



CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

Directive Current as of 18 November 2014

J-3
DISTRIBUTION: A, B, C, S

CJCSM 3122.05
15 December 2011

OPERATING PROCEDURES FOR JOINT OPERATION PLANNING AND EXECUTION SYSTEM (JOPES) - INFORMATION SYSTEMS (IS) GOVERNANCE

References: See Enclosure J

1. Purpose. The purpose of this document is to provide rules and procedures for JOPES Information Systems (IS) operating in the Global Command and Control System-Joint Version 4.X (GCCS-J v 4.X) environment in support of joint military operations, exercises, deployments, and rotations.
2. Cancellation. None.
3. Applicability. This manual applies to all agencies that develop or use planning information to support the Chairman of the Joint Chiefs of Staff, Joint Staff, unified (supported and supporting) commands, Services, and identified combat support agencies such as the Defense Logistics Agency (DLA) and the National Geospatial Intelligence Agency (NGA).
4. Procedures
 - a. Joint Staff directorate proposals to the Chairman which change source documentation information reflected in this publication will include, as an enclosure to their proposal, all proposed changes that would need to be made to this publication. All other users of this manual will notify the Director, J-3, Joint Staff, when changes to source documents reflected in this publication are initiated.
 - b. Recommendations for changes should be submitted to the Director for Operations (J-3/DDC2NO/CSOD), Joint Staff, Washington, D.C., 20318-3000.
5. Summary. None.

6. Releasability. This manual is approved for public release; distribution is unlimited. DOD components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this manual through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

7. Effective Date. This manual is effective immediately.



WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosures:

- A – Capabilities of JOPES IT
- B – JOPES IT Architecture
- C – User Account Management
- D – Database Access and Replication
- E – TPFDD Management
- F – Strategic Server Operations and Management
- G – Trouble Ticket Management
- H – JOPES Applications
- I – JOPES Performance Parameters
- J – Reference
- GL – Glossary

CJCSM 3122.05
15 December 2011

DISTRIBUTION

Distribution A, B, and C plus the following:

	<u>Copies</u>
Secretary of Defense.....	2
Commandant, US Coast Guard	2
Director, Central Intelligence Agency.....	2
Director, Federal Emergency Management Agency.....	2
Commanding General, Marine Corps Combat Development Command	2
President, National Defense University	2
Commandant, Joint Forces Staff College	2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	Page
ENCLOSURE A – CAPABILITIES OF JOPEs INFORMATION TECHNOLOGY (IT)	
Purpose	A-1
Background	A-1
Initial Requirements	A-2
General JOPEs Criteria	A-2
ENCLOSURE B – JOPEs IT ARCHITECTURE	
General B-1	
Fixed Strategic Server Enclave	B-2
Deployable Strategic Server Enclave	B-4
Master Management Server	B-5
Clients B-5	
External System Interfaces	B-5
Appendix A – External System Interfaces	B-A-1
ENCLOSURE C – USER ACCOUNT MANAGEMENT	
Purpose	C-1
Software Description	C-1
Types of JOPEs IT Accounts	C-1
JPERMS Operators	C-2
Roles and Responsibilities	C-3
Account Details	C-5
User Identification (ID) Construction	C-10
Password Management	C-12
Inactive User Accounts	C-14
JOPEs Permission Set	C-14
Access to JOPEs Data	C-16
Group/Joint Crisis Action Team (JCAT) Accounts	C-16
Access Authorization	C-16
ENCLOSURE D – DATABASE ACCESS AND REPLICATION	
Purpose	D-1
Responsibilities	D-1
Multi-Site and Single-Site Update	D-2
External Interface Replication	D-2
Request for Connection to a JOPEs Enclave	D-3

TABLE OF CONTENTS (con't)

	PAGE	
User Load-Balancing	D-3	
Series Enclave Assignment	D-4	
Command Enclave Assignment.....	D-4	
Daily Database Maintenance	D-5	
 ENCLOSURE E – TPFDD MANAGEMENT		
General E-1		
Upload and Deletion Notification	E-1	
Precedence and Prioritization.....	E-1	
TPFDD Backup and Restore	E-2	
 ENCLOSURE F – STRATEGIC SERVER OPERATIONS AND MANAGEMENT		
Introduction	F-1	
Background.....	F-1	
Continuity of Operations	F-1	
Management Hierarchy	F-2	
Roles and Responsibilities	F-2	
JSSC Management Process	F-4	
Security Certification and Accreditation.....	F-12	
Life Cycle Funding.....	F-12	
Outage Management.....	F-12	
Proactive and Administrative Management	F-14	
 Appendix A – Deployable Strategic Server Operations		F-A-1
 ENCLOSURE G – TROUBLE TICKET MANAGEMENT		
Submission	G-1	
Prioritization	G-1	
JSSC Service Desk Support	G-2	
Escalation	G-2	
Closure G-3		
 ENCLOSURE H – JOPES APPLICATIONS		
Purpose	H-1	
Application-Server Based Applications.....	H-1	
Web-Server Based Applications	H-1	
Database-Server Based Applications.....	H-2	

TABLE OF CONTENTS (con't)

	PAGE
ENCLOSURE I – JOPEs PERFORMANCE PARAMETERS I-1	
Appendix A – Critical Technical Parameters	I-A-1
Appendix B – Key Performance Parameters	I-B-1
Appendix C – Performance Attributes.....	I-C-1
ENCLOSURE J – REFERENCES	J-1
GLOSSARY	
Abbreviations and Acronyms	GL-1
Terms and Definitions	GL-5
FIGURES	
1 Strategic Server Enclave Notional Architecture	B-1
2 Fixed Strategic Server Site Enclave Architecture	B-2
3 Strategic Server Application Access	B-3
4 External System Interfaces	B-A-1
5 JPERMS Database Account Types	C-2
6 Notional JSSC Management Process	F-6
7 Strategic Server Enclave Management Process	F-15
8 Trouble Ticket Process.....	G-3
TABLES	
1 JPERMS Roles.....	C-7
2 Command/Service Designator	C-10
3 Series Permissions	C-14
4 TPFDD Permissions	C-16
5 Series Primary and Alternate Server Assignment.....	D-4
6 Command Primary and Alternate Enclave Assignment.....	D-5
7 GCCS-J JOPEs Critical Technical Parameters	I-A-1
8 GCCS-J JOPEs Key Performance Parameters	I-B-1
9 GCCS-J JOPEs Performance Attributes.....	I-C-1

(INTENTIONALLY BLANK)

ENCLOSURE A

CAPABILITIES OF JOPES IT

1. Purpose. Enclosure A outlines the basic capabilities of the JOPES Strategic Server Enclave environment (JOPES v4.X). Hereafter this environment will be referred to as JOPES IT.

2. Background

a. JOPES IT is an integrated joint command and control system used to support military operation monitoring, planning, and execution activities. Prior to the strategic server enclave environment, JOPES Classic consisted of 16 independently managed server suites utilizing client/server based applications. Each independent server suite had a distinct set of planning data and users resident. Over time, the underlying database and operating system software became outdated and unsupported. In addition, major concerns existed over synchronization of TPFDD data and lack of increased performance and functionality.

b. The current JOPES IT is a solution developed by the Defense Information Systems Agency (DISA), whose goal was to solve the data synchronization issues inherent in the JOPES Classic architecture and modernize the database architecture for JOPES. The Block IV JOPES v4.0 release provided a more robust infrastructure and a greatly enhanced method of synchronization for the Joint Planning and Execution Community (JPEC). It provided a technical solution to long standing JOPES database problems, and introduced Web-based applications to JOPES. The Block V (v4.1, 4.2, and v4.2.1) releases provide continued functionality improvements and greater migration to Web-based applications and a Service Oriented Architecture (SOA). Joint Staff/J-3 approved this initiative with the understanding that JOPES v4.X will meet the JOPES performance parameters as cited in Enclosure I and will achieve improvements in the following areas:

- (1) Application Integration
- (2) Data Access and Synchronization
- (3) Data Replication
- (4) JOPES Core Database
- (5) Service Oriented Architecture Design

(6) User Load Capability

(7) Web Technology

3. Initial Requirements. The minimum requirements and capabilities specified by the JPEC for the initial version of JOPES v4.X include the items listed below.

a. Maximize user ability to accomplish their deployment planning and execution mission, in support of the war planners and operators.

b. Provide full application functionality in limited bandwidth communications environments.

c. Achieve and maintain JOPES database synchronization throughout the entire process of transition, day-to-day operations, crisis operations, sustainment, and redeployment.

d. Be operational at fielding sites before commencement of the Initial Operational Capability (IOC). "Operational" was defined as users at all levels supported by GCCS JOPES had proven reliable access to JOPES IT and that all required feeder interfaces were working.

e. Have applications providing all required functionality to create, edit, and validate a Time Phased Force and Deployment Data (TPFDD) for transportation scheduling in a time-sensitive, crisis action environment, and to accomplish war planning TPFDD development, analysis, and execution.

f. Would not degrade information technology support for deployment execution or war planning mission.

g. Provide the commander with the best possible situational understanding of deployment planning and mission execution.

h. Provide the capability to display JOPES IT data on the Global Command and Control System (GCCS) Common Operational Picture (COP)

4. General JOPES Criteria

a. Application Functionality. The performance and effectiveness of the applications (Rapid Query Tool (RQT), JOPES Editing Tool (JET), Web Scheduling and Movement, etc.) within each release of JOPES IT software will be 'as good as or better' than the retired JOPES IT version.

b. Database Synchronization and Integrity. Data is processed into the database correctly, and synchronization of databases is maintained throughout

the network automatically, in accordance with Enclosure I, JOPES Key Performance Parameters (KPPs).

c. Coverage. All users who must participate in contingency and crisis action planning and execution, and are currently supported by GCCS, will have access to JOPES IT. JOPES IT supports shipboard/forward-deployed users in austere locations, with low bandwidth communications capability.

d. JOPES Functional Management. Ensures that TPFDD initiation, database audits, access controls, permission, and other required functional management capabilities are operational.

e. Interfaces. All required external interfaces are supported with existing input formats (B8, H3). Information required by and from interfaces is easy to transfer to and from the JOPES database. The Data Exchange Format (DEX) is an available format used by the JOPES Data Network Services (JDNETS) interface mechanism to exchange JOPES data with external systems in the JOPES V4.X format. Technical information and files have been made available for developers to achieve interface compatibility with the JOPES database.

f. User Interface. Applications will be developed which are easy to use, with imbedded "Help" capabilities and tutorials. User interface is consistent across multiple functional areas. User functions can be performed with minimal technical knowledge.

g. Performance. Response time meets or exceeds threshold JOPES performance parameters.

h. Reliability. Meets or exceeds threshold JOPES KPP reliability standards.

i. Documentation. JOPES IT is supported by required policy and procedural changes and user documentation.

j. Training. Users are adequately trained to conduct operations and accomplish their missions and tasks.

k. Newsgroups. References k and m require the establishment of newsgroups to support crisis operations. Newsgroups exist in two forms (local and global). Newsgroups are the primary means of coordinating deployment, redeployment, planning, and execution. This includes backup and restore capability.

(INTENTIONALLY BLANK)

ENCLOSURE B

JOPEs IT ARCHITECTURE

1. General. The JOPEs v4.X environment consists of Fixed and Deployable Strategic Server Enclaves. All enclaves communicate over the SIPRNET and provide services to registered users through GCCS-J v 4.X workstations employing the Mozilla FireFox Web browser. Figure 1 shows the overarching Strategic Server Enclave Architecture. Deployable Strategic Server Enclaves (DSSEs) have an identical logical configuration to the Fixed Strategic Server Enclaves (FSSEs).

JOPEs v4.X Strategic Server Enclave Notional Architecture

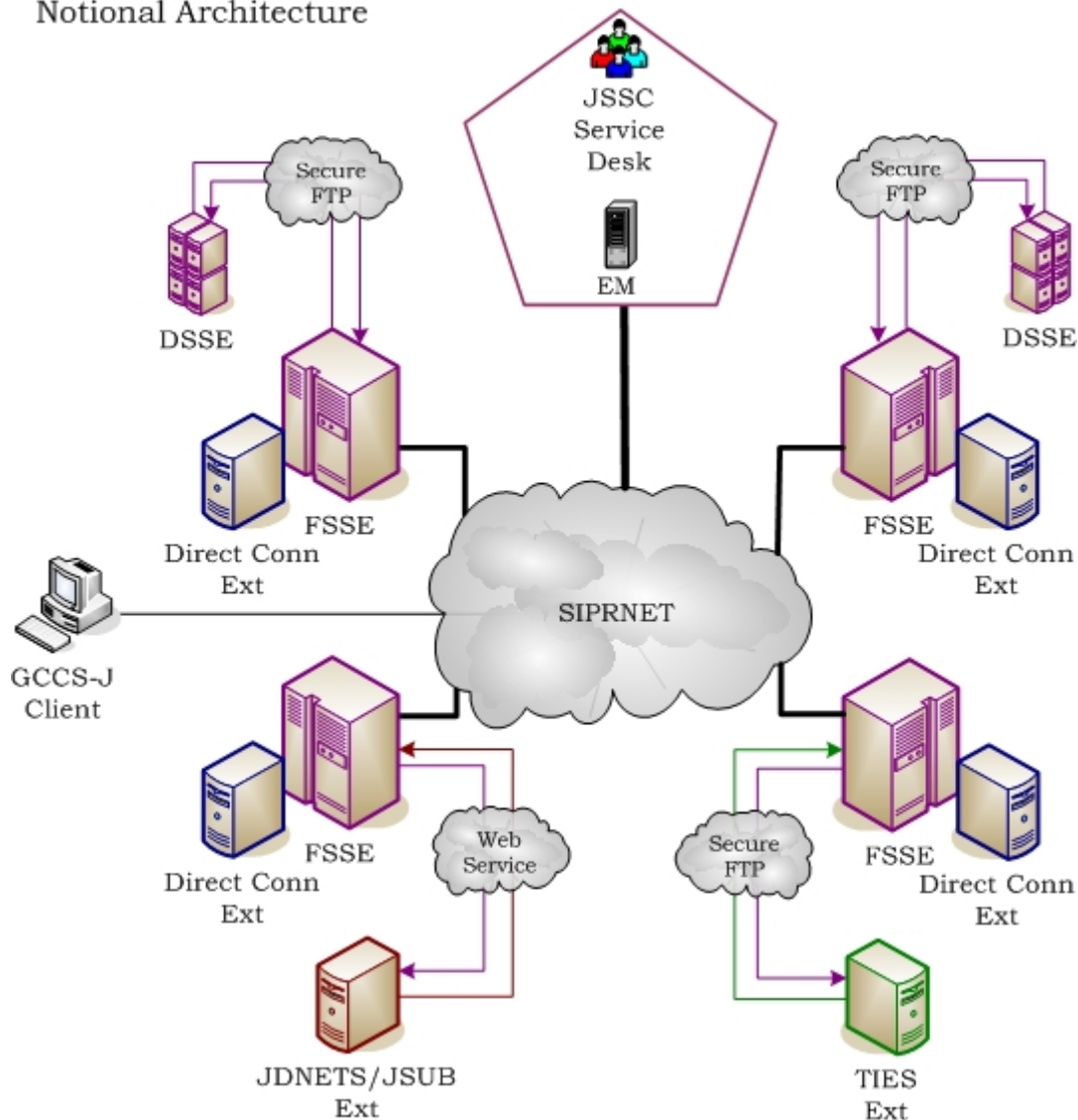


Figure 1. Strategic Server Enclave Notional Architecture

2. Fixed Strategic Server Enclave. Each enclave contains a JOPES database server, two application servers, two Web servers, a logical print server, and an enclave management server. To assure redundancy and security at each site, two 10Mbps-minimum circuits connect to two SIPRNET Nodes (1 circuit per node) from a premise/filter router, which in turn is connected to the JOPES Fixed Strategic Server enclave, as shown in Figure 2. This connection shall be external to any site-specific defense mechanisms such as firewalls or intrusion detection systems. Software available within the enclave includes JOPES IT products listed in Figure 3.

JOPES v4.X Strategic Server Enclave Fixed SSE Architecture

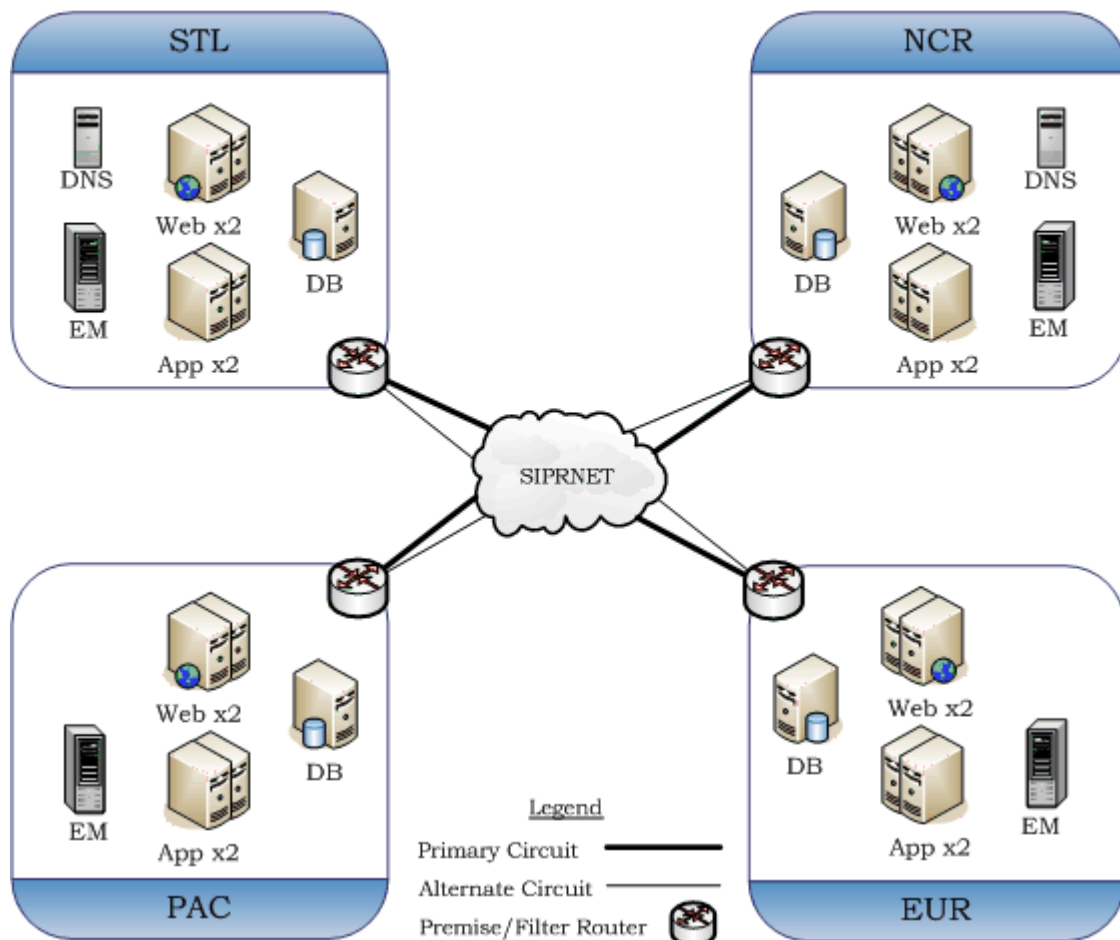


Figure 2. Fixed Strategic Server Enclave Architecture

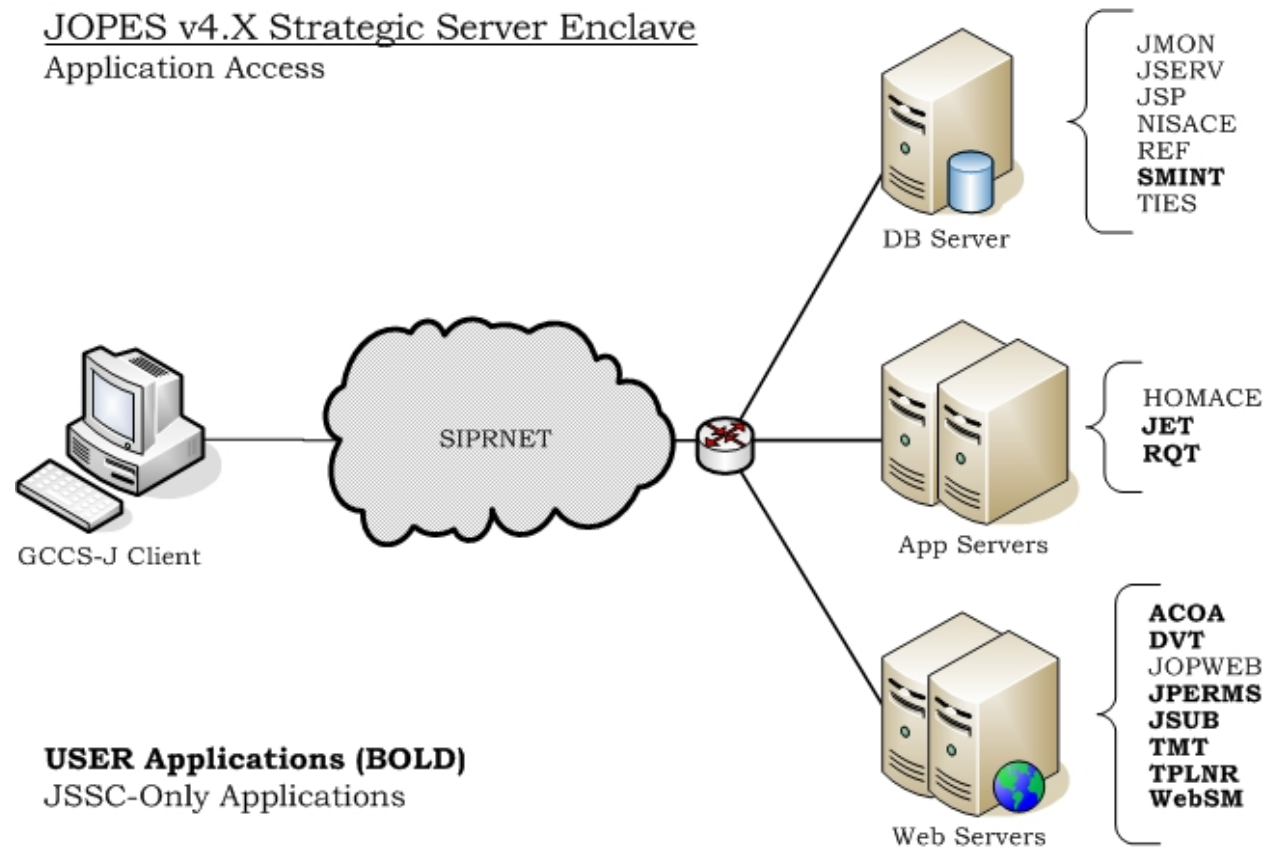
a. FSSE JOPES Database Server. A JOPES v4.X FSSE database server houses a fully synchronized and redundant instantiation of the JOPES v4.X database.

b. FSSE JOPES Application Server. Two JOPES v4.X FSSE application servers host the client-server based applications (JET and RQT). The primary application server also houses dedicated print services required for printing from the JOPES v4.X SSE environment to global printers.

c. FSSE JOPES Web Server. Two JOPES v4.X FSSE Web servers provide access to the Web-enabled applications and Web services to external systems.

d. FSSE Enclave Management Server. The Enclave Management Server will run Oracle Enterprise Manager (OEM) and other Commercial Off-the-Shelf (COTS) tools necessary for the centralized management of enclave servers. This server will be identically configured at each site and allows most management functions to take place within the local enclave. It is the only server within the enclave that communicates directly to the master management server located in JSSC.

e. Domain Name Server (DNS). The two CONUS FSSEs include DNS servers to resolve world-wide <...>.jopes.smil.mil addressing.



Note: ACOA and DVT expected to retire FY 12
Figure 3. Strategic Server Application Access

Index to JOPES application acronyms:

ACOA Adaptive Course of Action (*expected to retire FY12*)
DVT Deployment Visualization Tool (*expected to retire FY12*)
HOMACE Home Account Creation Extension
JET JOPES Editing Tool
JMON JOPES Monitor
JOPWEB JOPES Web Page
JPERMS JOPES Permissions
JSERV JOPES Server Manager
JSP JOPES Synchronization Processor
JSUB JOPES Subscriptions
NISACE NIS+ Account Creation Extension
REF JOPES Reference File Manager
RQT Rapid Query Tool
SMINT Scheduling and Movement Interface
TIES Transitional Interface to External Systems
TMT TPFDD Management Tool
TPLNR TurboPlanner
WebSM Web Scheduling and Movement

3. Deployable Strategic Server Enclave. Each DSSE contains a JOPES database/application server, a Web server, and an enclave management server. Dedicated bandwidth is highly desired but not required to field a DSSE. The DSSE will connect to a SIPRNET node or initial instantiation of the site network. This connection shall be external to any site-specific defense mechanisms such as firewalls or intrusion detection systems.

a. DSSE JOPES Database/Application Server. A JOPES v4.X DSSE Database/Application Server houses a fully synchronized instantiation of the JOPES v4.X database with the data necessary to support the deployment. This server also contains the print server functionality to perform print services for the deployed environment only.

b. DSSE JOPES Web Server. A JOPES v4.X DSSE Web Server includes Web access and Web automation software products. This functionality supports the requesting Combatant Commander's deployed environment only.

c. DSSE Enclave Management Server. The Enclave Management Server will run OEM and other COTS tools necessary for the centralized management of enclave servers. This server will be identically configured at each site and will allow most management functions to take place within the local enclave. It

will be the only server within the enclave that communicates directly to the master management server located in the JSSC.

4. Master Management Server. The Master Management Server is located at the JSSC and will run OEM and other COTS tools necessary for the centralized management of enclave management servers. This server will communicate directly with the enclave management servers located in the FSSEs and DSSEs.

5. Clients. GCCS-J v4.X releases support Windows XP (or later version depending on GCCS-J v4.X release) clients for JOPES functionality. Individual sites are responsible for developing local policies to manage their specific clients. Organizations should consult the current *GCCS Network/Hardware Standard Configuration and Recommendations* for guidance.

6. External System Interfaces. External systems interface with the JOPES v4.X database in multiple ways. Once the data is presented to JOPES v4.X environment, the JOPES synchronization performance parameters apply. External system interfaces are discussed in Appendix A.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE B

EXTERNAL SYSTEM INTERFACES

1. General. An external system represents any application or system external to the JOPES enclave that accesses JOPES data. There are several methods external systems use to share data with JOPES IT. These methods are listed in Figure 4.

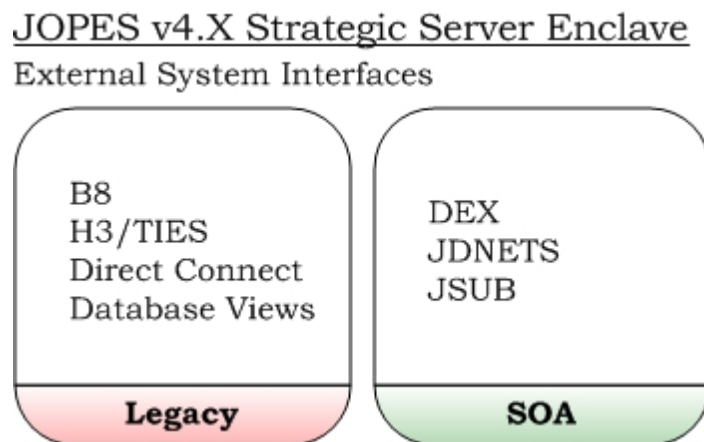


Figure 4. External System Interfaces

2. Legacy Interfaces. Legacy interfaces will be deprecated from JOPES IT once all external systems using them migrate to a SOA interface.

a. B8

(1) The B8 is an acronym derived from a menu structure that existed in the Worldwide Military Command and Control System (WWMCCS), pre-dating the Global Command and Control System (GCCS). The B8 is often referred to as a “flat-file” format in that a positional format is used to define the location of a data element in a character string. The B8 has not been maintained and does not fully support all JOPES Reporting Structure (JOPESREP) data requirements or all JOPES v4.X data elements. The B8 does not process carrier data.

(2) The TPFDD Management Tool (TMT) provides the only capability to download and upload a B8 file. Use of the B8 is a manual process; JOPES-IT provides no automated B8 transfer mechanisms for use by external systems.

b. H3

(1) The H3 is an acronym derived from a menu structure that existed in the WWMCCS, pre-dating the GCCS. The H3 represents a set of WWMCCS formatted synchronization transactions. This transaction set was used by JOPES Classic for synchronization prior to migration to JOPES v4.X. The H3 has not been maintained and does not fully support all JOPESREP data requirements or all JOPES v4.X data elements. The H3 can contain carrier data.

(2) The TMT provides the capability to manually download and upload an H3 file.

c. Transitional Interface to External Systems (TIES)

(1) External systems that utilize the H3 JOPES Classic transaction format are able to interface with JOPES through the TIES interface. Data both sent and received from JOPES is converted to the JOPESREP current format, resulting in the potential loss of JOPES v4.X data elements and meaning.

(2) TIES processes all H3 formatted transaction files transferred by both automated means from external systems or manually through TMT. Both incoming and outgoing H3 files are handled through TIES.

d. Direct Connect

(1) Direct connect refers to unrestricted access by an external system to the JOPES database. This approach optimizes performance and data access but results in adverse programmatic entanglements.

(2) In the event of performance and interoperability issues for a critical interface, an external system may be permitted to directly connect to a JOPES database. Examples of this include the four Deliberate and Crisis Action Planning and Execution Segments (DCAPES) enclaves co-located with the four JOPES fixed strategic server enclaves.

(3) Direct connect is not a preferred method for access primarily because of the tight coupling implications between systems. The future intent of JOPES IT is to minimize the use and/or eliminate all direct-connect interfaces.

e. Database Views. Database views are very similar to direct connect except that the external system does not have direct access to the core JOPES database tables. Database views allow external systems to view the JOPES

v4.X database structure in any desired format, to include the JOPEsREP 1996 format. Access to specific tables and fields can be controlled through a database view. Use of database views are preferred over direct connect, although it is less preferred than SOA approaches.

3. Service Oriented Architecture (SOA) Interfaces

a. Data Exchange

(1) The DEX format is an extension of the JOPEs Synchronization Processor (JSP). DEX is a set of XML-compliant JSP transactions created from JSP transactions that are passed between enclaves. A DEX transaction represents a row within a JOPEs database table. External systems may subscribe to outgoing DEX transactions using the JSSC controlled DEX/JDNETS interface or the DEX/JSUB interface (but not both for the same domain).

(2) Incoming DEX updates to JOPEs are only supported through the JDNETS Web services that interface with JSP. JSUB does not support incoming DEX JOPEs database updates, although an external system may elect to receive DEX updates via JSUB and send DEX updates via JDNETS. DEX update transactions will be processed commensurate with the permissions granted to the JOPEs username passed in the DEX transaction.

(3) The DEX/JDNETS implementation requires the JSSC FM Office to use the JSP application to setup specific TPFDD subscriptions and data content, to include JOPEs table and data field names. The JSSC also uses the JSP application to monitor the health of the interface at the JOPEs point of connectivity.

(4) The DEX/JSUB implementation removes control of the data subscription from JSSC and requires administrators of the external system to manage the TPFDD subscription and data content through the JSUB Web application. A JOPEs user account used by the external system administrator requires the JSUB USER application role in JPERMS to access the JSUB Web application. JSUB also provides a tool for the JSSC to monitor the health of the JSUB interface.

b. JOPEs Data Network Services

(1) The primary purpose of the JDNETS interface is to field a comprehensive suite of fine-grained Web services as a machine-to-machine interface available to an external system to query and/or update JOPEs data. An external system can develop user applications based on these Web services,

avoiding the complexity of implementing a mirror JOPES database and supporting JOPES business logic.

(2) JDNETS also provides Web services that allow external systems to send and receive subscribed DEX formatted transaction files between the external system and JOPES.

(3) JDNETS Web services are accessed through the username and password of the external system. Access to JOPES TPFDD data is controlled by the individual permissions of the JOPES username presented by the external system at the time of the service request by the external system.

c. JOPES Subscription (JSUB)

(1) The JSUB interface is a Web application that permits external system administrators to directly manage DEX TPFDD subscription content. JSUB collects the subscribed DEX transactions generated by JSP, and provides them to the external system.

(2) The DEX/JSUB interface provides the same outgoing DEX content as the DEX/JDNETS content, but requires external system administrators to manage their TPFDD subscriptions, as opposed to JSSC managing the subscription on their behalf. JSUB does not support incoming DEX JOPES updates to the JOPES database, but JDNETS Web services may be used in conjunction with JSUB for this purpose.

ENCLOSURE C

USER ACCOUNT MANAGEMENT

1. Purpose. This enclosure establishes procedures throughout the JPEC necessary for the establishment, control, and management of JOPES user accounts in the JOPES Permissions (JPERMS) application. Information contained in this enclosure set standard procedures for User Identification (USERID) naming convention across all JOPES v4.X applications and for account management in JPERMS.

2. Software Description

a. The JPERMS Web-based application provides JOPES account management capability. User accounts have various attributes that provide basic user information and, most importantly, TPFDD permissions by OPLAN-series with specific access and interface authorizations.

b. JPERMS is used to create and maintain JOPES IT accounts. Account security and access permission changes are then replicated to other JOPES enclaves using a combination of transaction replication and Network Information Service Plus (NIS+) replication.

3. Types of JOPES IT Accounts. JPERMS supports three types of accounts.

a. Regular User Account. A regular user JOPES IT account is a composite of a UNIX account, an Oracle account, and a JOPES permission set. User accounts have various attributes that provide basic user information and, most importantly, allow FM's to grant TPFDD permissions by Series or by individual PID. The UNIX account provides GCCS-J security and access permissions. The Oracle account enables the interface with the Oracle-based JOPES database. All three levels are required for access to JOPES data.

b. External User Account. An external user JOPES IT account consists of only a JOPES permission set; no Oracle or UNIX account is created. External JOPES IT accounts exist to give users of JDNETS-based systems external to JOPES access to JOPES data in those systems, without the burden of a JOPES IT password to maintain. No access to a JOPES enclave is available with an external JOPES account

c. Domain Account. A domain account consists of only an Oracle account and password; no UNIX account is created nor TPFDD permissions granted. This type of account establishes external domains within JOPES IT, and

provides external systems authorization to connect through the JDNETS and JSUB interfaces.

JOPEX v4.X Strategic Server Enclave
JPERMS Account Types

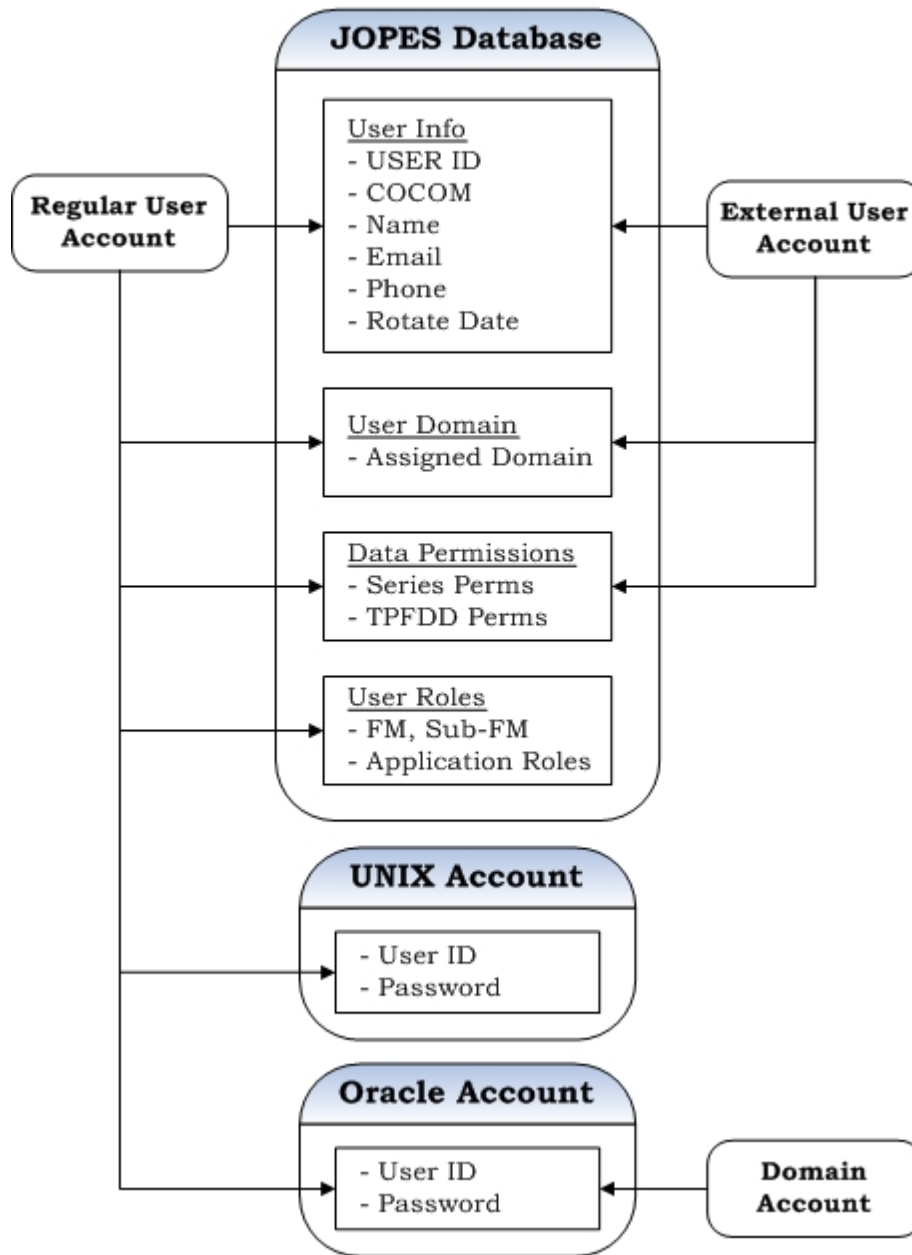


Figure 5. JPERMS Account Types

4. JPERMS Operators. JPERMS supports five levels of JPERMS operators.

a. JOPESFM Super-User. The JSSC FM office has the all-series JOPES Functional Manager (JOPESFM) super-user account. This account can look across all series and TPFDDs. It has the ability to create, modify, or delete any user at any site, create and remove external domains, and grant any application role to any user. This account is used to create and modify series functional manager (series-FM) accounts.

b. Series-Functional Manager. The Series-FM privilege is assigned per TPFDD series. The Series-FM has access across all TPFDDs in their respective series. More than one user account may have series-FM privileges for a series providing series-FM backup. They can create and delete JOPES Subordinate Functional Manager (sub-FM) accounts for their series. Series-FMs and sub-FMs can create, delete, and manage user accounts with access to their series or individual TPFDDs in their series. They may grant accounts created by other series-FMs privileges to their series, or to individual TPFDDs in their series. They are not able to modify or delete user accounts that are assigned command or Service series outside the series-FM's assigned command or service series. Each series-FM will be granted sub-FM privileges to all other series at account creation to facilitate their own user management processes.

c. Sub-FM. The sub-FM privilege is assigned per TPFDD series. The Sub-FM for a series can look across all TPFDDs in their series. More than one user account may have sub-FM for a series. A sub-FM may **not** create or delete other sub-FM accounts for their series. A sub-FM may create, delete, and manage user accounts, but may only assign read and update permissions for TPFDDs in their series. Sub-FM for a series can re-activate a user, but may not adjust the rotate date for a user. Sub-FM permissions are granted by the series-FM.

d. User (JOPES User). A JOPES user may use JPERMS to see what application roles they have been granted; view their password expiration date; access their user detail information; and update password, user name, SIPRNET e-mail address, and the phone number of their user detail information. A JOPES user may also search for other JOPES users and view their contact information. The series-FM or sub-FM will make the final determination of application roles assigned to a user. Application roles available in JPERMS are listed in Table 1.

e. ACOA Administrator. An ACOA administrator can view and modify echelons for users in their command.

5. Roles and Responsibilities

a. JSSC Service Desk

(1) The JSSC service desk is the primary point of contact for all user account problems forwarded by the user's series-FM. All non-FM JOPEs users will initially be directed to their command/service JOPEs Functional Manager for problem validation. The only exceptions to this policy are listed below.

(a) The JSSC service desk will assist deployed users with password reset requests through the SIPRNET e-mail address stored in JPERMS without series-FM validation. If the deployed user has a deployed SIPRNET e-mail address different from the JPERMS e-mail address, the user's name must clearly match the new e-mail address in order for a password reset to be performed and sent to the user.

(b) The series-FM may request the JSSC service desk by e-mail to assist their command's/Service's JOPEs users while no series-FM will be available. Examples of this include holiday office closings and non-duty hour requests. The e-mail request must specify specific duties that the JSSC service desk is permitted to perform.

(2) No requests for expiration date, TPFDD permission, or application role modifications for non series-FM users will ever be acted upon by the JSSC service desk.

b. JSSC Functional Manager Office

(1) The JSSC FM office is responsible for creating, modifying, and deleting all series-FM accounts.

(2) The JSSC FM office will create, manage, and delete all Joint Staff and National Military Command Center (NMCC) JOPEs accounts, on behalf of the CJCS JOPEs series-FM.

c. Series Functional Manager

(1) FMs are responsible for maintaining their command's users in JPERMS. Series-FMs will create, manage, and delete users in their command and manage their command's series TPFDDs permissions.

(1) Series-FMs will review user accounts bi-annually at a minimum. FMs will reconcile users with other command FMs bi-annually in order to purge the databases of outdated accounts and to ensure that each user has a requirement to access specific series TPFDDs.

(1) Annually, series-FMs will ensure expired passwords are updated or expired accounts are deleted.

d. Series Information Assurance Office (IAO)

(1) Series IAOs will assist the JSSC FM office IAO and Series-FM with password management.

(2) The Series IAO will enforce security regulations within their respective commands.

6. Account Details. The following fields define each JOPEs user account.

a. Account Type. All new users that require access to a JOPEs or DCAPEs enclave are created as a 'Regular User' account. Users of external systems that access JOPEs data, but do not utilize the JDNETS interface, also require a 'Regular User' account. Users that will only access JOPEs data on external systems utilizing the JDNETS interface require an 'External User' account. An external user cannot access JPERMS or use JOPEs directly. This account type is used to define a JOPEs permission set for access control to series and TPFDDs. An 'External User' will only be granted external domains (see paragraph 6.i.(3) below).

b. User ID. Identifier that the JOPEs user will use for login. A user ID must be 8 characters. This is a required field. See paragraph 7 below for user ID construction.

c. Password. A required field for a regular user account. No password is required for external accounts. Password entry shall have a second field where the password will be re-entered to validate the password entered in the first field. See paragraph 8.a. for password composition.

d. User Name. User name will be in last name, first name, middle name, and rank format. User Name is a required field for an account.

e. Phone. This is a free text field that could contain one or several phone numbers and/or pager or other contact information.

f. Secret Internet Protocol Router Network (SIPRNET) E-mail. SIPRNET e-mail is a required field for an account. A single SIPRNET e-mail address will have a single user name associated to it. Multiple user names will not contain the same SIPRNET e-mail address.

g. Rotate Date. Rotate date will follow the MM/DD/YYYY format. On the rotate date for an account, the account will automatically be inactivated. Reactivation requires positive action by the series-FM.

h. Command. Command is a required field for an account. From this drop down menu each account creator will select the user's parent combatant command (primary) or higher headquarters (secondary). JPERMS provides a list of the following commands.

- (1) CJCS (Chairman of the Joint Chiefs of Staff)
- (1) COMDT COGRD
- (1) HQ AIR FORCE
- (1) HQ ARMY
- (1) HQ MARINES
- (1) HQ NAVY
- (1) NORAD/USNORTHCOM (North American Aerospace Defense/United States Northern Command)
- (1) USAFRICOM (United States Africa Command)
- (1) USCENTCOM (United States Central Command)
- (1) USEUCOM (United States European Command)
- (1) USPACOM (United States Pacific Command)
- (1) USSOCOM (United States Special Operations Command)
- (1) USSOUTHCOM (United States Southern Command)
- (1) USSTRATCOM (United States Strategic Command)
- (1) USTRANSCOM (United States Transportation Command)

i. Domain(s). A JOPES user is assigned each domain needed for access to JOPES data. The three categories of domains available are:

(1) JOPES. Standard JOPES users will only be assigned the JOPES NIS+ master domain. The domain list for JOPES enclave access includes the JOPES NIS+ master for the FSSEs and each DSSE. Adding a JOPES domain requires a new password to be supplied.

(2) DCAPES. The DCAPES domain is intended for users that will access DCAPES enclaves. Adding the DCAPES domain requires a new password to be supplied.

(3) External. The domain list for external access includes all external systems utilizing the JDNETS interface with JOPES. To successfully process updates generated on external domains through JDNETS, that external domain must first be granted in JPERMS to the user that generated the updates. Adding an external domain does not require a new password to be supplied.

j. Group(s) (Optional field). A given user ID may be in one or more groups. User IDs are not required to be in a group. A group is a list of user names, which behaves in other parts of JPERMS as if the entire user name list had been entered one at a time. The group concept is for convenience when many users need the same privileges granted or revoked.

k. FM (Granted by the JSSC FM Office). Assigns series-FM permissions to a user name on one or more series. Only the JSSC FM office super-user account can create or delete series-FM accounts.

1. Sub-FM (Granted by JSSC FM Office or Series-FM). Assigns sub-FM privileges to a user name on one or more series. The list of series available from which to choose from is limited to those which are granted by the FM privileges. A series-FM may only assign sub-FM permissions for their series. All series-FM accounts are assigned sub-FM permissions on all other series at account creation.

m. JPERMS Database (DB) Role. This field allows the series-FM or sub-FM to assign roles to users enabling/disabling access to particular applications for regular accounts. No roles can be granted to external accounts.

(1) Only roles granted to a FM/sub-FM are visible in JPERMS. No FM can view or grant a role they are not assigned.

(2) Table 1 below lists roles that can be assigned to a USERID. The table is grouped by operational areas. The first group is for a general JOPES user (all users should receive these roles). In the second grouping are specific user roles granted if the user responsibilities require the role. The third group consists of roles intended for JSSC use only.

JPERMS Database Roles		
User Type	Database Role	Database Role Explanation
General User	JET_USER	The JET_USER role is necessary for the operation of the JOPES Editing Tool (JET)
General User	RQT_USER	The RQT_USER role is necessary for the operation of the Rapid Query Tool (RQT).
Mission-specific User	ACOA_ADMIN *	The ACOA_ADMIN role is necessary for a user to modify the echelon for other users in their command for the Adaptive Course of Action (ACOA) Web application.
Mission-specific User	ACOA_USER *	The ACOA_USER role is necessary for a user to access the ACOA Web application.
Mission-specific User	CLASSIC_USER	The CLASSIC_USER role is created for 3.X Classic users connecting to the JOPES database. The data returned represents the current JOPESREP. Common Operational Modeling,

JPERMS Database Roles		
User Type	Database Role	Database Role Explanation
		Planning and Simulation Strategy (COMPASS) and FOCUS users require the CLASSIC_USER role.
Mission-specific User	DVT_USER *	The DVT_USER role is for Deployment Visualization Tool (DVT) users.
Mission-specific User	GORA_COP_USER	The GORA_COP_USER role modifies the role created by GORA for COP users connecting to the JOPEs database.
Mission-specific User	JOPEs_COMPASS_USER	The JOPEs_COMPASS_USER role is needed for COMPASS users to access JOPEs data.
Mission-specific User	JOPEs_DARWIN_USER	The JOPEs_DARWIN_USER role is required for Dynamic Analytical Reporting Web-based Interactive Navigator (DARWIN) users to access JOPEs data.
Mission-specific User	JOPEs_GCSS_USER	The JOPEs_GCSS_USER role is necessary for Global Combat Support System (GCSS) and Joint Planning and Execution Services (JPES) users to access JOPEs data.
Mission-specific User	JOPEs_GORA_USER	The JOPEs_GORA_USER role is necessary for GSORTS Oracle Client (GORA) users to access JOPEs data.
Mission-specific User	JOPEs_JRAMS_USER	The JOPEs_JRAMS_USER role allows JOPEs Readiness Automated Management System (JRAMS) users to access JOPEs data.
Mission-specific User	JOPEs_SMS_USER	The JOPEs_SMS_USER role allows Single Mobility System (SMS) users to access JOPEs data.
Mission-specific User	JOPEs_WHQ_USER	The JOPEs_WHQ_USER role is used for Web Hoc Query (WHQ) users to access JOPEs data.
Mission-specific User	JSUB_USER	The JSUB_USER role allows an administrator for a JSUB external system to access the JSUB Web-based application and modify settings for JPERMS assigned JSUB external systems.

JPERMS Database Roles		
User Type	Database Role	Database Role Explanation
Mission-specific User	SMINT_USER	The SMINT_USER role allows the user to access the database using the Scheduling and Movement Interface (SMINT). This is a USTRANSCOM-assigned database role.
Mission-specific User	TMT_PID_USER	The TMT_PID_USER role allows the user to create, delete, and update TPFDDs using the TPFDD Management Tool (TMT).
Mission-specific User	TMT_USER	The TMT_USER role allows the user to download or upload TPFDDs using the TMT.
Mission-specific User	TPLN_ADMIN	The TPLN_ADMIN can create other TPLN_ADMIN users, TPLN_CREATOR users and TPLN_USERS. They can also edit other users plans in TPLNC should an author of a plan get deleted from the database. They can delete plans and create or edit organizations.
Mission-specific User	TPLN_CREATOR	The TPLN_CREATOR allows a user to create and edit plans in TurboPlanner. They can create other users if they are an FM or SubFM. They have permission to view and edit plans that they are given permission to in TurboPlanner Client.
Mission-specific User	TPLN_USER	The TPLN_USER role allows read-only access in TurboPlanner to a user. The user has permissions to view plans that they are given permission to in TurboPlanner Client.
Mission-specific User	WEBSM_ORGANIC_USER	The WEBSM_ORGANIC_USER role allows organic carrier changes plus manifesting of common carriers via the Web Scheduling and Movement (WebSM) application.
Mission-specific User	WEBSM_READ_USER	The WEBSM_READ_USER role allows the user to view common user and organic carrier itineraries and associated allocation/manifest data via the WebSM application.

JPERMS Database Roles		
User Type	Database Role	Database Role Explanation
Mission-specific User	WEBSM_USTC_USER	The WEBSM_USTC_USER role allows the user to enter common user (USTC assigned/managed) carrier itineraries and associated allocation/manifest data via the WebSM application.
JSSC User	JDNETS_ADMIN	The JDNETS_ADMIN roles allow administrators access to the JDNETS diagnostic Webpage.
JSSC User	JOPWEB_ADMIN	The JOPWEB_ADMIN role allows administrators access to Web-based application errors and provides the ability to modify the JOPES Web menu. This is a JSSC-only database role.
JSSC User	JSERV_ADMIN	The JSERV_ADMIN role starts the JSERV GUI. This is a JSSC-only database role.
JSSC User	JSERV_<server>_USER	The JSERV_<server>_user role starts the JSERV GUI. This is a JSSC-only database role.
JSSC User	JSP_USER	The JSP_USER role is created for administrators accessing JOPES Synchronization Processor (JSP). This is a JSSC-only database role.
JSSC User	JSUB_ADMIN	The JSUB_ADMIN role allows administrators to access the JSUB Web-based application and modify settings for all JSUB external domains. This is a JSSC-only database role.
JSSC User	REF_USER	The REF_USER role allows the user to access the Reference application. This is a JSSC-only database role.
JSSC User	TIESRV_ADMIN	The TIESRV_ADMIN role grants permissions to operate the Transitional Interface to External Systems (TIES) GUI. This is a JSSC-only database role.
JSSC User	TIESRV_DAEMON	The TIESRV_DAEMON role is only assigned to the TIESERV user. This is a JSSC-only database role.
JSSC User	TIESRV_TG	The TIESRV_TG (Transaction Generator) role is only assigned to the TIESRV_DAEMON role. This is a JSSC-only database role.

JPERMS Database Roles		
User Type	Database Role	Database Role Explanation
JSSC User	TIESRV_TP	The TIESRV_TP (Transaction Processor) role is only assigned to the TIESRV_DAEMON role. This is a JSSC-only database role.

** ACOA and DVT expected to retire FY12*

Table 1 JPERMs Database Roles

7. User Identification (ID) Construction. User IDs will be eight characters long as described below.

a. The first digit reflects the command, Service, or agency designator. Permanently assigned subordinate units of combatant commands (to include USFK, USFJ) shall use that combatant command as their first digit. Units having multiple command relationships shall use the first digit of their respective Service. Organizations not listed in this sub paragraph shall use 'Z' as the first digit. See Table 2 below.

Command Service Designator			
0	Not to be used	I	Not to be used
1	Not to be used	J	Joint Staff
2	Not to be used	K	AFRICOM
3	Not to be used	L	RESERVED
4	Not to be used	M	Marines
5	Not to be used	N	Navy
6	Not to be used	O	Not to be used
7	Not to be used	P	USPACOM
8	Not to be used	Q	USSOCOM
9	Not to be used	R	NORAD
A	Army	S	USSOUTHCOM
B	USNORTHCOM	T	USTRANSCOM
C	USCENTCOM	U	USSTRATCOM
D	DISA	V	DIA
E	USEUCOM	W	DLA
F	Air Force	X	RESERVED
G	Coast Guard	Y	DTRA
H	Joint Staff <i>(will transition to J over time)</i>	Z	Other Government Agency (OGA)

Table 2. Command/Service Designator

b. The second digit defines the functional relationship to the first digit, including other government agencies (OGAs, first digit = 'Z').

- C Combatant Command
- A Army
- F Air Force
- J Joint
- K SOC
- M Marines
- N Navy
- Q USFK
- R USFJ
- S ALCOM
- T NORAD

For Other Governmental Agencies (OGAs)

- 0 Primary organization or headquarters of first digit
- 1 CIA
- 2 FBI
- 3 NSA
- 4 RESERVED
- 5 FAA
- 6 NGA
- 7 FEMA
- 8 RESERVED
- 9 RESERVED

c. The remaining six characters are assigned by the FM/sub-FM using the letters of the last-name, first initial, middle initial, and numeral(s) on the end for short names.

d. It is recommended, but not required, that the third character be assigned to define the functional area as user is assigned.

- 1 (Personnel)
- 2 (Intelligence)
- 3 (Operations)
- 4 (Logistics)
- 5 (Plans)
- 6 (Communications)
- 7 (Civil Engineer)
- 8 (Force Structure)
- 9 (Integration)

e. User ID examples:

hj3rowai	Joint Staff user (Ms. Iris Rowand)
bccoxrj0	NORTHCOM user (Mr. R. J. Cox)
pfblaimt	PACAF user (Sgt Michael T. Blair)
z34dalbt	NSA logistical user (Ms Beau T. Dallis)
z6pughn0	NGA user (Mr. N. (No middle initial) Pugh)
mmuzahcc	1st MEU user (Zahara LCpl Christopher C)

8. Password Management. Each new regular user is provided with a unique USERID/password pair. When the new user logs onto JOPES v4.X for the first time, the user must change the password immediately to a new password that is known only to the user.

a. Password Composition. A password must meet all of the following criteria:

- (1) Be exactly 15 to 30 characters in length
- (2) Contain at least two upper case and two lower case alphabetic characters
- (3) Contain at least two numeric characters
- (4) Contain at least two of the following special characters:
! #) (* + , - ; : < = > ? ~ ^ } { |
- (5) Contain no repeated characters, such as aa
- (6) Contain no special character as the first character.
- (7) Contain at least four new characters from the user's previous password
- (8) Cannot closely resemble the user ID
- (9) Must begin with a letter
- (10) JPERMS does not permit the user to imbed the USERID string or any word string from the user name in the password. For example, if the USERID is TC5J7000 and the JPERMS associated user name is John Doe, JPERMS will not allow the strings TC5J7000, John or Doe to be part of the password.

b. Password Lifetime. Password lifetime refers to how long a password is valid on the system. IAW DODI 8500.2, to the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password. The minimum password lifetime is 14 days to ensure that a user does not change his or her password multiple times in a short period of time (i.e., a few minutes, hours, or several days). This rule does not apply if another user changes the password within that time. For example, if a sub-FM changes a user's password, the user may then change the password even though it had recently been changed. The maximum lifetime for a password is 56 days. The user is responsible for changing his/her password every 56 days. Users may not repeat a password used as one of their previous 10 passwords.

c. Password Monitoring. JSSC will execute a password crack tool to check the strength of each password maintained on the system. The JSSC will notify the series-FM regarding "weak" passwords that are cracked belonging to users

within their respective series. The series-FMs will promptly notify the user of the cracked passwords, remind them of the password composition instructions, and instruct them to create new passwords.

d. Other Password Considerations. All factory set, default, or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys.

9. Inactive User Accounts. A user account becomes inactive under any of these conditions: the account reaches its rotate date; a password reaches its expiration date; activity ceases permanently; or activity ceases for a period that exceeds site-specified rules (30 days within JOPES). Examples of inactivity include: the user is on extended leave or travel; the user may have changed work location; or account access is no longer required because the user's work responsibilities have changed.

a. Deactivating Inactive Accounts. The Series FM is responsible for deactivating JOPES user accounts which lapse for non-use (a period of 30 days or more). Deactivation shall occur within 48 hours of the disqualifying event. The JSSC also has the authority to deactivate accounts. If the account is not re-activated within 30 days, the JSSC shall notify the series-FM of the account to be deleted. JPERMS and procedures in paragraph 9.c. apply.

b. Expired Accounts. JOPES account passwords expire 56 days from the last password change. Accounts expired for a period of 30 days will be considered inactive IAW paragraph 9.a. and be deleted.

c. Deleted Accounts. A JOPES user will have no access to JOPES IT once the user account is deleted. Functional managers may identify deleted user accounts to the JSSC service desk for re-entry to the operational system within a period of 30 days from the date of deletion. Thirty days after the user account is deleted, all information will be removed from the system.

10. JOPES Permission Set. The JOPES permission set controls user's access and privileges to individual TPFDDs and entire series. This permission is to be enforced in all external systems that access JOPES data. The JOPES permission set also determines the delegation of privileged capabilities to other users. Because JOPES uses Oracle's Row Level Security (RLS), proper TPFDD permissions are necessary for a user to see that a given TPFDD exists.

a. Series Permissions. Permissions assigned at the Series level are automatically inherited by each of the associated non-restricted TPFDDs in that series, unless specifically overridden at the TPFDD level. Table 3 lists the available series-level permissions available to a JOPES user.

Series Permissions	
Permission	Description
Read	The user has read access to all TPFDDs in the series, except restricted TPFDDs.
Update	The content of TPFDD in the series may be changed, except restricted TPFDDs.
Create	The user can create a new TPFDD in the series.
sgComp	The Supporting Component validation date may be set for any ULNs within the TPFDD series, except restricted TPFDDs.
sgCCDR	The Supporting Combatant Commander validation date may be set for any ULNs within the TPFDD series, except restricted TPFDDs.
sdComp	The Supported Component validation date may be set for any ULNs within the TPFDD series, except restricted TPFDDs.
CCDR	The Supported Combatant Commander validation date may be set for any ULNs within the TPFDD series, except restricted TPFDDs.
USTC	The USTRANSCOM status flag may be set for any ULNs within the TPFDD series, except restricted TPFDDs.
FM	The user has been granted Functional Manager permission for this series. If this is permission is granted, Read and Update access is granted by default.
SubFM	The user has been granted Sub-Functional Manager permission for this Series. If this is permission is granted, Read and Update access is granted by default.

Table 3. Series Permissions

b. TPFDD Permissions. Permissions assigned at the TPFDD level override any permission inherited from the series level. Table 4 lists the available TPFDD-level permissions available to a JOPES user.

TPFDD Permissions	
Permission	Description
Read	The user has read access to the TPFDD.
Update	The content of TPFDD may be changed.
PID	Permission granted to modify certain aspects of the TPFDD record using JET (title and comments) or TMT (title and C-Day).
sgComp	The Supporting Component validation date may be set for the ULNs within the TPFDD.
sgCCDR	The Supporting Combatant Commander validation date may be set for the ULNs within the TPFDD.
sdComp	The Supported Component validation date may be set for the ULNs within the TPFDD.
CCDR	The Supported Combatant Commander validation date may be set for the ULNs within the TPFDD.
USTC	The USTRANSCOM status flag may be set for the ULNs within the TPFDD.

Table 4. TPFDD Permissions

11. Access to JOPES Data. All users desiring access to JOPES data are required to obtain an individual JOPES user account. Non-GCCS-J applications will not be given direct access to the JOPES database. Non-JOPES applications will receive information via JOPES database views or an approved external system interface (B8/H3/TIES/JDNETS) only after interoperability testing and appropriate approval has been granted by Joint Staff J3. A GCCS-J user account request form must be submitted by the requestor detailing the type of access required. Current access request forms may be obtained from the local command or Service JOPES functional manager. Per this manual, the series FM will set the standards for granting access; it is highly encouraged that prior to creating an account, the user will provide completion certification of JOPES training.

12. Group/Joint Crisis Action Team (JCAT) Accounts. GCCS-J v 4.X will not utilize group/JCAT watch-team accounts in accordance with reference f. Each individual user that requires access to JOPES data is required to obtain and maintain an individual JOPES account. Re-use of existing accounts for new personnel is prohibited.

13. Access Authorization. The originator is the release authority for all JOPES documents and information. Unless the originator specifically restricts release, the information may be released by authorized holders to agencies (other Defense components, executive branch agencies, contractors, auditors, and Congress) not on original distribution provided the agencies have a valid need to know, hold the appropriate level of security clearance, and if the release is within any limitations contained in such documents. If the authorized holder is uncertain about the appropriateness of releasing the information to a specific requester, release approval should be requested from the originator. The supported commander, as delineated in the Joint Strategic Capabilities Plan, or other joint operation planning authority, is the release authority for all JOPES TPFDD files. Service component commands may release their own Service's information.

ENCLOSURE D

DATABASE ACCESS AND REPLICATION

1. Purpose. This enclosure establishes the responsibilities and assignments of functional managers and commands/Services to maintain accurate and synchronized data across all JOPES Strategic Server Enclaves (SSEs).

2. Responsibilities

a. Series Functional Manager responsibilities. The primary series-FM is the owner of each specific series of Operation Plans (OPLANs) at the combatant command, Services, and DOD agencies, as specified in reference d. As such, they are responsible for ensuring data accuracy across the JOPES SSEs. The system as developed has the capability to ensure accuracy across the OPLANs, but crosschecks are still required of series-FMs. Series-FMs have the JOPLOG auditing capability provided in the RQT application to review a history of TPFDD updates. Auditing questions on past updates not obtainable through RQT will be directed to the JSSC FM office.

b. JSSC Functional Manager responsibilities. JOPES v4.X provides improved synchronization over previous versions, although the potential for inaccurate or dissimilar data still exists. The JSSC FM Office will actively inspect for data conflicts and replication errors, and take appropriate actions to correct.

(1) Data Conflicts. Data conflicts occur when users at separate SSEs update the same item of data, such as the same requirement, within the time required for data replication to take place. The user with the latest update will overwrite and undo the changes entered by the first user. This can result in possibly inaccurate data at all SSEs. A daily data conflict report will be provided to the USTRANSCOM FM office.

(2) Replication Errors. The JSSC FM Office will inspect all TPFDDs that experience failed transactions at any SSEs. Critical TPFDDs identified by the Joint Staff J3 will be inspected daily for dissimilar data. The JSSC FM office will recover data as necessary to ensure TPFDD synchronization.

(3) JOPLOG Auditing. The JSSC will maintain a minimum of one year of auditing data online within the JOPES SSEs at all times. The JSSC FM office is responsible for addressing all auditing questions that cannot be determined through JOPLOG within the RQT application.

c. USTRANSCOM FM responsibilities. The USTRANSCOM FM Office, working in conjunction and as a partner with the JSSC FM Office for all data accuracy issues, will inspect all data conflicts for overwritten data and correct as appropriate. The JSSC FM Office will provide all required data and access to the USTRANSCOM FM Office to perform this function. Terminal and database SQL access is required by all USTRANSCOM FM accounts that perform this function.

3. Multi-Site and Single-Site Update. TPFDDs will be replicated across all FSSEs and assigned DSSEs through one of two mechanisms.

a. Multi-Site Update. The JSP will keep data updates flowing throughout the network in near real time (within 3 minutes). Users may update or view up-to-date information at any FSSE. This is the standard method of replication within JOPES.

b. Single-Site Update (SSU). This is a non-standard replication methodology by which a Combatant Commander may request from Joint Staff J3 the use of SSU. The SSU methodology invokes software-based policies that will only allow updates to TPFDD information at that series designated single-site master enclave. This includes USTRANSCOM-managed data. This currently can be implemented by TPFDD-series only, and not by individual TPFDD. A listing of all TPFDD-series in SSU will be maintained on the JSSC Service Desk Website; users will be notified upon any change to the SSU listing in the gccs.jopes.fm and the gccs.jopes.tech newsgroups.

4. External Interface Replication. External interfaces will procedurally operate IAW joint rules to the fullest extent possible regardless of replication mechanism (direct database connect, JSP, TIES, JDNETS/DEX, JSUB, B8, or H3). A list of all external systems, connection method, and assigned FSSE will be posted on the JSSC JOPES Web site.

a. An administrator of an external system using the B8 or H3 file replication mechanism will log in to the Web server supporting the enclave for the requisite TPFDD.

b. An external systems utilizing the JSP, JDNETS/DEX, JSUB, or TIES replication mechanism will be assigned to a primary Strategic Server Enclave in such a way as to provide the best overall system performance and synchronization to the maximum extent possible. JSP, JDNETS, and TIES replication settings will be directed and managed from the JSSC FM office. Any changes to JSP, JDNETS, or TIES replication settings will be communicated to the primary Help Desk of the requisite external interface (e.g., FORSCOM for DRRS-A). JDNETS DEX configurations specifying the format and content of the replicated data will be specified by the external system.

c. A direct connect external interface will automatically be tied to the FSSE and will adhere to all Joint user rules and requirements. Any changes to Joint databases will be communicated to the primary Help Desk of the requisite external interface (e.g.: GCCS-AF DCAPEs Help Desk for DCAPEs).

5. Request for Connection to a JOPES Enclave

a. External systems may officially request to connect to one or more JOPES enclaves through a Memorandum of Understanding available on the JSSC JOPES Web site under 'Operations'.

b. For connection consideration, an external system must have successfully completed a Joint Interoperability Test Command interoperability test connected to the operational version of JOPES and possess a Global Authority to Operate.

c. Final approval to connect an external system to a JOPES enclave will be made by the JS J36 CSOD. Enclave assignment will be chosen IAW paragraph 5.b. above.

6. User Load-Balancing

a. Application Server Load Balancing. Each FSSE contains two application servers (ss#a1, ss#a2). There is no automated load balancing within JOPES IT. It is incumbent on the user to choose the best performing application server at that time. Web-based tools on the JSSC JOPES Website (listed under 'Tools') display the number of users currently on each application server, allowing the FM or user to make an informed choice.

b. Enclave Load Balancing. In the event of a FSSE experiencing abnormally increased loads as compared to the other FSSEs, The JSSC will post newsgroup messages to the gccs.jopes.fm newsgroup recommending users to move to its secondary or tertiary enclave as defined in Table 5 below.

7. Series Enclave Assignment. Table 5 identifies Series assignments – primary, secondary, and tertiary server assignments specifically.

Series Primary and Alternate Server Assignment			
Series	Primary Enclave	Alternate Enclave	Tertiary Enclave
0000-0599/JCS	JOPESNCR	JOPESTL	JOPESEUR
0600-0699/HQ USA	JOPESNCR	JOPESTL	JOPESEUR
0700-0799/HQ USN	JOPESNCR	JOPESTL	JOPESEUR
0800-0899/HQ USAF	JOPESNCR	JOPESTL	JOPESEUR
0900-0999/HQ USMC	JOPESNCR	JOPESTL	JOPESEUR
1000-1999/USCENTCOM	JOPESTL	JOPESNCR	JOPESEUR
2000-2999/AFRICOM	JOPESEUR	JOPESNCR	JOPEPAC
3000-3399/NORAD	JOPESTL	JOPEPAC	JOPESNCR
3400-3999/USNORTHCOM	JOPESTL	JOPEPAC	JOPESNCR
4000-4999/USEUCOM	JOPESEUR	JOPESNCR	JOPESTL
5000-5999/USPACOM	JOPEPAC	JOPESNCR	JOPESTL
6000-6999/USSOUTHCOM	JOPESNCR	JOPESTL	JOPESEUR
7000-7999/USSOCOM	JOPESNCR	JOPESEUR	JOPESTL
8000-8999/USSTRATCOM	JOPESTL	JOPESEUR	JOPESNCR
9000-9599/USTRANSCOM	JOPESTL	JOPESEUR	JOPESNCR
9600-9699/RESERVED	JOPESNCR	JOPESTL	JOPESEUR
9700-9999/USCG	JOPESNCR	JOPESTL	JOPESEUR

Table 5. Series Primary and Alternate Server Assignment

8. Command Enclave Assignment. Table 6 provides a list of Primary and Alternate sites for accessing JOPESE. The JSSC Service Desk will provide to the gccs.jopes.fm newsgroup notification and direction of which FSSE to access when a FSSE experiences a processing slowdown or a sharply increased level of activity.

a. Commands are distributed between enclaves in such a way as to balance user load between FSSE's throughout the planning cycle day to the maximum extent possible.

b. If JOPES IT functionality is not available on the assigned application server, the affected Command users will use the other application server within the assigned enclave for the missing functionality.

Command Primary and Alternate Enclave Assignment			
Command	Primary Enclave	Alternate Enclave	Tertiary Enclave
ACC	JOESNCR	JOESSTL	JOPESEUR
AFMC	JOESSTL	JOESNCR	JOESPAC
AFRICOM	JOPESEUR	JOESNCR	JOESPAC
AMC	JOESSTL	JOESNCR	JOESPAC
ARCENT	JOESSTL	JOESNCR	JOPESEUR
AREUR	JOPESEUR	JOESNCR	JOESSTL
CENTAF	JOESSTL	JOESNCR	JOPESEUR
CENTCOM	JOESSTL	JOESNCR	JOPESEUR
CNO	JOESNCR	JOESSTL	JOPESEUR
COMMANDANT, USCG	JOESNCR	JOESSTL	JOPESEUR
EUCOM	JOPESEUR	JOESSTL	JOESNCR
FORSCOM	JOESNCR	JOESSTL	JOPESEUR
HQ USAF	JOESNCR	JOESSTL	JOPESEUR
HQDA	JOESNCR	JOPESEUR	JOESSTL
HQUSMC	JOESNCR	JOESSTL	JOPESEUR
JOINT STAFF	JOESNCR	JOPESEUR	JOESSTL
LANTFLT	JOESNCR	JOESSTL	JOPESEUR
MARFORCENT	JOESPAC	JOESNCR	JOESSTL
MARFORCOM	JOESNCR	JOESSTL	JOPESEUR
MSC	JOESSTL	JOPESEUR	JOESNCR
NAVCENT-F	JOESSTL	JOESNCR	JOPESEUR
NAVCENT-R	JOESSTL	JOESNCR	JOPESEUR
NAVEUR	JOPESEUR	JOESNCR	JOESSTL
NMCC	JOESNCR	JOESSTL	JOPESEUR
NORTHCOM	JOESSTL	JOESPAC	JOESNCR
OSF-DISA	JOESNCR	JOESSTL	JOPESEUR
PACOM	JOESPAC	JOESNCR	JOESSTL
SDDC	JOESSTL	JOPESEUR	JOESNCR
SOCOM	JOESNCR	JOPESEUR	JOESPAC
SOC PAC	JOESPAC	JOESSTL	JOESNCR
SOUTHCOM	JOESNCR	JOESSTL	JOPESEUR
STRATCOM	JOESNCR	JOESPAC	JOESSTL
USAFE	JOPESEUR	JOESSTL	JOESNCR
USTRANSCOM	JOESSTL	JOPESEUR	JOESNCR

Table 6. Command Primary and Alternate Enclave Assignment

9. Daily Database Maintenance. The JSSC reserves the right to perform scheduled maintenance within a 2-hour window during each enclave's local non-business hours. During this time effected commands will be requested to

CJCSM 3122.05
15 December 2011

use their alternate enclave. The daily database maintenance window for all enclaves will be posted on the JSSC JOPES Website under 'Operations.'

(INTENTIONALLY BLANK)

ENCLOSURE E

TPFDD MANAGEMENT

1. General. JOPES IT provides the ability to rapidly disseminate information globally among the JOPES Strategic Servers. Due to this enhanced capability, guidelines have been developed to ensure that TPFDD loading, deleting and copying does not affect processing of priority requirements. External applications rely on a variety of interfaces to transfer data. These interfaces (JDNETS, TIES, TMT) may cause impact to system responsiveness and are bound by the same requirements. In the event system performance degrades, newsgroup notification will be made in accordance with established procedures for JPEC notification.

2. Upload and Deletion Notification. All large network TPFDD uploads and deletions should be scheduled with the JSSC Service Desk in accordance with the thresholds below. The threshold definition is defined by the total number of requirements (Unit Line Number/Cargo Increment Number/Personnel Increment number (ULN/CIN/PIN)) that are contained in the upload or deletion. Once the total is calculated apply the following rules:
 - a. Total less than 5,000: Proceed with actions, no notification is needed.

 - b. Total between 5,000 and 10,000: Notify the JSSC Service Desk via gccs.jopes.fm newsgroup message and telephone of intention and schedule. Scheduled time for load or deletion should be at least 1 hour after newsgroup notification. No response from the JSSC Service Desk indicates concurrence.

 - c. Total greater than 10,000: Schedule with the JSSC Service Desk via gccs.jopes.fm newsgroup message. Include in the message the estimated total number of requirements in the upload or deletion and desired timeframe to start. Factors considered in scheduling include, but are not limited to: network load, priority of the TPFDD, and enclave load availability. The goal of scheduling TPFDDs is to start the loading within 24 hours of notification.

3. Precedence and Prioritization. Real-world contingency plans supporting a national security crisis take the highest precedence for TPFDD loads and mass updates at all times. The Joint Staff J3 will determine the precedence and prioritization when the operational situation requires. In the event a database is in the process of deleting or loading a lesser priority TPFDD, the crisis TPFDD for the primary server will take precedence during the synchronization of databases.

a. Planning Conferences. TPFDD loads during scheduled planning conferences can receive a dedicated channel to distribute data. This dedicated channel will not impact real-world network operations. If system data prioritization must occur, the JS J3 will determine priority of planning conference data within the overall hierarchy of operational requirements.

b. Prioritizing TPFDDs by JSP. Daily processing of transactions require no prioritization of TPFDDs. If required, TPFDDs can be prioritized either by Series, by subset, or by specific identifier. JSP has two methods to affect the rate of TPFDD processing. For both, non-TPFDD data is considered high-priority. For example, user creation transactions are non-TPFDD, and would be part of the high-priority processing. Each strategic server site can have a specific, individual TPFDD priority set.

(1) Dedicated Processors. A maximum of 16 processors can be activated simultaneously to process incoming transactions. Up to four processors can be reserved as dedicated, up to two reserved for incoming transactions from JDNETS-based external systems, and the other remaining processors available for normal TPFDD processing. Dedicated processing can accommodate both background and critical TPFDD processing requirements. Assignment of a TPFDD to a dedicated transaction processor eliminates the delay of sequentially processing all other transactions, and allows dedicated TPFDD transactions to be processed soon after they are loaded into the queue. There may be a greater demand for system resources as additional processors are assigned. Processing management for non-dedicated TPFDDs is set by the system.

(2) Transaction File Prioritization. All incoming transaction files are separated into high- and low-priority transactions. All transactions containing high priority TPFDDs and non-TPFDD data will be loaded for processing before any waiting low priority transactions. A maximum of six TPFDD criteria may be set for prioritization.

c. How Priorities are established. TPFDD load priorities will be based on Combatant Commander requirements. Non-TPFDD transactions will have the highest priority over TPFDD transactions to maintain user capability in the event of a crisis in each unified command theater.

4. TPFDD Backup and Restore. Combatant Commanders desiring to backup a TPFDD may use one of the following options.

c. B8/H3 Offloads through TMT. An individual user with access to TMT may create a B8 (no transportation data) or an H3 (includes associated transportation data) and store according to local directions for later use. B8 and H3 flat files are GCCS 3.X and earlier formats and do not fully capture JOPES v4.X data elements and values. Their use is not recommended.

c. JSP Bulk Dump through TMT. The TMT allows a FM the ability to offload or upload JSP “Bulk Dump” files in the DEX format for OPLAN backup and recovery. The user has the option to download force or force and carrier data. A JSP Bulk Dump file is an exact backup in the JOPES v4.X format.

c. TPFDD Copy through JET. Users may initiate a TPFDD copy (no transportation data) IAW the procedures and limitations described in paragraph 2. above. TPFDD copies do not initialize new plans, which must be performed prior to a TPFDD copy in TMT.

c. Scheduled TPFDD Backups. The JSSC FM office will perform weekly backups of all TPFDD’s. Upon request of the series-FM, these backups can be reloaded when needed. TPFDD backups will be maintained for a minimum of 1 month. Daily backups can be performed on TPFDD’s deemed necessary by request of the series-FM with concurrence of the Joint Staff J3. The daily and weekly backup schedule will be posted on the JSSC JOPES Website.

(INTENTIONALLY BLANK)

ENCLOSURE F

STRATEGIC SERVER OPERATIONS AND MANAGEMENT

1. Introduction. This enclosure discusses JOPES v4.X Strategic Server Management and details the policies and procedures for the JSSC to effectively control the global JOPES strategic server enclaves as a single virtual data source. This will be accomplished through active monitoring of the systems performance, directing and/or performing remote system and site corrective and optimization actions and effective configuration management. Specifically, how the JSSC, in coordination with other DISA directorates, the Joint Staff, and the SSE host sites, will centrally manage the JOPES v4.X FSSE and the DSSE.

2. Background. The JOPES v4.X architecture addresses data replication and dissemination problems by providing an updated infrastructure combined with end-to-end management capabilities that will enable real-time management. The GCCS-J v 4.X JOPES system carries a deployable capability that's based on established deployment criteria, and provides deployed Combatant Commanders and joint task forces a DSSE in-theater.

3. Continuity of Operations. Continuity of operations is assured within the overall architecture of the JOPES system. If any single enclave is unavailable, the remaining enclaves in the system will handle the resulting traffic volume. All JOPES users and TPFDDs exist at all FSSEs. The JSSC is responsible for maintaining its Continuity of Operations Plan (COOP) and exercising that plan periodically. The JSSC management configuration has full capabilities at the COOP location.

a. Database Backup and Recovery. Backup and recovery of the JOPES v4.X databases will be centrally managed and controlled from the JSSC. Daily routine backups will be scheduled at times outside the local work hours of the site hosting the server in question. In order to minimize the adverse impact on database accessibility, backup schedules will be published in the gccs.jopes.tech newsgroup. Outages resulting from a database backup will be reported in the gccs.jopes.outage newsgroup. Accessibility and outage information will also be made available in the gccs.jopes.fm newsgroup.

(1) Database Backup. An open database backup of each Strategic Server site database will be performed daily. During the daily backup, the database will remain open and accessible to users. The daily backup will be scheduled outside the local work hours to minimize any adverse impact of the backup on system performance. A closed database backup of a Strategic Server will be conducted as necessary. When performed, such backup will

normally be scheduled to occur on only one SSE site at a time and outside of normal local work hours. During a closed database backup, the database at that site will not be accessible to users. Notice will be posted in the [gccs.jopes.outage](#) and [gccs.jopes.fm](#) newsgroups in advance of any closed backup. Users may connect to the JOPEs v4.X database at another SSE site to continue working. System administrators at sites hosting SSE equipment will be tasked to change magnetic tapes as required. Archive tapes will be placed in the host site's offsite storage facility and held in accordance with current JOPEs v4.X backup and recovery guidelines.

(2) Database Recovery. JSSC Service Desk Database Managers will report JOPEs 4.X database site outages in the [gccs.jopes.outage](#) and [gccs.jopes.fm](#) newsgroups. When recovery is complete and the database is accessible, users will be notified in the [gccs.jopes.fm](#) newsgroup. The JSSC will be responsible for the periodic backing up to tape of the SSE database servers. Normal (open and closed) backups of JOPEs v4.X databases will be maintained on both disk and on magnetic tape. Backups will be maintained on magnetic tape for a minimum of 2 weeks; only the most recent database backup will be maintained on disk. The tapes used for storing backups will be used in a circular fashion: once the entire set has been used, they will be overwritten starting with the oldest tape. Any direct connect external interface will receive direct communication from the JSSC Service Desk to the primary help desk of the requisite external interface (e.g., GCCS-AF DCAPEs Help Desk for DCAPEs).

b. Network Information System Plus (NIS+) Promotion. Under normal circumstances, the master database will remain the same. In any event requiring a different enclave to be stood up as the NIS+ master, newsgroup messages will be posted in the [gccs.jopes.outage](#) and [gccs.jopes.fm](#) newsgroups. During this time, functional managers must refrain from adding or editing user accounts. Newsgroup messages will be posted when account maintenance actions are once again allowed.

4. Management Hierarchy. The Operational Management structure for JOPEs Strategic Servers will be under the NetOps concept. The JSSC and its operational constituents fall under the Global Information Grid Operations directorate of DISA (DISA/GO). Operational Control will ultimately reside within the NetOps construct known as the Global NetOps Center (GNC).

5. Roles and Responsibilities

a. Joint Staff

(1) The Command Systems Operations Division (J3/DDC2NO/CSOD) within the Joint Staff provides guidance and operational direction for the day-

to-day operational activity throughout JOPES. The Joint Staff JOPES Program Manager functions as the lead for all series-FMs functioning within the JPEC.

b. Defense Information Systems Agency

(1) DISA/JSSC. The JSSC will provide centralized management of the GCCS-J v 4.X JOPES SSEs. This will enable 24x7 support on strategic servers, to include installation, optimization, upgrades, repairs, and on-site deployment of DSSEs. Funding for deployments will be covered by the requesting Combatant Commander/JTF or operation supported. Additionally, JSSC will be responsible for providing operating and management status to the OPS Directorate, the Joint Staff, and the DISA Global Network Operations and Security Center (GNOSC) in accordance with NetOps Concepts. JSSC will provide input to and execute the life-cycle management plan for the GCCS-J v 4.X JOPES SSE. Finally, the JSSC will act as chair for the Global Management Center (GMC) Configuration Control Board (CCB).

(2) DISA/GCCS-J PMO. The GCCS-J PMO manages the continued development and sustainment of the JOPES mission application within the overall context of the GCCS-J program. Additionally, GCCS-J PMO will be responsible for funding the following:

(a) Life-cycle management of the JOPES SSEs. With input from JSSC, GCCS-J PMO will develop the life-cycle management plan for the GCCS-J v 4.X JOPES Fixed and DSSEs.

(b) Hardware/software replacement as required by the JOPES Life-Cycle Management Plan, to include the necessary toolsets to provide end-to-end System and Network Management (S&NM) and Information Dissemination Management (IDM).

(c) Oracle Platinum-level service agreements or equivalent third party service level agreements for the server suites and replacement parts for the premise/filter routers as required

(3) DISA/GO/GNOSC/Regional Network Operations and Security Center/SIPRNET Monitoring Center (SMC). The SMC will provide end-to-end SIPRNET situational awareness to the JSSC Service Desk as required by current operational directives. Further, the SMC, through the SIPRNET Network Operations Center (SIPRNOC), will work with other regional Network Operations Centers (NOCs) to obtain Wide Area Network (WAN) status and provide the JSSC Service Desk with operational awareness of network issues affecting JOPES Operations.

(4) DISA/Network Services (NS)52. NS52 will allow the JSSC Service Desk direct access to their monitoring software toolset. This enables the JSSC to complete the end-to-end management piece as required by NetOps concepts.

c. Strategic Server Enclave Host Site. Each SSE Host Site will assist in system management by providing touch labor at the enclave as defined in applicable memorandum of agreement (MOA) between DISA/JSSC and the host site. Personnel will have appropriate equipment and administrator skills to perform touch labor functions. Additionally, each enclave will provide escorts to any technician or installation team visiting the site to institute changes or repairs to the enclaves. This support may be provided by the DISA element located at each site currently based on agreements between the DISA element and the host site support unit.

d. Primary Series Functional Manager. The Primary Series-FM is the owner of specific series of OPLANs at Combatant Commanders, Services, and DOD agencies as specified in reference d. The Primary Series-FM will assist in the system management by resolving user data access issues, including account and TPFDD management.

6. JSSC Management Process

a. Management of the GCCS-J v 4.X JOPEs network requires close coordination between the JSSC Service Desk, the GNOSC as part of the GNC, and the global SIPRNET NOCs as part of the various Theatre NetOps Centers. This synergy will be achieved through the support of the SMC, the JSSC Service Desk, and the GNOSC. JSSC Service Desk personnel who manage the devices attached to the JOPEs v4.X enclaves provide application, system, and database administration support. SMC personnel will manage the overall network connectivity, to include management of the premise/filter routers on behalf of the JSSC Service Desk, between each enclave and the user community.

b. Strategic Server Management is composed of two main areas: system management and administrative management. System management will be accomplished both locally and remotely with database management and automated toolsets to ensure a collaborative, integrated, and seamless end-to-end “horizontal fusion of information.” Administrative management is composed of five general functions required to keep system hardware and software current and to maintain efficient system performance. These areas are:

(1) Enforcing the system standards, KPPs, and policy directives through effective configuration management.

(2) Providing increased system-wide performance visibility.

(3) Coordinating the local security certification and accreditation.

(4) Providing funding for both life cycle replacement of strategic server site hardware and software and the travel and training requirements to keep the system mission-effective.

(5) Managing and delegating system access.

c. These management processes will enable real-time Fault, Configuration, Accounting, Performance and Security (FCAPS) status management on 24x7 basis. This will be accomplished through performance data gathering, correlating system information, repairing or optimizing the system, performing asset inventories, installing and maintaining hardware, and providing help desk support. Management and monitoring tools allow operations support personnel to operate in a proactive mode, providing awareness of application, performance, and capacity problems before applications are adversely affected. This application service management is composed of two main areas: one of proactive system management and the other of administrative management. Proactive system management encompasses the day-to-day mission and responsibilities of ensuring the best class of service possible to the warfighting customer. Administrative management encompasses the various critical support activities necessary to ensure smooth continuing operation free of extraneous network, application, and support problems. System Management and Administrative Management are essential contributions to ensure JOPES performance parameters (as documented in Enclosure I) are met.

JOPES v4.X Strategic Server Enclave
JSSC Management Process

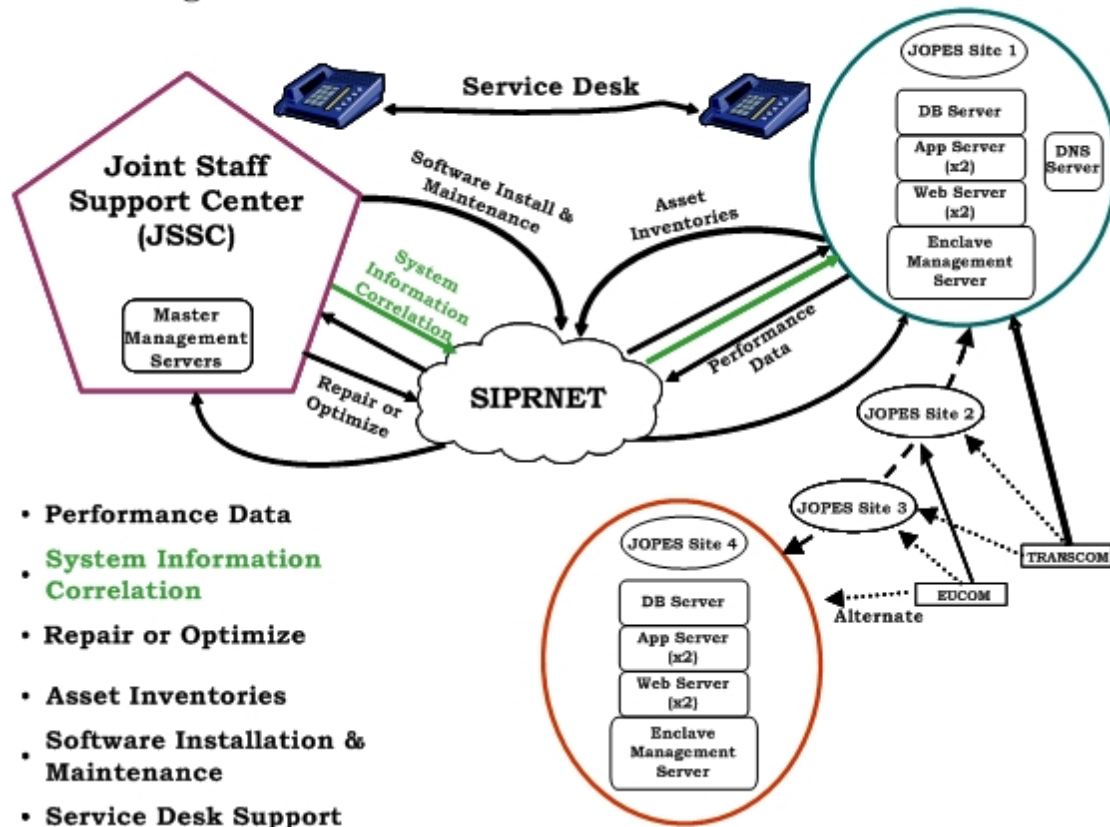


Figure 6. Notional JSSC Management Process

d. System Management. Within system management are found all the day-to-day analysis and management undertaken to ensure FCAPS is met on a 24x7 basis. Using automated network management tools and internal processes and procedures, the JSSC manages the SSEs through six distinct parallel and recurring steps: gather performance data, correlate system information, repair and optimization, perform asset inventory, install and maintain software, and help desk support. The net result is an end-to-end, comprehensive S&NM and IDM process (refer to Figure 6).

(1) Performance Data. On a continuous basis, JSSC Service Desk will remotely monitor architecture performance, to include:

- (a) Application/process performance/status.
- (b) Hardware performance.
- (c) Network performance.

(2) System Information Correlation. Using the enterprise management tools and centrally generated scripts, the JSSC Service Desk will:

(a) Conduct event correlation as appropriate and disseminate, as required, correlated and evaluated system/site health and status information.

(b) Monitor and maintain database performance, database operations, and data synchronization of JOPEs 4.X FSSEs and DSSE databases.

(c) Compile performance statistics for the SSEs.

(d) Make available to the community daily, weekly, and monthly reports, as required. These reports will include, but are not limited to, network traffic loads, throughput, site outages, network congestion, etc. The JSSC Service Desk will use the reports to modify and enhance the network accordingly.

(e) Provide each host site with a monthly report on the performance of the host site as seen from the JSSC. The JSSC Service Desk will use this report to ensure system operation meets and maintains the level of performance required by the KPPs.

(f) Maintain historical data on network performance and utilization.

(g) Publish an annual report analyzing past versus present performance.

(h) Provide “real-time” system performance status through a combination of application, hardware, and network monitoring.

(i) Ensure this information is available to all stakeholders and briefed to the GNOSC as part of the GNC in accordance with GNOSC defined reporting criteria. SSE Host Sites will review host site monthly performance reports for information on required actions to improve host site performance

(3) System Repair or Optimization

(a) DISA/JSSC

1. Proactively initiate corrective actions.

2. Institute performance optimization. This may include:

a. System reboots.

b. Database startup, shutdown, monitoring, maintenance, replication, and synchronization.

c. Monitor and troubleshoot database and network problems.

d. Perform system and database backups.

(b) DISA/SMC

1. **Proactively** and upon request from the JSSC Service Desk, implement corrective actions to the network. This may include:

a. Router reboots.

b. Crypto reboots.

2. Monitor and troubleshoot WAN network performance problems.

3. Perform router maintenance IAW the router maintenance policy.

(c) GCCS-J PMO

1. Address corrective actions or work-arounds for applications.

2. Develop performance optimization methods for incorporation in to the operational network.

(d) SSE Host Sites. Execute existing MOA between supporting organizations and JSSC. Each MOA defines the touch labor required by the SSE host site. Examples of touch labor requirements include:

1. Conduct power-up, emergency power-down, and hardware reboot procedures.

2. Conduct telephone coordination with the JSSC Service Desk to execute system fault isolation, to include any problems arising from remote system reboots.

3. Perform system tape back-up and restore procedures.

4. Perform basic operating system commands as directed .

5. Escort contract maintenance representatives during fault or failure analysis and repair actions.

6. Provide on-site system administration 7-days a week, 24-hours a day.

(4) Asset Inventories. DISA/JSSC/Global Configuration Management maintain a system-wide and a site-specific inventory of hardware (to include the premise/filter routers, the database servers, the Web servers, the master and enclave management servers, and any other pertinent equipment) and software (to include software licensing, Network components, to include IP addresses).

(5) Software Installation and Maintenance

(a) DISA/JSSC. Performs software installation/upgrades (which includes application of Information Assurance and Vulnerability Assessments (IAVAs) and software patches) as provided by the GCCS-J PMO. JSSC personnel will coordinate hardware and/or software changes requiring hands-on assistance as far in advance as possible. Users will be notified of these changes, and possible impact to their access via appropriate newsgroup messages, Web pages, and other means of communication. Coordinate upgrades directly with DISA/SMC for premise/filter router installation.

(b) DISA/GCCS-J PMO. Provide DISA/JSSC with access to Program Office's software testing prior to software release. This will support the development of load procedures and preparation for executing JSSC Service Desk help desk after software release.

(c) DISA/SMC. Perform router Integrated Operating System (IOS) upgrades as required and ensure latest routing protocols are optimized for JOPES use. Coordinate premise/filter router initial installation and upgrades directly with the JSSC.

(d) DISA/NS52. Perform extensive testing of premise/filter Router IOSs for vulnerabilities and performance issues. Deliver new IOS versions for installation by the SMC. Test Network routing protocol architecture before implementation across the network.

(6) Help Desk Support. Help desk support is handled by the same process used for previous versions of GCCS-J as outlined in reference E.

(a) Local User Site

1. Provide Level I help desk support in accordance with local procedures.

2. Receive initial calls from users.

3. Ensure the GCCS Site Coordinator is aware of any site problems and resolution actions.

(b) Primary series-FM

1. Provide initial resolution actions on user data access issues.

2. Refers unresolved data access issues to the JSSC Service Desk.

(c) DISA/JSSC Service Desk

1. Provide 24/7, Level II help desk support to resolve problems, via phone, e-mail, Web, or newsgroups.

2. Facilitate problem resolution to application developers and transport layer providers.

3. Provide online “lessons learned” information.

(d) GCCS-J PMO

1. Provide Level III developer support in accordance with current procedures.

2. Initiate the Global System Problem Report process for any Problem Reports that cannot be resolved quickly and easily.

e. Administrative Management. Provides a foundation for an operational 24X7 system. The various components that make this possible are dependent on the decisions made in Administrative Management.

(1) Configuration Management. All SSEs will adhere to standard configuration management rules as defined in reference E. DISA will provide the configuration management functions to collect and provide data on JOPES for status, accounting, and auditing purposes. Configuration management duties include:

(a) Maintain network configuration

(b) Maintain system hardware configuration

(c) Maintain system software configuration

(d) Maintain naming and addressing

(e) Maintain inventory control

(2) GCCS-J Configuration Management Board performs configuration control management of strategic servers, to include the JOPES Web server, application server, and database server. These servers will consist of only authorized baseline software and will have no site-unique software. Any necessary changes to JOPES strategic server configuration should be addressed through the established process using the NET-Enabled Requirements Database (NRID).

(3) GMC CCB will charter and implement a CCB to ensure standard configurations outside of the GCCS-J baseline are met on all management systems supporting JOPES strategic servers. The GMC CCB will perform the following functions.

(a) Monitor and enforce configuration management, security certification, and accreditation management as designated by the GCCS Management Board.

(b) Responsible for the current management system configuration; executes Configuration Status Accounting to ensure integrity.

(c) Maintain a software configuration inventory for operational support applications (network management, problem report, and directory services), management support applications (modeling tools, data analysis tools), and associated databases.

(d) Maintain a list of names and addresses of various points of contact, trouble reports, performance reports, change management logs, and network topologies.

(e) Monitor JOPES Strategic Server sites to ensure management devices maintain baseline configurations.

(f) Addresses emergency actions necessary to support global management architecture (IAVAs, urgent upgrades/patches, network issues).

(g) Specific CM policies and procedures can be found in reference E.

f. Account Management

(1) DISA/JSSC Service Desk will manage and control primary series-FM Accounts at each of the owning organizations as specified in reference D.

(2) The Primary Series-FM

(a) Manage series-FM accounts, subordinate FM accounts, and all other user accounts controlled by that primary series-FM.

(b) Each primary series-FM or designated representative will coordinate their specific user access requests with the respective primary series-FMs or designated representatives in accordance with procedures established by the JPEC (currently by posting messages in the gccs.jopes.fm.newsgroup.)

7. Security Certification and Accreditation. All SSEs (both fixed and deployable) will be split in two for certification and accreditation purposes. The baseline (database, application, Web servers) equipment and SIPRNET connectivity (tie circuits from SIPRNET point of presence at each host site) will fall under GCCS-J program management control while the Management Gateway architecture will fall under the Strategic Server Management policy.

a. USSTRATCOM, as the Designated Accreditation Authority, will perform type accreditation of the database, applications, and Web servers and circuit accreditation.

b. The Defense Intelligence Agency will perform type certification of the database, application, and Web servers.

c. DISA/GO will perform accreditation on the management servers.

d. DISA Field Security Office will perform certification on the management servers.

8. Life Cycle Funding

a. DISA/GCCS-J PMO. The GCCS-J PMO will provide initial funding for installation of hardware and software at each site. In coordination with the JSSC, the GCCS-J PMO will develop a life-cycle management plan in support of the JOPES v4.X SSEs. The GCCS-J PMO will also provide funding for the developed life cycle management plan.

b. DISA/JSSC. The JSSC, in coordination with GCCS-J PMO, will develop the life-cycle management plan in support of the JOPES v4.X SSEs. The JSSC will also execute the developed life-cycle management plan.

9. Outage Management. Outage management falls under administrative and proactive system management but for the purposes of this document we have combined the outage management process into one heading. The JSSC Service

Desk will be responsible for receiving information from the SSE host site, compiling, writing, and forwarding the reports to designated Joint Staff elements. All reports and notifications will be in accordance with Enclosure H.

a. SSE Outages. Scheduled JOPES SSE outages will be performed during the daily maintenance window for that enclave when practical. For all other scheduled outages, the final decision will be a coordinated effort between the Joint Staff J36/DDC2NO/CSOD and the JSSC. JSSC will notify all affected SSE users at least 48 hours in advance of any necessary server outages via newsgroup message. Any direct connect external interface will receive direct communication from the JSSC Service Desk to the primary Help Desk of the requisite external interface (e.g., GCCS-AF DCAPEs Help Desk for DCAPEs). Notification procedures and timelines are listed below.

b. SSE Host Sites Responsibilities

(1) Notify the JSSC Service Desk of all scheduled outages at least 96 hours in advance. This encompasses all situations involving the physical condition of the facility housing or infrastructure supporting the strategic server enclave.

(2) Notify the JSSC Service Desk ASAP for any unscheduled outages. Notification must occur no later than 10 minutes after outage initiation.

(3) Provide the following information via secure e-mail or secure voice when coordinating a scheduled outage or reporting an unscheduled outage:

(a) Reason for Outage - Explanation of the problem.

(b) Status of Actions - Explanation of what actions are being taken to resolve the problem.

(c) Estimated Time to Restore Service - Best estimation of how long the outage will last.

(d) Corrective Action (as necessary) - Final closeout status report with corrective actions and time service was restored.

c. DISA/JSSC Service Desk Responsibilities

(1) Scheduled outages

(a) Coordinate outage with the Joint Staff J36/DDC2NO/CSOD and strategic server users no later than 96 hours in advance. Any direct connect external interface will receive direct communication from the JSSC Service

Desk to the primary Help Desk of the requisite external interface (e.g., GCCS-AF Help Desk for DCAPEs).

(b) The JSSC Service Desk will provide the following information via email to the Joint Staff J36/DDC2NO/CSOD and appropriate agencies when requesting approval for a scheduled outage.

1. Reason for the outage.
2. Status of the actions being taken to resolve the problem.
3. Estimated time to restore services.
4. Corrective action (final closeout report with corrective actions and time service was restored).

(c) Notify the JPEC of all approved scheduled outages at least 48 hours in advance. Notification will be distributed via newsgroup, subscriber service, and other communications media as available.

(2) Unscheduled outages

(a) Notify the JPEC within 15 minutes of outage detection (per Table 7) and the Joint Staff J3 PMO as soon as practical of any unscheduled outage via newsgroups. Notification through other communications media will follow as soon as practical. Any direct connect external interface will receive direct communication from the JSSC Service Desk to the primary help desk of the requisite external interface (e.g., GCCS-AF Help Desk for DCAPEs).

(b) Provide the following information via newsgroup to the JPEC when reporting an outage.

1. Reason for the outage.
2. Status of the actions being taken to resolve the problem.
3. Estimated time to restore services.
4. Corrective action (final closeout report with corrective actions and time service was restored).

10. Proactive and Administrative Management. Enabled though a platform independent setup. Toolsets comprise Enterprise Management, Network and Performance Management, and Database Fault Management functional areas and, in turn, make the aforementioned Proactive and Administrative Management processes possible.

JOPES v4.X Strategic Server Enclave Enclave Management Process

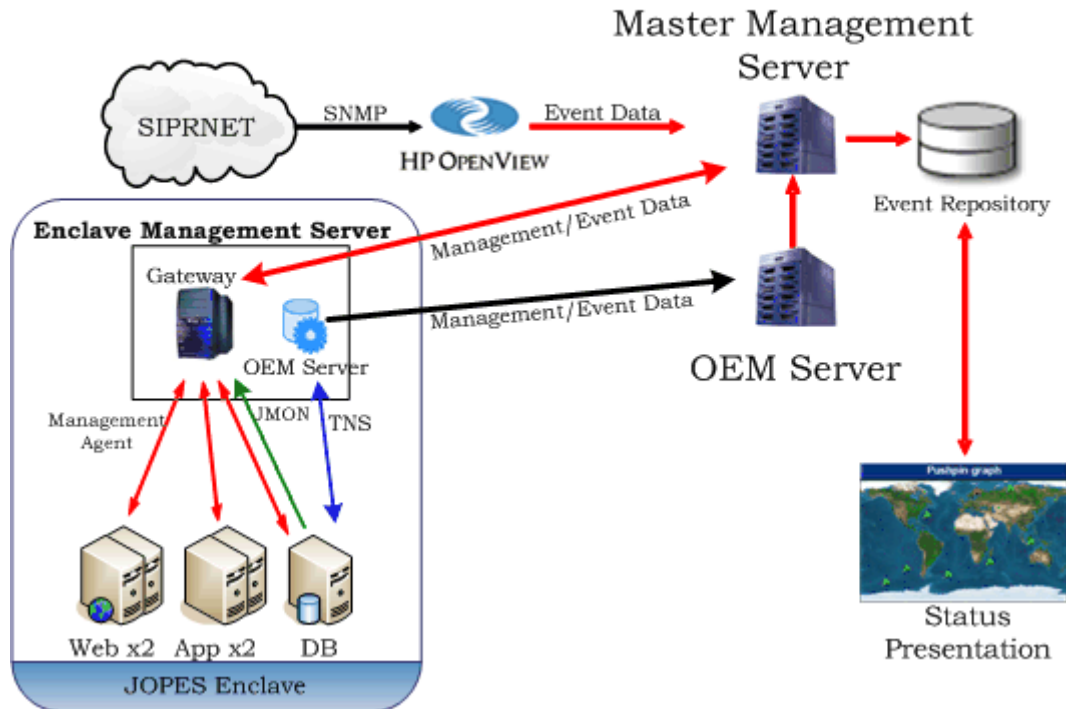


Figure 7. Strategic Server Enclave Management Process

a. Enterprise Management. The Strategic Server Management structure is based on a variety of COTS and government off-the-shelf (GOTS) tools that will provide a complete picture of the overall health of the system and network components at each enclave. These tools will also provide centralized management capabilities for the systems, databases, and network. Management capabilities include, but are not limited to, systems and database monitoring, software installation, hardware/software inventory, event correlation, network monitoring, and task automation. Figure 7 depicts the SSE Management Process.

(1) The management tool(s) used will provide a foundation and infrastructure for facilitating the proactive and administrative management. Any software including intelligent agent(s) that needs to be loaded on the strategic servers must be packaged in accordance with established GCCS-J v 4.X processes.

(2) The monitoring tools will provide a collection of monitors for checking a variety of hardware, system, database, and network resources. Monitors will be configured to run at specific intervals and will forward events

to a centralized management console when predefined thresholds have been met. These tools will automate a vast majority of the system checks on the strategic servers.

(3) The centralized management console will receive, process, and correlate events from the aforementioned monitoring tools. It will also provide customized “views” of the event data based on administrator and end user requirements. Events from Oracle Enterprise Manager (OEM) and the JOPES Monitoring (JMON) tool will be forwarded to the centralized management console to provide a complete picture on the overall health/status of each enclave. This console will also have the capability to initiate corrective action based on the events received. It will play a major role in the pro-active monitoring of the servers and network and will be the single place to view events from all monitoring sources.

(4) Software installation tools will provide the ability to centrally manage the loading of new software/packages on the strategic servers. These tools will have the ability to automatically load new software/packages on the server or simply push raw packages to the servers.

(5) Inventory tools will facilitate the collection and retrieval of hardware and software inventories on the strategic servers. It will automatically collect detailed hardware, software, and package information about each managed server. All this data is stored in a database for easy retrieval and report generation. This is a key component in the configuration management of the strategic servers.

(6) The central management console and repository are currently based on the Tivoli application. The Tivoli Event Console is the primary fusion agent for all management data. Data is provided to users in a hierarchical fashion using views incorporating specific subsets of overall data pulled back for management purposes.

b. System, Application, and Network Management. The JSSC Service Desk is the center of all S&NM activities for the GCCS-J v 4.X JOPES. In this capacity, two of the critical functions performed by the JSSC Service Desk are the monitoring of the JOPES 4.X databases and the collection of performance data. The SMC/SIPRNOG will provide monitoring capabilities of the WANs and communications infrastructure to the SSE to detect, isolate, and when possible correct JOPES 4.0 network related problems.

(1) System Performance Management. The JSSC Service Desk uses COTS tools to monitor all critical system performance metrics of the server enclaves, e.g. critical hardware, critical processes, and physical system parameters.

(2) Application Performance Management. The JSSC Service Desk uses JMON and the FM-view to monitor all JOPES strategic servers. JMON provides near real-time status of the servers, critical processes, and replication of JOPES data. Monitoring tools are available on the JSSC JOPES Website.

(3) Database Fault Management. The intent of fault management is to detect, log, notify users, and to the extent possible; automatically fix database problems in order to ensure maximum operation. Fault management involves determining the symptoms and then isolating the root cause. Once the problem is fixed, and the solution successfully tested, the methods of detection and resolution of the problem are recorded. The JSSC Service Desk uses a variety of software tools to provide these database fault management components. Each of these software products provides the required detection, event recording, and repair.

(a) JOPES Data Logs. Logging capability is provided in JOPES v4.X by the JOPES Logging package. Capture of changes on JOPES TPFDDs and user permission tables are stored automatically in a log/journal format. Compression is used to archive this data to facilitate storage of large amounts of data generated, and to provide for quick and easy access. The functional managers can view this data using the RQT.

(b) Database Fault Conditions. Indications of a fault in the Oracle databases include but are not limited to:

1. Failed replication of JOPES 4.X databases.
2. Loss of synchronization between SSE sites.
3. Errors in establishing user accounts and granting permissions to site-designated Primary Functional Managers.
4. Failed database backup.
5. Oracle journaling begins writing to the error queue.

(c) Network Performance Management

1. The JSSC Service Desk will use the COTS and GOTS tools identified below to perform the performance management role. The tools used to track the following parameters will determine at a minimum:

a. Bandwidth utilization, packet drop rates, and end-to-end performance on access circuits.

b. Access circuit availability/reliability.

c. Input/Output utilization rates.

d. Hard disk and CPU utilization rates of JOPES v4.X servers.

2. The requirements for performance management are based on a multitude of parameters associated with acceptable levels of performance. The collecting of statistical information is used to analyze system and network utilization trends. Performance management functionality will aid greatly in optimizing system and network performance for GCCS-J v 4.X JOPES.

3. Key components of performance management are the smart agents deployed at the SSE sites. They are the heart of the statistical collection effort as they allow real-time objective data analysis to determine the health of each location. These smart agents use Simple Network Management Protocol (SNMP) to send their statistical reports to a centralized network management server at the JSSC Service Desk.

4. COTS network monitoring tools will perform Internet Control Message Protocol requests, “pings,” to determine network node status. Additionally, it will display SNMP “traps” received from devices to indicate either significant events or errors.

5. COTS network health tools will gather data from network devices and strategic servers using SNMP agents, giving visibility of polled network status from a single configurable Web page. The tools will compare each physical network element or network performance (such as LAN/WAN, router, remote access, or response) to a calculated default range. This will calculate a “health index” for each element and made available for real-time analysis while also being stored and available for trend analysis. Trend analysis reports will be available for each of the monitored strategic servers and can be configured to provide data for specific time periods. Events from all network performance monitoring tools will be forwarded to the centralized Enterprise Management console to help provide the complete picture on the status of each strategic server enclave.

APPENDIX A TO ENCLOSURE F

DEPLOYABLE STRATEGIC SERVER OPERATIONS

1. General. The Combatant Commander regards the JOPES database as a critical component of the overall command and control suite. JOPES 4.X architecture must be resilient to support the Combatant Commander's requirements to perform a wide range of operations involving force deployment planning and execution. The requirement to possess a DSSE is an operational prerogative of the Combatant Commander.

2. Scope. The purpose for the Combatant Commander's DSSEs is to provide additional support and performance for the Combatant Commander, especially under situations involving high tempo user-intensive operations. Experience shows that under these situations, intense SIPRNET activity complicates command and control and database synchronization. The DSSE, to a smaller degree, should possess similar capability of its SSE in system component, setup, performance, and operation. DSSEs are deployed and initially set-up by the JSSC forward-deployed personnel and are centrally managed by the JSSC.

3. Request for DSSEs

a. A CJCS Order must be issued to the Director of DISA, ATTN: Principal Director of Operations, to deploy a DSSE. Earliest possible notification increases DISA ability to provide timely support to the Combatant Commander receiving the DSSE. Early notification goal is 30 days or greater. A 3-week, on site response is desired (21 days from the DTG of the Joint Staff notification message). The Combatant Commander is responsible for funding and managing movement for the JSSC personnel and equipment from their home location to the Combatant Commander area of operations.

b. DSSE may be deployed throughout the range of military operations. These operations may occur in a mature, robust communications or an austere communications environment. Specific conditions are indicated below:

(1) When operational assessment by Joint Staff and Combatant Commanders determine a valid operational requirement.

(2) When JSSC, a Combatant Commander, or a JTF involved in crisis action planning or execution of an ongoing mission determines that the JOPES KPPs are not being met on a continuing basis.

(3) The JOPES KPPs are not anticipated to be met based on the expected level of network performance as determined by DISA.

(4) For events such as joint exercises that test the operational capability of the DSSEs.

c. Performance of the DSSE is dependent on many variables. In a pristine environment with robust communication linkages it should support the JOPES KPP thresholds for deployability. In an austere communications environment the DSSE must be able to update data from the FSSE in an efficient manner based on availability of communication lines. Local updating of data on a stand-alone DSSE will not traverse the network. Alternate means of communications must be available to source requirements from any external organization. The commander must be able to conduct operations within local TPFDDs (no external agency support required) throughout the course of stand-alone operations. When reconnected to the FSSE environment, the DSSE must be able to transmit all stored data and receive appropriate updates to resident TPFDDs.

d. Combatant Commander requirements for DSSEs which exceed a 12-month period require approval by the Joint Staff J3. The current GCCS-J v4.X JOPES architecture supports a maximum of 3 DSSEs. This limit and the continued need of a deployable asset must be considered in the decision to maintain a DSSE beyond a 12-month period.

4. Responsibilities

a. Supported Commander. The supported commander will consider the need for a DSSE within his COA selection process (references d and k) and identify within his named operation TPFDD or submitted Request For Forces to the Joint Staff the requirement to deploy a DSSE in support of his operation. Additionally, the supported commander (Combatant Commander or CJTF) will:

(1) Identify specific theater entrance criteria.

(2) Manage and fund initial and recurring movement of JSSC personnel and equipment to/from the deployed location.

(3) Provide SIPRNET connectivity for deployed enclave.

(4) Meet specific site support requirements as identified in the Memorandum of Agreement prior to installation of the DSSE, such as bandwidth availability; heating, ventilation, and air conditioning (HVAC); physical space (to include living, storage, and work areas); and personnel logistics requirements.

(5) Provide force protection for assigned personnel.

(6) Assume OPCON of personnel under the condition that JSSC personnel will support the DSSE. ADCON remains with DISA.

b. Joint Staff. The Joint Staff will publish appropriate orders to alert and task DISA to support DSSE deployment IAW named operation/exercise.

c. DISA

(1) Principal Director of Global Information Grid Operations will cross coordinate with Combatant Commanders to provide network support and any other necessary actions.

(2) JSSC will be tasked to deploy a DSSE in accordance with deployment request.

(3) JSSC will provide support for DSSEs, and will maintain all servers with the latest software and patches at all times. Upon receipt of the DISA/GO tasking in response to a CJCS Order, within the time prescribed, JSSC will:

(a) Load the specific TPFDDs involved in the tasking onto the tasked DSSE.

(b) Ensure the DSSE consists of the hardware and software described in this CONOPS.

(c) Provide personnel to maintain the asset for up to 120 days in-theater to allow for initial startup and troubleshooting. Once the DSSE is set up and operational, a host-site MOA will be initiated. JSSC and host-site will have 120 days from the date the DSSE is operational to complete the MOA. JSSC will return/coordinate any necessary hardware/software upgrades required during DSSE deployment. JSSC will return at completion of the contingency/operation to prepare and ship all enclave equipment to JSSC.

(d) Coordinate with the requesting Combatant Commander as per normal deployment channels to execute the order.

(e) Deploying DSSE support will fall under the OPCON of the Supported Commander while deployed in to the AOR.

5. Requirements

a. DSSEs must address hardware requirements and software configurations in order to achieve KPPs (Enclosure I) as clarified by this document. DSSEs must meet the same logical configuration as the FSSEs. Each enclave contains a JOPES database server, a logical application server, a

logical print server (database/application server), a Web server, and an enclave management server. Bandwidth requirements are as follows:

(1) Austere Conditions. This emulates early field deployments of a command headquarters served by satellite connections. Bandwidth assumes non-dedicated use for the deployable enclave. Bandwidth: 512Kbps, latency 615ms.

(2) Disadvantaged Conditions. This emulates more normal initial field deployment of the command headquarters served by satellite connections. Bandwidth assumes non-dedicated use for the deployable enclave. Bandwidth: 1.2Mbps, latency 615ms.

(3) Normal Conditions. This emulates a mature bandwidth environment for a forward-deployable command headquarters. This assumes land-line connections are available to the deployed enclave. Bandwidth assumes non-dedicated use for the deployable enclave. Bandwidth: 10Mbps, latency 200ms.

(4) Mature Conditions. This emulates a robust bandwidth environment for a forward-deployable command headquarters. This assumes land-line connections are available to the deployed enclave. Bandwidth is dedicated for the deployed enclave's use. Bandwidth: 10Mbps, latency 200ms.

(5) All the above connections are external to any site-specific defense mechanisms such as firewalls or intrusion detection systems.

b. DSSEs will remain part of the operational JOPES network to ensure they are fully functional before deployment. Deployable enclaves will retain current user permissions and minimal test data to ensure the enclaves operate within normal system parameters.

c. DSSE management will occur IAW Enclosure F.

d. System backup will be performed IAW Enclosure F.

6. Concept of Operations

a. DSSEs are DISA/JSSC maintained servers available to a Combatant Commander upon request to respond to emerging crises. DSSEs will be deployed to a Combatant Commander's AOR for no longer than 12 months. The 12 month limit can be extended by intervals of up to 12 months by request of the supported Combatant Commander and the approval of the Joint Staff J3. Combatant Commander requests for extension should be done not later than the beginning of the ninth month of current deployment cycle. Current prioritization of Combatant Commander's requirements and the maximum use

of three DSSEs will be considered before the Joint Staff J3 extension will be given. The DSSE will be deployed in accordance with an appropriate execute order (EXORD) or deployment order (DEPORD). The Supported Commander is responsible for providing sufficient bandwidth to support operation of the DSSE. Sufficient bandwidth is essential for the operation of the overall Strategic Server environment. The Supported Commander will designate the TPFDDs that will be resident on the DSSE. The number of TPFDDs on the DSSE should be minimized to reduce the amount of traffic between the DSSE and the SSEs. The SSE is always the database of record for the enterprise.

b. Connected Operations. When the DSSE is connected to the designated SSE the designated TPFDDs will be kept in synchronization. JSSC will determine the cycle time for synchronization and notify ALCON of that time. The standard between the SSEs is an average of 3 minutes. Depending on the communications environment and the volume of transactions, this time may be adjusted as required. Knowing this figure is important to the decision cycle-time. During connected operations changes can be made within the SSE environment or on the DSSE. Monitoring of the queues between the SSEs and the DSSE is essential. Should queues begin to build, the JSSC may have to execute “minimize” procedures.

c. Disconnected Operations. When the DSSE becomes disconnected from the SSE, procedures must be executed to minimize the impact of bringing the DSSE back into connected operations. When the DSSE rejoins the database, synchronization of the database will begin. The basic rule is that of all changes made to a single ULN, the transaction with the latest date-time stamp will be retained in the database. When operating in disconnected operations, it is essential to keep track of the ULNs that have been changed so that changes made in the SSE can be compared with the DSSE for ULNs that have been changed in both environments. Alternatively, the supported commander may direct work on a PID cease in either the SSE or DSSE during the disconnected period. This alternative would depend on the planning/execution timeline. A second alternative, if SIPRNET access were available, would be for remote users to access the SSE to make their changes.

d. Intermittent Connected Operations. Intermittent connected operations, where the DSSE is sporadically connected to an SSE, are the most difficult. The JSSC Service Desk must place the DSSE on a special watch list. When this happens the JSSC Service Desk will inform users through newsgroup message. End users must be aware of this condition and need to be careful when making changes to the same ULN in both the DSSE and SSE. If reliable SIPRNET is available, remote users may consider going direct to the SSE for more efficient work.

7. Minimize Procedures. The JSSC Service Desk will continuously monitor the operation of the system. If queues begin to build up an operational pause may

be required to allow the queues to be reduced. Which users are directed to reduce or stop their activity will be dependent upon which queues are affected (e.g., send, receive, both). When an operational pause is required, the JSSC Service Desk will inform users via a gcs.jopes.fm newsgroup message.

ENCLOSURE G

TROUBLE TICKET MANAGEMENT

1. Submission

a. Any user may report a problem; however, the user should coordinate with the GCCS-J Site Coordinator and/or series-FMs to verify a problem exists prior to generating a trouble ticket. Each trouble ticket will contain only one problem to be resolved. The submission of a trouble ticket generates a GCCS-J problem report incident (INC) that will be adjudicated by the JSSC Service Desk. The JSSC Service Desk is the focal point for coordinating all GCCS-J trouble tickets from creation through resolution. Site managers will have access and be able to view all tickets in the system for situational awareness.

b. Trouble tickets may be submitted by the most appropriate method:

- (1) Phone call to the JSSC Service Desk.
- (2) The Web-based requester console on the JSSC GMC or JOPES Web page.
- (3) An e-mail to the JSSC Service Desk.
- (4) A newsgroup message posted to the gccs.jopes.fm newsgroup.

c. Actual trouble tickets may be classified if they describe events that security policies and documents deem classified within GCCS-J. Trouble tickets are considered system high (i.e., SECRET), until they can be reviewed by the JSSC technicians and re-assigned classification based on the security classification documents. For this reason, all trouble tickets will contain a classification.

2. Prioritization

a. The priority of a trouble ticket is a derived value based upon the reported mission impact and urgency of the issue. The availability of an acceptable work-around is also important to the determination of priority. The guidelines for determining priority are as follows:

- (1) PRIORITY 1: Mission failure, no work-around, immediate action required, 2-hour response time.

(2) PRIORITY 2: Major mission degradation, no work-around, immediate action required, 2-hour response time.

(3) PRIORITY 3: Major mission impact, work-around available. Standard GPR procedures, 48-hour response time.

(4) PRIORITY 4 & 5: Minor or minimal mission impact. Standard GPR procedures, 48-hour response time.

b. Response times annotated above are for initial response from the JSSC Service Desk to the end user and/or the GCCS-J Site Coordinator/series-FMs with feedback on the progress towards solution. No guarantees are made that the problem will be solved within the timeframes specified.

c. The GCCS-J end users will assign the operational priority. The JSSC service desk will be required to coordinate recommended changes to priority with the GCCS-J Site Coordinator and/or series-FMs, who will inform the end user of recommended changes. The end user/GCCS-J Site Coordinator must approve priority changes.

3. JSSC Service Desk Support. The JSSC Service Desk has five major tasks in relation to the trouble ticket process.

a. Accurately and completely record all trouble ticket information into the INC. This includes all follow-up e-mail and phone calls with the ticket originator and technicians.

b. Coordinate the assignment of the trouble ticket priority.

c. Ensure the classification field is appropriately assigned for each trouble ticket.

d. Ensure the trouble tickets are assigned to the proper organization or person for corrective action. All trouble tickets not resolved at the JSSC Service Desk are escalated to the appropriate subject matter expert or developer for resolution.

e. Providing current status updates to the trouble ticket originator as the information changes.

4. Escalation. If an incident cannot be resolved under JSSC Service Desk stewardship, it is escalated to the GCCS-J Technical Assistance Center (GTAC) where a Problem Investigation (PBI) number is assigned and technical engineering action is initiated. Upon review by the GTAC, a GCCS Software Problem Report (GSPR) number may be assigned for correction in a future release of JOPES. GSPRs will be available for review and comment by site

managers for situation awareness. The Joint Staff J3 and DISA PEO will conduct periodic Problem/Change Review Board meetings to address new Change Requests and GSPRs and review existing priorities.

5. Closure. Once an incident has been resolved, the JSSC Service Desk will contact the originator or GCCS-J Site Coordinator to verify resolution. After verification that the reported issue has been satisfactorily resolved, the incident will be closed within the trouble ticket system. All new instances of the closed trouble ticket will be reported as a new incident, referencing the closed trouble ticket when possible. Figure 8 illustrates the flow of information based on type of user problem.

JOPES v4.X Strategic Server Enclave
Trouble Ticket Process

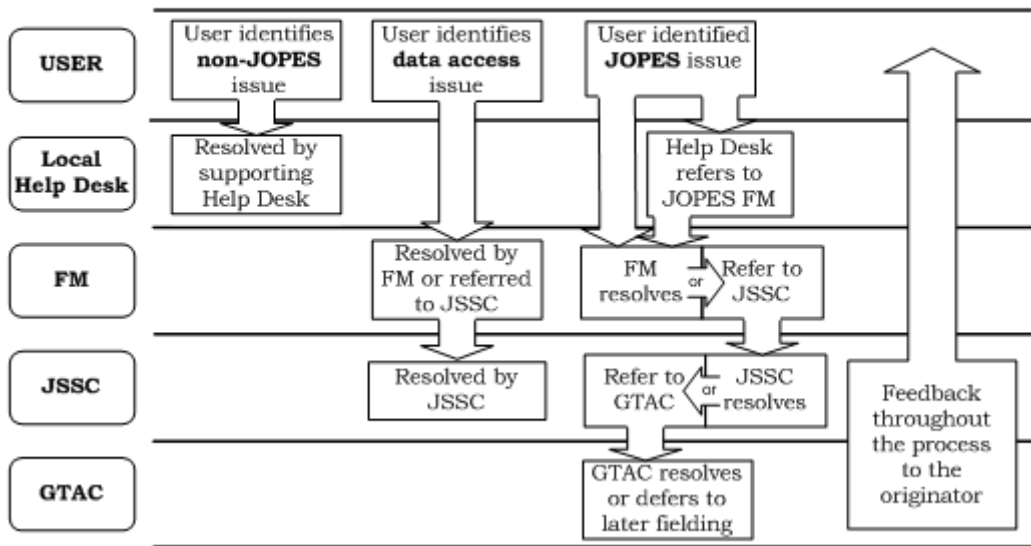


Figure 8. Trouble Ticket Process

(INTENTIONALLY BLANK)

ENCLOSURE H

JOPEs APPLICATIONS

1. Purpose. Enclosure H outlines the basic capabilities of the JOPEs v4.X applications, organized by access method.

2. Application-Server Based Applications

a. JOPEs Editing Tool. JET provides the capability to create, add, modify, delete, and generate deployment-related information contained in a TPFDD. JET processes both force and non-unit TPFDD data. JET allows the user to view carrier related information for selected force requirements. Reports may also be generated for JET list displays. For more detailed reports, the RQT may be directly accessed for predefined or ad hoc reports on selected force or non-unit records.

b. Rapid Query Tool. RQT prints or saves tailored ad hoc reports and provides graphical and mapping displays to help "visualize" JOPEs data. RQT will consist of several "domains" that focus on a cross section of data to include TPFDD, Carrier, GSORTS, standard JOPEs reference files, and audit information. Reports will be developed using user-defined parameters, stored queries, predefined reports, or tabular reports. Standard reference files may be saved in specified JOPEs formats for import into other offline systems. The audit domain allows for analysis of TPFDD update history by USERID and update date. The TPFDD "visualization" tools will permit force data to be depicted graphically by using the "Flow Analysis" functions or overlaid on a rudimentary map display utilizing the "Map Requirements" function. RQT will be integrated with the JET to permit editing of RQT displayed requirements in selected functions, or, conversely, launching of RQT based on requirements displayed in JET.

3. Web-Server Based Applications

a. Adaptive Course of Action (ACOA). ACOA gives operational planners the ability to input, modify, and view the development of joint plans in real-time. Access privileges are applied to users to restrict access during this process. The ACOA application helps geographically separated planners work jointly to rapidly conduct planning and make decisions. ACOA is expected to retire in FY 12.

b. JOPEs Permissions. JPERMS provides the ability to establish JOPEs accounts. The JPERMS provides the JOPEs FM and Sub FMs the ability to assign roles, Series access, and individual TPFDD access to JOPEs users. The

tool also provides users the ability to input user specific data associated to his/her account such as contact number and e-mail address. All JOPES accounts are established through the use of JPERMS.

c. TPFDD Management Tool. TMT application has two packages, TMT and TMT Configuration (TMTCNF). The TMT is a Web-based application used by the JOPES FM to create, delete, and perform simple editing of TPFDDs in the JOPES database. TMT can upload or download either B8, H3, or JSP BULK formatted files. TMT also handles unlocking or setting the restricted mode for TPFDDs. TPFDDs must be created in TMT before permissions can be assigned to these TPFDDs via the JPERMS Tool application. TMTCNF establishes an Oracle TMT_USER role and grants appropriate privileges to TMT_USER associated with TMT. The TMT_USER role is assigned to a USERID through JPERMS.

d. Web Scheduling and Movement (WebSM). WebSM provides the capability to add, review, update, and delete carrier data. Carriers may be created and linked to supported TPFDDs, complete with itinerary information. Itinerary information will include planned and reported arrival/departure times at itinerary routing locations. WebSM provides the capability to allocate and manifest TPFDD requirements on carriers, linked to specific carrier onload and offload locations.

4. Database-Server Based Applications

a. JOPES Synchronization Processor. JSP provides a capability for changes made on one JOPES database server to be replicated to another JOPES database server. JSP provides a mechanism to translate transactions between different JOPESREP versions and transaction formats (backward compatibility).

b. Scheduling and Movement Interface (SMINT). SMINT interprets transactions from the Global Transportation Network and updates the JOPES database with Scheduling and Movement related data supporting OPLANs in execution.

ENCLOSURE I

JOPEs PERFORMANCE PARAMETERS

1. General. GCCS-J Block V requirements, as determined by the Global Command and Control Review Board, are published in reference k. The GCCS operational community established the priority ranking for the NRID where detailed descriptions of most requirements can be found. Reference J defines the Critical Operational Issues (COI) and Measures of Effectiveness (MOE) or Measures of Suitability (MOS) that apply to testing of Block V GCCS-J JOPEs testing.

a. Appendix A to Enclosure I. Table 8 lists the JOPEs Critical Technical Parameter thresholds and objectives for specific functions published in the TEMP (GCCS J Test and Evaluation Master Plan Block V Annex, 21 March 2006) Annex.

b. Appendix B to Enclosure I. Table 9 lists the GCCS-J Block V Acquisition Program Baseline (APB) JOPEs KPP thresholds and objectives for operational requirements for each baseline.

c. Appendix C to Enclosure I. Table 10 lists the Original GCCS-J Block V RID JOPEs Performance Attributes for additional clarification of high interest operational requirements that define threshold and objective values that are measurable and testable.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE I

CRITICAL TECHNICAL PARAMETERS

Table 8. GCCS-J JOPES Critical Technical Parameters

Category	Critical Technical Parameter	Threshold	Objective Value
<p>Force Planning – COI - How well does GCCS-J provide, within deliberate and crisis planning, the capability to provide deployment/redeployment planning and execution, identify forces and total assets, plan force movement; and provide personnel, logistic, sustainment, and other support required to execute military operations until assigned missions are accomplished? COI - How well does GCCS-J provide the capability to transition from force-level planning to execution including C2 activities associated with management of air, space, and joint fires/maneuver assets?</p>			
<p>JOPES Performance</p>	<p>JOPES Synchronization: JOPES data is the same on all strategic server enclaves (SSEs) at an instance in time</p>	<p>Single record update within 3 minutes: Under a loaded networked environment with 500 network-wide concurrent JOPES users at a general ratio of 60% Query and 40% Update. Independently measure the time (stop watch) from the originating box (Single record update) to each of the other JOPES SS enclaves.</p>	<p>Single record update is available to users at all databases not to exceed an average of 1 minute: Under a loaded networked environment with 500+ and up to 1,050 network-wide concurrent users at a general ratio of 60% Query and 40% Update. Enhance the software to automatically capture the latency between the sender and each receiver. The latency times can be automatically gathered and</p>

Table 8. GCCS-J JOPES Critical Technical Parameters

Category	Critical Technical Parameter	Threshold	Objective Value
			measured
JOPES Performance	The ability of the system to load and network a 150,000-record (8 MB file) TPFDD to include Level III, Level IV, and force module details.	The system must be able to load a TPFDD within 1 hour. This is measured by individual users	The system must be able to load a TPFDD within 5 hours. This is measured by individual users
JOPES Availability	One of the JOPES database servers must be available to a user so that they can perform the following functions: F1: Create and Modify Data F2: Create and Modify Reference Data F3: Provide Database Queries F4: Print reports F5: Manage User's Accounts	JOPES must be available for usage 99.7% of the time (24*7*365). Availability = (Uptime / Uptime + scheduled downtime) (F1*F2*F3*F4*F5). Note: F values are either 1 or 0 (1=yes, 0=no). If any of the "F" values are 0, the system is not available.	JOPES must be available for usage 99.99% of the time (24*7*365). Availability = (Uptime / Uptime + scheduled downtime) (F1*F2*F3*F4*F5) Note: F values are either 1 or 0 (1=yes, 0=no) If any of the "F" values are 0, the system is not available.
JOPES Availability	The JOPES System must be able to support mission essential (minimize in effect) Joint operational planning and execution activities after the loss of one or more strategic server enclave sites and/or loss of JOPES Network Support. Definition: The ability of a system to continue to exist and	JOPES must be capable of supporting users after the loss of 50% of the sites for a period of not less than 96 hours. NOTE: The communications network requirements must be delineated in order for JOPES sites to know the technical and hardware requirements for efficient and reliable JOPES connectivity.	JOPES must be capable of supporting users after the loss of 50% of the sites for a period of not less than 96 hours. NOTE: The communications network requirements must be delineated in order for JOPES sites to know the technical and hardware

Table 8. GCCS-J JOPES Critical Technical Parameters

Category	Critical Technical Parameter	Threshold	Objective Value
	function satisfactorily after, or in spite of, loss of any one of its parts due to combat, hostile countermeasures, sabotage, or natural disaster. This includes such performance characteristics as connectivity, denial, dispersion, mobility, diversity, and redundancy. It includes the ability to continue to function through alternate means or through regeneration of system to perform required functions.	Under a loaded networked environment with 500 network-wide concurrent users at a general ratio of 60% Query and 40% Update.	requirements for efficient and reliable JOPES connectivity. Under a loaded networked environment with 500+ and up to 1,050 network-wide concurrent users at a general ratio of 60% Query and 40% Update.
JOPES Strategic Server Maintainability	Recover from a catastrophic failure. Mean time to restore function (MTTRF) Applied to UNIX or Oracle Recovery Process. Catastrophic failure: any fault, failure or malfunction caused by system error, operator error, etc, resulting in a server failure.	A JOPES Web server must be able to recovery from a catastrophic failure within 24 hours. A JOPES database server must be able to recover from a catastrophic failure within 12 hours	A JOPES Web server must be able to recovery from a catastrophic failure within 16 hours. A Jobs database server must be able to recover from a catastrophic failure within 8 hours
JOPES Deployability	DSSE configuration. GCCS-J v4.x provides access to the JOPES database for the most remote users. GCCS-J 4.x	GCCS-J v4.x will provide a deployable strategic server enclave (DSSE) to remote users. Per CJCSM 3122.05,	GCCS-J beyond Block IV will provide a net-centric solution to provide access to the JOPES SSEs data.

Table 8. GCCS-J JOPES Critical Technical Parameters

Category	Critical Technical Parameter	Threshold	Objective Value
	will provide the same functionality for users to access the JOPES data for designated (limited set) PIDS. Access to supporting data (e.g. GSORTS) will be via the SSEs. See CJCSM 3122.05 for additional information on the deployable server. CJCSM 3122.05 will address communications resources and support to be provided by the combatant command.	the combatant command is responsible for providing communications resources and support sufficient to support the DSSE. The DSSE must operate in such a way that it does not adversely impact FSSE performance, Performance will be dependent upon resources provided to support the deployable server	For example: data cached with Web-based interface.
Interoperability – KPP			
Interoperability	Technical details of external and internal interfaces identified in the GCCS-J Interface Control Document are described in a base-lined and configuration-controlled Interface Design Description (IDD), or equivalent documentation.	Technical details of 100% of mission critical interfaces and 70% of non-mission critical interfaces are documented in an IDD, or equivalent.	Technical details of 100% of mission critical interfaces and 85% of non-mission critical interfaces are documented in an IDD, or equivalent.
Interoperability	Data assets shall be made visible by creating and associating metadata (“tagging”), including discovery metadata, for each asset. Discovery metadata	50% of data produced by GCCS-J is tagged and formatted in the Extensible Markup Language (XML). 80% of data formatted in XML is registered in the Metadata	70% of data produced by GCCS-J is tagged and formatted in the Extensible Markup Language (XML). 100% of data formatted in XML is registered in the

Table 8. GCCS-J JOPES Critical Technical Parameters

Category	Critical Technical Parameter	Threshold	Objective Value
	shall conform to the Department of Defense Discovery Metadata Specification. Data assets shall be made understandable by publishing associated semantic and structural metadata in a federated metadata registry.	Registry.	Metadata Registry.
Security – KPP			
Security-IA	Enable GCCS users to seamlessly access all authorized system resources, on the basis of a single authentication.	75% of all GCCS-J applications are accessed via a single authentication. 100% of all JAVA 2 Enterprise Edition (J2EE) GCCS-J applications are accessed via a single authentication.	75% of all GCCS-J applications are accessed via a single authentication. 100% of all J2EE GCCS-J applications are accessed via a single authentication.
Security-IA	The confidentiality of data passed into or out of a GCCS-J enclave shall be ensured.	60% of external systems that communicate with GCCS-J communicate via secure connections. 100% of client/server-architected applications encrypt all authentication transactions. 100% of Web-browser-to-Web-server transactions are protected.	75% of external systems that communicate with GCCS-J communicate via secure connections. 100% of client/server-architected applications encrypt all authentication transactions. 100% of Web-browser-to-Web-server transactions are protected.

APPENDIX B TO ENCLOSURE I

KEY PERFORMANCE PARAMETERS

Table 9. GCCS-J JOPES Key Performance Parameters

Key Performance Parameters		
Operational Requirements	Threshold	Objective
JOPES Synchronization. JOPES data is the same on all strategic server enclaves (SSE) at an instance in time.	Single record update is available to users at all databases not to exceed an average of 3 minutes. Under a loaded networked environment with 500 network-wide concurrent JOPES users at a general ratio of 60% Query and 40% Update.	Single record update is available to users at all databases not to exceed an average of 1 minute. Under a loaded networked environment with > (equal to or greater than) 1,050 network-wide concurrent JOPES users at a general ratio of 60% Query and 40% Update.
JOPES Performance. The ability of the system to process inputs such that queues are not built up on the system to include single data entries as well as plan uploads, copies, and merges. Load and network a 150,000-record (8 MB file) TPFDD to include Level III, Level IV, and force module details.	All GCCS-J system transactions must clear the queue within 10 minute average over a 24 hour period. Must be able to load the TPFDD within 1 hour.	All GCCS-J system transactions must clear the queue within 3 minute average over a 24 hour period. Must be able to load the TPFDD within 30 minutes.

Table 9. GCCS-J JOPES Key Performance Parameters

Key Performance Parameters		
Operational Requirements	Threshold	Objective
<p>Strategic Server (JOPES and SORTS) Operational Availability. Systems must be available to perform the following functions:</p> <ul style="list-style-type: none"> - F1. Create and modify data - F2. Create and modify reference data - F3. Provide database queries - F4. Print reports - F5. Manage user's accounts <p>The probability that system functional capabilities are ready for use by the user at any one database.</p>	<p>99.7%</p> <p>$A = (\text{Uptime} / (\text{Uptime} + \text{unscheduled downtime})) (F1 * F2 * F3 * F4 * F5)$. Note: F values are either 1 or 0 (1=yes, 0=no)</p>	<p>99.99%</p> <p>$A = (\text{Uptime} / (\text{Uptime} + \text{unscheduled downtime})) (F1 * F2 * F3 * F4 * F5)$. Note: F values are either 1 or 0 (1=yes, 0=no).</p>

Table 9. GCCS-J JOPES Key Performance Parameters

Key Performance Parameters		
Operational Requirements	Threshold	Objective
Strategic Server (JOPES and SORTS) Maintainability. Recovery from a catastrophic failure. Mean time to restore function (MTTRF) Applied to UNIX or Oracle Recovery Process. Catastrophic failure: any fault, failure or malfunction caused by system error, operator error, etc, resulting in a server failure.	JOPES: A specific database or Web server must be able to recover from a catastrophic failure. System functionally available within 24 hours. JOPES database recovery within 12 hours. SORTS: A specific database or Web server must be able to recover from a catastrophic failure. System functionally available within 24 hours. SORTS database recovery within 12 hours. Recovery to an alternate location within 24 hours.	JOPES: A specific database or Web server must be able to recover from a catastrophic failure. System functionally available within 16 hours. JOPES database recovery within 8 hours. SORTS: A specific database or Web server must be able to recover from a catastrophic failure. System functionally available within 24 hours. SORTS database recovery within 12 hours. Recovery to an alternate location within 24 hours.

LEGEN D:					
A	Army	GIG	Global Information Grid	NRT	Near Real Time
APB	Acquisition Program Baseline	ISR	Intelligence, Surveillance and Reconnaissance	PID	Plan ID
ATO	Authority to Operate	J2EE	JAVA 2 Enterprise Edition	PKI	Public Key Infrastructure
CJTF	Commander, Joint Task Force	JOPEs	Joint Operation Planning and Execution System	RM	Reference Model
COI	Critical Operational Issue	KIP	Key Interface Profile	SIGIN T	Signals Intelligence
COP	Common Operational Picture	KPP	Key Performance Parameters	SORT S	Status of Resources and Training
DII	Defense Information Infrastructure	MB	Megabyte	SSE	Strategic Server Enclave
F	Function	MTTRF	Mean Time To Restore Function	TPFD D	Time-Phased Force Deployment Data
GCCS- J	Global Command & Control System – Joint	NCOW	Net-Centric Operations and Warfare	UIC	Unit Identification Code

APPENDIX C TO ENCLOSURE I

PERFORMANCE ATTRIBUTES

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
Force Sustainment	Provide the capability to develop sustainment estimates to support Deliberate and Crisis Action Planning.	Provide sustainment estimates to support Deliberate Planning.	Same as threshold but also provide sustainment estimate capability to support Crisis Action Planning.
GCCS-J Access During Maintenance/Reduced Maintenance Cycle for Strategic Server Enclave	GCCS-J users will maintain global capability to access and employment GCCS-J data/applications/and query service.	During maintenance/reduced maintenance cycles for GCCS-J SSE, users maintain global capability to access and employ GCCS-J data/applications/and query service.	During maintenance/reduced maintenance cycles for GCCS-J SSE7, users maintain global capability to access and employ GCCS-J data/applications/and query service.
Force Planning	Provide JOPES responsiveness to President/SecDef and senior military leadership decisions. Provide the capability to support the CJCS directed requirement to validate at level 4 detail per time goals designated by SecDef, CJCS, and the combatant commander. Provide access to source data at the point of	Provide synchronized, accurate, and collaboratively enabled force planning capability that facilitates designated SecDef, CJCS, and/or combatant commander goals by ensuring a 99.7% operational rate, with added	In addition to the threshold, achieve a 99.99% operational rate along with performance latency that does not exceed 60 seconds across the network for upload and edit of a medium OPLAN/TPFDD.

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
	<p>its creation and maintenance. Enabled collaborative planning capability from President/SecDef to unit level. Update and maintain the currency of the database, which generates sustainment levels. Capability to capture the results of all planning and execution activities (such as but not limited to meetings, conferences, video teleconference, collaboration sessions, minutes, reports, etc) in digital format.</p>	<p>functionality for seamless integration of force module editing and TPFDD manipulation capability.</p> <p>Provide a single source feeder system, available for use by all services.</p>	<p>Provide access to source data eliminating the need for feeder systems.</p>
JOPES Data	<p>Implement JOPES database per reference 1. Provide all cargo data (both standard and nonstandard) stored within each JOPES PID.</p>	<p>Fully articulated JOPES database per reference 1.</p> <p>All cargo data (both standard and nonstandard) within a JOPES PID is store and capability of display</p>	<p>Fully articulated JOPES database per reference 1.</p> <p>All cargo data (both standard and nonstandard) within a JOPES PID is store and capability of display</p>
Force Deployment / Redeployment	<p>Provide graphical display and ability to manipulate a TPFDD to display deployment of forces (by UIC, ULN, Force Module, Task Force, operational capability) for planned/actual data. Provide forces and sustainment by unit type by C-day to provide combat power ratio. Provide capability to rapidly select forces and/or</p>	<p>Provide capability to edit force module information in an integrated and seamless manner closely linked to unit level data editing.</p> <p>Ability to graphically display and manipulate a TPFDD to indicate forces by UIC, ULN,</p>	<p>Also provide capability to provide combat power build up in theater for planned versus actual movement and combat power ratio for planned versus actual and scheduled movement.</p>

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
	operational capabilities to meet requirements. Perform end-to-end transportation analysis. Provide the capability to automate the maintenance of Force Modules through pre-defined module rules, thus avoiding the need to update the module whenever the TPFDD is revised. Provide the capability to link scheduling and movement information from the Global Transportation Network into JOPES.	Force Module, and Task Force for planned versus actual movement. Fully developed end-to-end transportation analysis capability.	
Force Employment – Spectrum Operations	Provide capability to anticipate spectrum dependent assets entering a theater.	Provide data structure, interface, and supporting software to flag assets requiring spectrum use prior to entering a theater.	Same as threshold but also provide the means for data source managers to coordinate with spectrum managers assuring verified/validated data fill.
Upgraded B8/H3/DEX	Review, maintain, and sustain B8/H3/DEX capability to allow interface and data transfer/exchange/update with GCCS-J applications/tools and feeder application and tools. Incorporate JOPES database updates per reference 1	Fully functional B8/H3/DEX capability to facilitate interface and provide data transfer/exchange/update with GCCS-J applications/tools and feeder application and tools. Allow full articulation of	Fully functional B8/H3/DEX capability to facilitate interface and provide data transfer/exchange/update with GCCS-J applications/tools and feeder application and tools. Allow full

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
		JOPES database per reference 1	articulation of JOPES database per reference 1
Local PID Functionality	Per classic JOPES environment, provide the capability to initiate, develop, review/edit, and manipulate a JOPES PID on local database prior to networking across the global strategic server network.	Capability is provided to initiate, develop, review/edit, and manipulate a JOPES PID on local database prior to networking across the global strategic server network.	Capability is provided to initiate, develop, review/edit, and manipulate a JOPES PID on local database prior to networking across the global strategic server network.
JOPES Performance – Key Stroke Response	Key Stroke Response. When a user enters a data value the response from this data entry should timely.	Data value entered must be accepted and ready for next data value entry within 2 seconds.	Data value entered must be accepted and ready for next data value entry within 1 seconds.
JOPES Performance – Query Response	Query Response. Data retrieval from primary query application is timely.	Given a 150,000 record (8 MB File) TPFDD to include Level III, Level IV, and force module details that has its query constructed and is ready to execute the query. Complete processing a Force Requirement Detail Report (F11W) (less sorting the report) in a period of less than 5 minutes.	Given a 150,000 record (8 MB File) TPFDD to include Level III, Level IV, and force module details that has its query constructed and is ready to execute the query. Complete processing a Force Requirement Detail Report (F11W) (less sorting the report) in a period of less than 3 minutes.

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
JOPES Performance – Application Error Notification	JOPES applications must provide a visual and/or audible alert when a user enters invalid formatted data.	Less than 5 seconds. Under a loaded networked environment with 500 network-wide concurrent users at a general ratio of 60% Query and 40% Update.	Less than 2 seconds. Under a loaded networked environment with 1050 network-wide concurrent users at a general ratio of 60% Query and 40% Update.
JOPES Performance – Time Synchronization:	All JOPES systems must be synchronized to a single SIPRNET time standard.	Yes, synchronized JOPES systems within single SIPRNET time standards. Under a loaded networked environment with 500 network-wide concurrent users at a general ratio of 60% Query and 40% Update.	Yes, synchronized JOPES systems within single SIPRNET time standards <i>Under a loaded networked environment with \geq (equal to or greater than) 1,050 network-wide concurrent users at a general ratio of 60% Query and 40% Update.</i>
JOPES Performance – Systems Alert and Notification:	Message notifying user of any event that will affect the user’s current work session.	Manual posting of message on a SIPRNET newsgroup in less than 15 minutes from problem detection. Under a loaded networked environment with 500 network-wide concurrent users at a general ratio of	Manual posting of message on a SIPRNET newsgroup in less than 5 minutes from problem detection. Under a loaded networked environment with \geq (equal to or greater

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
		60% Query and 40% Update.	than) 1,050 network-wide concurrent users at a general ratio of 60% Query and 40% Update.
JOPES Supportability	JOPES Global Helpdesk: Support must be available to provide timely feedback on user reported problems on a continuous, 7x24/365 days per year basis. Helpdesk provides support to user-level problems with application software, system connectivity, and database and Web servers in a timely fashion.	Provide problem resolution feedback within 2 hours of notification 80 percent of the time for priority 1 problems.	Provide problem resolution feedback within 90 minutes of notification 90 percent of the time for priority 1 problems.
JOPES Survivability	(a) System must be capable of supporting users after the loss of the network management support. (b) JOPES Network Support must be available from an alternate site.	(a) For a period of not less than 4 hours. (b) Within 4 hours.	Same
JOPES Availability	System must be able to support mission essential (minimize in effect) Joint operational planning and execution activities after the loss of one or more strategic server enclave sites and/or loss of JOPES Network Support. Definition. The ability of a system to continue to exist and function	JOPES must be capable of supporting users after the loss of 50% of the sites for a period of not less than 96 hours. NOTE: The communications network requirements must be delineated in order for JOPES sites to know the	JOPES must be capable of supporting users after the loss of 50% of the sites for a period of not less than 96 hours. NOTE: The communications network requirements must be delineated in order for

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
	<p>satisfactorily after, or in spite of, loss of any one of its parts due to combat, hostile countermeasures, sabotage, or natural disaster. This includes such performance characteristics as connectivity, denial, dispersion, mobility, diversity, and redundancy. It includes the ability to continue to function through alternate means or through regeneration of system to perform required functions.</p>	<p>technical and hardware requirements for efficient and reliable JOPES connectivity.</p> <p>Under a loaded networked environment with 500 network-wide concurrent users at a general ratio of 60% Query and 40% Update.</p>	<p>JOPES sites to know the technical and hardware requirements for efficient and reliable JOPES connectivity.</p> <p>Under a loaded networked environment with \geq (equal to or greater than) 1,050 network-wide concurrent users at a general ratio of 60% Query and 40% Update.</p>
<p>JOPES Deployability</p>	<p>Deployable Strategic Server Enclave configuration. GCCS-J v4.x provides access to the JOPES database for the most remote users. GCCS-J v4.x will provide the same functionality for users to access the JOPES data for designated (limited set) PIDs The JOPES database will generate in connected to the SSEs via secure communications. Access to supporting data (e.g. GSORTS) will be via the SSEs. See CJCSM 3122.05 for additional information on the deployable server. CJCSM 3122.05 will address communications resources and support to be provided</p>	<p>GCCS-J v4.x will provide a DSSE to remote users. Per CJCSM 3122.05, the combatant command is responsible for providing communications resources and support sufficient to support the DSSE. The deployable must operate in such a way that it does not adversely impact FSSE performance. Performance will be dependent upon resources provided to support the deployable server.</p>	<p>GCCS-J beyond Block IV will provide a net-centric solution to provide access to the JOPES SSEs data. For example: data cached with Web-based interface.</p>

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
	by the combatant command.		
<u>JOPES Interoperability</u>	<p>The system will interoperate with external systems with data that is usable within the terms of the Joint Reporting Structures. Will provide a backward compatibility to previous versions of JOPES within the limitations of legacy transaction and B8 formats. Differences will exist with external systems that have not migrated to the latest JOPESREP (reference 1).</p> <p>Threshold: Under a loaded networked environment with 500 network-wide concurrent users at a general ratio of 60% Query and 40% Update.</p> <p>Objective: Under a loaded networked environment with \geq (equal to or greater than) 1,050 network-wide concurrent users at a general ratio of 60% Query and 40% Update.</p>	<p>JOPES External Interfaces (such as but not limited to; see GCCS-J / JOPES interface agreement(s):</p> <ul style="list-style-type: none"> Allied Deployment & Movement System (ADAMS) AMC Deployment Analysis System (ADANS) Computerized Movement Planning & Status System (COMPASS) Consolidated Air Mobility Platform (CAMPS) Defense Readiness Reporting System (DRRS) Deliberate & Crisis Action Planning & Execution Segments (DCAPES) Global Command & Control System (GCCS-J) GCCS-Army (GCCS-A) GCCS-Maritime (GCCS-M) Global Combat Support System (GCSS) Global Status of Resources & Training System (GSORTS) 	<p>Per Threshold value and as updated in GCCS-J / JOPES interface agreements.</p>

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
		<p>Integrated Data Environment (IDE) Global Transportation Network (GTN) Convergence (IGC) Joint Exercise Support System (JESS) Joint Engineer Planning & Execution System (JEPES) Joint Flow & Analysis System for Transportation (JFAST) Joint Force Requirements Generator (JFRG II) Joint Readiness Automated Management System (JRAMS) Medical Analysis Tool (MAT 1.0) Reserve Unit Data Resources System (RUDRS) Single Mobility System (SMS) Sustainment Generator (SUSGEN) Transportation Visualizer (TranzViz)</p> <p>Once data generated by an external system is submitted to GCCS-J JOPES it must</p>	

Table 10. GCCS-J JOPES Performance Attributes

ATTRIBUTE	OPERATIONAL REQUIREMENT	THRESHOLD	OBJECTIVE
		<p>arrive for operational use in an average of 3 minutes. Once external system data arrives in the GCCS-J environment it must traverse the network within the requirements identified in JOPES Synchronization KPP.</p> <p>External systems using B8s must be as good or better than GCCS-J 3.x.</p>	

ENCLOSURE J

REFERENCES

- a. VDJ-3 memorandum, 28 March 2002, "JOPES Key Performance Parameter"
- b. Global Command and Control System Systems Security Support, Trusted Facility Manual version 1.1 CM Number 72930 06 November 2003
- c. GCCS Network/Hardware Standard Configuration and Recommendations
- d. CJCSM 3122.01 series, "Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures)"
- e. Director, DISA letter, 4 April 2003, "GCCS-J v 4.0 JOPES Strategic Server Enclaves"
- f. CJCSI 6731.01 series, "Global Command and Control System – Joint Security Policy"
- g. CJCSI 5714.01 series, "Policy for the Release of Joint Information"
- h. DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"
- i. GCCS-J Test and Evaluation Master Plan (TEMP) Block V Annex, 21 March 2006
- j. Requirements Identification Document (RID), 19 August 2005
- k. CJCSM 3122.02 series, "Joint Operation Planning and Execution System (JOPES) Volume III (Time Phased Force and Deployment Data Development and Deployment Execution)"
- l. CJCSM 3150.16 series, "Joint Operation Planning and Execution System Reporting Structure (JOPESREP)"

(INTENTIONALLY BLANK)

GLOSSARY

AP	Adaptive Planning
ASI	Authorized Service Interruption
C4	Command, Control, Communications, and Computers
CCB	Configuration Control Board
CM	Configuration Management
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
DARWIN	Dynamic Analytical Reporting Web-based Interactive Navigator
DBA	Database Administrator
DCAPES	Deliberate and Crisis Action Planning and Execution Segments
DEX	Data Exchange Format
DISA	Defense Information Systems Agency
DISA/GE	DISA/Principal Director of Global Information Grid Engineering
DISA/GO	DISA/Principal Director of Global Information Grid Operations
DSSE	Deployable Strategic Server Enclave
FCAPS	Fault, Configuration, Accounting, Performance and Security
FDBM	Functional Database Manager
FM	Functional Manager; Force Module
FSSE	Fixed Strategic Server Enclaves
GCCS-A	Global Command and Control System – Army
GCCS-AF	Global Command and Control System – Air Force
GCCS-J	Global Command and Control System – Joint
GCCS-M	Global Command and Control System – Maritime
GCSS	Global Combat Support System
GNC	Global Network Operations Center
GNOSC	Global Network Operations and Security Center
GOTS	Government Off-the Shelf
GSPR	Global System Problem Report
GTAC	Global Technical Assistance Center
IAM	Information Assurance Manager
IAO	Information Assurance Office

IDM	Information Dissemination Management
INC	Incident
IOC	Initial Operational Capability
IT	Information Technology
JCAT	Joint Crisis Action Team
JDNETS	JOPES Data Network Services
JEPES	Joint Engineer Planning and Execution System
JET	JOPES Editing Tool
JOPES	Joint Operation Planning and Execution System
JPEC	Joint Planning and Execution Community
JPERMS	JOPES Permissions
JSP	JOPES Synchronization Processor
JSSC	Joint Staff Support Center
JSUB	JOPES Subscription
KPP	Key Performance Parameter
MOA	Memorandum of Agreement
NIS+	Network Information Service Plus
NOC	Network Operations Center
OEM	Oracle Enterprise Manager
PBI	Problem Investigation
PEO	Program Executive Office
PMO	Program Management Office
RLS	Row Level Security
RQT	Rapid Query Tool
S&NM	System and Network Management
SA	System Administrator
SIPRNET	Secret Internet Protocol Router Network
SIPRNOC	Secret Internet Protocol Router Network Operations Center
SMC	SIPRNET Monitoring Center
SMINT	Scheduling and Movement Interface
SMS	Single Mobility System
SOA	Service Oriented Architecture
SQL	Structured Query Language
TIES	Transitional Interface to External Systems
TLT	TPFDD Loader Tool
TMT	TPFDD Management Tool

TPFDD	Time-Phased Force Deployment Data
TPLNC	TurboPlanner Client
TPLNR	TurboPlanner
TransViz	Transportation Visualizer
WebSM	Web Scheduling and Movement
WHQ	Web Hoc Query

TERMS AND DEFINITIONS

Data Exchange Format (DEX). Defines the format of data files exchanged between JOPEs and external systems. DEX formatted files contain XML-tagged rows of data. The specific format details are found in the JSP FDD. This format is the native format of JOPEs v4.X.

Deployable Strategic Server Enclave (DSSE). DISA provided, DISA managed enclave housing a sub-set of users and TPFDDs required for the exercise/contingency/operation.

Fixed Strategic Server Enclave (FSSE). DISA provided, DISA managed enclave housing all world-wide users and TPFDDs.

JOPEs Data Network (JDNETS). Interface mechanism to exchange JOPEs data with external systems. JDNETS provides Web services to allow decoupling of external systems from JOPEs. Specific Web services available can be found in the JDNETS FDD.

JSSC JOPEs Web site. The main Web site for the JSSC FM Office. Location for all JOPEs management information, also containing links to all operational JOPEs enclaves, application manuals, and server monitoring tools. SIPRNET address - <http://www.gmc.nmcc.smil.mil/jopes>

JSSC Service Desk. The 24/7 central point of contact for all GCCS-J JOPEs IT related questions and problems. The JSSC Service Desk is responsible for the day-to-day centralized management of all JOPEs strategic server enclaves. Primary phone number – DSN 312.225.0671, Comm. 703.695.0671
Primary JOPEs IT email address – jopes@nmcc.smil.mil

Time-Phased Force and Deployment Data (TPFDD). The Joint Operation Planning and Execution System database portion of an operation plan; it contains time-phased force data, non-unit-related cargo and personnel data, and movement data for the operation plan, including:

- a. In-place units.
- b. Units to be deployed to support the operation plan with a priority indicating the desired sequence for their arrival at the port of debarkation.
- c. Routing of forces to be deployed.
- d. Movement data associated with deploying forces.
- e. Estimates of non-unit-related cargo and personnel movements to be conducted concurrently with the deployment of forces.
- f. Estimate of transportation requirements that must be fulfilled by common-user lift resources as well as those requirements that can be fulfilled by assigned or attached transportation resources. (JP 1-02)

Unit Line Number (ULN). A seven-character, alphanumeric field that uniquely describes a unit entry (line) in a Joint Operation Planning and Execution System time-phased force and deployment data. (JP 1-02)

(INTENTIONALLY BLANK)