2012

AMCI 24-101 Vol 11, *Cargo and Mail Policy*, 27 February 2013

AMCI 24-101 Vol 14, *Military Airlift Passenger Service*, 23 September 2015

AMCI 24-101, Vol 22, *Training Requirements for Aerial Port Operations*, 31 December 2012

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 2875, *System Authorization Access Request (SAAR)*

Abbreviations and Acronyms

2D—Two Dimensional

AB—Air Base

ACA—Airlift Clearance Authority

ADLS—Advanced Distributed Learning System

AFB—Air Force Base

AFMAN—Air Force Manual

AFRC—Air Force Reserve Command

AISS—Applications Infrastructural Systems Support

AIT—Automatic Identification Technology

AMC—Air Mobility Command

AMCI—Air Mobility Command Instruction

ANG—Air National Guard

AOR—Area of Responsibility

APC—Aerial Port Code

APIS—Advanced Passenger Information System

APOE—Aerial Port of Embarkation

APOD—Aerial Port of Debarkation

BCR—Baseline Change Request

BGAN—Broadband Global Area Network

C&A—Certification & Accreditation

C2—Command and Control

CA—Central Analysis

CAC—Common Access Card

CAP—Close and Process

CAT—Customer Acceptance Testing

CCB—Configuration Control Board

CIO—Chief Information Officer

CIPS/WOM—Cyberspace Infrastructure Planning System/Work Order Management

CLE –— Continuous Learning Environment

CMOS—Cargo Movement Operations System

CCDR—Combatant Commander

CONOPS—Concept of Operations

COTS—Commercial Off-The Shelf

CPRP—Chief Information Officer (CIO) Program Review Process

CRAF—Civil Reserve Air Fleet

CRG—Contingency Response Group

CRW—Contingency Response Wing

CTUS—Continental Territory of the United States

DCAPES—Deliberate and Crisis Action Planning and Execution Segments

DCBS—Defense Consolidated Billing System

DCD—Defense Courier Division

DEAMS—Defense Enterprise Accounting and Management System

DGATES—Deployable GATES

DHS—Department of Homeland Security

DLA—Defense Logistics Agency

DOC—Designed Operational Capability

DOD—Department of Defense

DPR—Document Problem Report

DSS—Distribution Standard System

DTR—Defense Transportation Regulation

DTS—Defense Transportation System

FACTS—Finance Air Clearance Transportation System

FIDS—Flight Information Display System

FM—Functional Manager

FMB—Functional Management Board

FQT—Formal Qualification Testing

GATES—Global Air Transportation Execution System

GDSS—Global Decision Support System

GEMS—GATES Enterprise Management Services

GHOST—GATES Handheld Operations System Tablet

GIOD—GATES Installation and Operations Document

GMW—GATES Mobile Workstation

GTN—Global Transportation Network

GUM—GATES User Manual

HDB—History Data Base

HHI—Hand Held Interrogator

HHT—Hand Held Terminal

HQ—Headquarters

ICODES—Integrated Computerized Deployment System

ID—Identification

IDD—Interface Design Document

IGC—Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence

ILSP—Integrated Logistics Support Plan

IT/NSS—Information Technology/National Security System

ITV—In Transit Visibility

JFRB—Joint Functional Requirements Board

LAN—Local Area Network

MAJCOM—Major Command

MISCAP—Mission Capability

MMHS—Mechanized Material Handling System

MODEM—Modulator Demodulator

MSL—Military Shipping Label

NACI—National Agency Check with Inquiries

NTC—National Targeting Center

O/S—Over/Short

OPlans—Operational Plans

OPR—Office of Primary Responsibility

OR—Operationally Reportable

PC—Personal Computer

PDO—Publishing Distribution Office

PM—Program Manager

PMO—Program Management Office

RF—Radio Frequency

RMRC—Remote Manifesting Resolution Center

RFID—Radio Frequency Identification

RF-ITV—Radio Frequency-In-transit Visibility

RGATES—Remote GATES

SAAR—System Authorized Access Request

SDDC—Surface Deployment and Distribution Command

SIPRNet—Secret Internet Protocol Router Network

SM—System Manager

Space A/R—Space Available/Required

SPR—Software Problem Report

SSO—System Security Office

SUM—Software User's Manual

TACC—Tanker Airlift Control Center

TAV—Total Asset Visibility

TC-AIMS II—Transportation Coordinators–Automated Information for Movements System II

TCMD—Transportation Control and Movement Document

TCN—Transportation Control Number

TDR—Transportation Discrepancy Report

TM—Test Manager

TO—Transportation Officer

TWCF—Transportation Working Capital Fund

URL—Uniform Resource Locator

USB—Universal Serial Bus

USTRANSCOM—United States Transportation Command

UTC—Unit Type Code

WASO—Workstation Area Security Officer

WLAN—Wireless Local Area Network

WPS—Worldwide Port System

Terms

Aerial Port—An airfield that has been designated for the sustained air movement of personnel and materiel as well as an authorized port of entrance into or departure from the country where located.

Automatic Identification Technology (AIT)—The group of technologies consisting of bar codes, radio frequency identification tags, Common Access Cards, and biometrics, which, then interfaced to information systems, provide automatic identification.

Baseline Change Request (BCR)—BCRs are used to make enhancements to the system or to change the way the system operates due to new or changing requirements. The BCR form is filled out and submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB, IL. Since any change to the GATES software takes time and funding, and must compete with other validated requirements, a formal BCR process has been established to ensure critical changes are addressed first.

Broadband Global Area Network (BGAN)—BGAN is the INMARSAT broadband digital service and is used by DGATES computers for their connectivity requirements. Downlink speeds of high-end BGAN terminals are up to 492kb/s and upload speeds slightly lower at 300-400kb/s.

C2 Remedy—C2 Remedy is the tool used to track GATES TTs and corrective actions. It provides the capability of managing, tracking, or monitoring problem ticket information, including creating problem resolution requests, searching for existing problem ticket data, generating reports, and creating macros. When a user experiences a problem with GATES and calls the GATES help desk, an entry is made in C2 Remedy and a TT is assigned.

Configuration Control Board (CCB)—The CCB is the mechanism used to prioritize competing GATES requirements to ensure the most critical can be satisfied in the resource constrained software development environment. Members of the CCB are the GATES functional managers, GATES Security Office, the GATES system managers, and the GATES program management office. The CCB reviews requirements against known resources and develops a prioritized list of requirements that can be met in the next GATES release cycle.

Continuous Learning Environment (CLE)—- The CLE provides a GATES environment that is dedicated to training aerial porters to use GATES. The CLE provides both formal classroom training and informal training capabilities. Users of the training system have the ability to simulate a selected APC during the Login process, or create a new one. The system runs the current version of GATES and will update when new versions are released.

Document Problem Report (DPR)—DPRs are used to correct errors in the GATES documentation, such as the GIOD or user manuals. If users find an error in the GATES documentation, the DPR should be completed and submitted to the GATES Functional Managers at HQ AMC/A4TI at Scott AFB, IL. The GATES Functional Managers will validate the DPR and submit to the GATES PMO for processing.

Functional Management Board (FMB)—The FMB is the mechanism used to prioritize GATES functional requirements. Unsatisfied requirements from the functional community are reviewed and prioritized before meeting the CCB. This way, the most critical functional requirements are clearly identified and won't be overlooked during the CCB negotiations. The

FMB is chaired by AMC/A4TI and consists of members from every A4T branch, the TACC, and FM.

INMARSAT—INMARSAT is the corporation that owns the INMARSAT satellite-based communication system. The satellite constellation was previously known as International Maritime Satellite (INMARSAT), developed by an intergovernmental organization consortium in 1979 to provide global safety and other communications for the maritime community. In 1999 it was transformed into a private company, INMARSAT, and INMARSAT no longer is a term used to identify the satellites.

Integrated Logistics Support Plan (ILSP)—ILSP provides general policies, procedures and practices for the development, implementation, and continued operation of program hardware, software and communication assets.

Joint Functional Requirements Board (JFRB)—GATES has become more than an aerial port management tool and now incorporates aerial port, water port, and Defense Courier Service (DCD) functional requirements. Each functional community independently submits their requirements to the GATES PMO, which at times, will result in conflicting requirements or too many requirements to implement with the resources available. The JFRB was created to deconflict and prioritize these competing functional requirements. The JFRB is convened as required and is chaired by USTRANSCOM/J3 who has tie breaking authority and also represents the DCD functional community. The Surface Deployment and Distribution Command (SDDC), representing the water port functional community and AMC, representing the aerial port functional community are voting members.

Program Management Office (PMO)—The PMO manages system development and acquisition of system hardware. The PMO is responsible for budgeting and scheduling GATES development to meet the functional requirements as stated in BCRs and the Software Requirements Specifications.

Software Problem Report (SPR)—SPRs are used to correct deficiencies in the GATES software when the system is not operating as it should. Most SPRs result from a user reporting a problem to the GATES help desk, and in the subsequent investigation of the TT, it is determined that a problem exists in the software. Rarely, if ever, will a user submit an SPR directly. In most cases, the developer will document the required fix action on the SPR and submit it to configuration management. The SPR will then be allocated to a GATES release, the software fixed, and then implemented when the next GATES software is released worldwide.