# GCCS REQUIREMENTS IMPLEMENTATION DOCUMENT (RID) AND EPIP

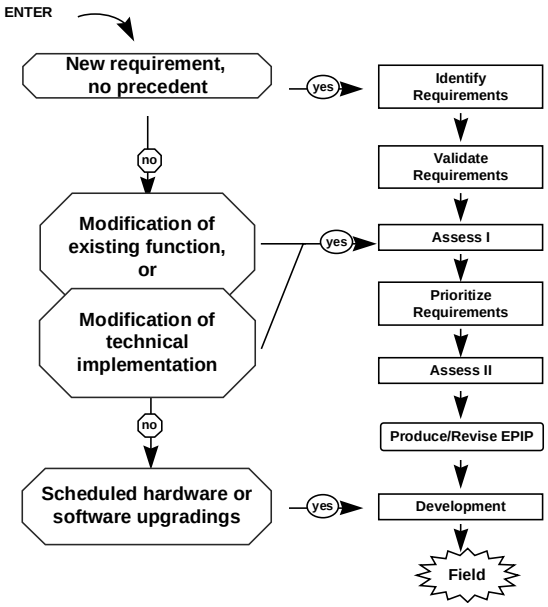
Reference(s): CJCSI 6721.01, Global Command and Control Management Structure, 18 Feb 95
CJCSM 6721.01, Global Command and Control System (GCCS) Functional Requirements Evaluation Procedures, 30 Mar 97

1. Purpose. This section describes the purpose of the RID and EPIP documents stemming from the acquisition approach taken to field the Global Command and Control System (GCCS). It briefly explains the evolutionary acquisition approach to GCCS, how GCCS requirements are determined, how each phase of development is planned via the EPIP, and how GCCS software is developed, tested, and fielded. The final section identifies responsibilities for the EPIP implementation.

2. Evolutionary Approach. The Global Command and Control System (GCCS) is being developed using an evolutionary acquisition strategy. This means there is no "grand design" for the system. The reason for this is that technology changes occur too rapidly to settle on a design that will remain fresh throughout the years. Instead, additional functionality and capabilities are added incrementally over time. User requirements define and shape future changes. Each release expands capabilities and interoperability while retaining many of the software and hardware features common to previous releases - essentially a continuous, measured upgrade of GCCS designed not to overwhelm the operator. In the future, there will be periodic additional releases as needs and technical capabilities continue to evolve. Not only does this approach allow the GCCS architecture to be responsive to rapidly changing technology, but also, to be responsive to CINC, Service, and Agency (CSA) requirements. The main procedural steps in the evolutionary development process are (a) defining and prioritizing requirements, (b) development and testing, (c) fielding.

3. Requirements Process. GCCS development is driven by the requirements and priorities of CINCs, Services, and Agencies (CSAs). CSAs identify new command and control requirements to J-3 (using the GCCS Requirements Data Base (GRiD)). Requirements are assigned for validation to the appropriate GCCS Working Group (these groups are defined by CJCSI 6721.01 and contain representatives from the CSAs). After validation of the requirement, candidate applications or technical solutions are searched for and tested. Users in conjunction with DISA and the GCCS management structure select the best possible technical solution to the requirement. The GCCS Review Board takes recommendations of functional working groups to set priorities of implementation of new GCCS applications. Requirements selected for implementation are added into the most appropriate GCCS incremental phase. These phases are formalized in the Requirements Implementation Document (RID). For technical solutions identified by the GCCS Review Board for implementation in upcoming GCCS releases an Evolutionary Phase Implementation Plan (EPIP) is developed. Based upon the EPIP, implementation is undertaken and products tested and fielded. Figure 1 illustrates the process:

**Figure 1. GCCS Requirements Process**




4. Requirements implementation document. The RID is an overarching document that describes functional requirements necessary for a particular GCCS implementation phase. It provides a short description of the function of each desired requirement.

5. Evolutionary Phase Implementation Plan. The EPIP is a "contract" among the CSAs, DISA, and the Joint Staff (stakeholders). The primary purpose of the EPIP is to provide a common ground for the stakeholders that must work together to successfully deploy GCCS. It documents the following:

- Requirements addressed in a GCCS development phase
- Responsibilities for funding and development of the requirements
- Testing
- Training
- Implementation
- Security
- Systems Architecture
- Integrated Logistics Support
- Risk
- Economic analysis

Experience with the early deployment phases of GCCS has proven that close teamwork, a common understanding of tasks, and realistic expectations among all participants are essential features of the evolutionary development process. The EPIP is the mechanism for accomplishing these goals.

6. Responsibilities.

a) RID. The Joint Staff, J-3 is responsible for developing the RID.

b) EPIP. Defense Information Systems Agency (DISA) is responsible for preparing the EPIP. This work is supported by appropriate CSAs. An EPIP is approved by both the ASD(C3I) and the J3. This approval mechanism replaces the formal milestone review process. The EPIP preparation and approval process significantly streamlines the oversight of the program relative to the traditional, formal process.

c) Systems Integration/Testing. The overall integrator for GCCS is DISA. D-2 and D-6 oversee the development of the Common Operational Environment (COE), and ensure that functional software is properly integrated. Individual applications (and components of the COE), Air Force CTAPS or the Navy METOC programs for example, are developed by the CSAs. Testing includes developmental testing which is the responsibility of DISA. In addition operational testing is performed as appropriate. Operational testing entails only testing changes made to the baseline system of record. The baseline system is the system fully implemented under the last RID/EPIP.

d) Fielding. Fielding is managed by DISA in coordination with CSA action officers. Fielding entails three main activities: training, installation, testing, and the reporting of problems. Fielding includes taking the system from concept to operational capability throughout the entire network.

e) Training. New equipment training (NET) and some new application training is provided by DISA. Field action officers participate in DISA training, and they must train the operators and end users within their commands. DISA will provide training to system administrators on changes to the system administration functions. Included with the delta training will be system documentation of the changes out to the system administrators before fielding begins. The training CONOPS address specific training responsibilities.

f) Installation. Installation is done by both DISA and Service installation teams. DISA will provide installation assistance at the data base sites and major clients. DISA will provide training to Service and Agency installation teams to perform the remaining cut over.

g) Deficiency Reporting. Deficiency reporting is another key element of fielding an evolutionary program. Field action officers are expected to report problems and deficiencies through the GCCS Situation Problem Report (GSPR) feature of the Help Desk as appropriate.

h) User/Field Responsibilities. Specific user responsibilities include:

- Defining and prioritizing requirements: Nominating requirements to J-33. Participating in Requirements Working Groups (RWGs). Supporting GCC Review Board deliberations.

- Testing and evaluation: Support operational testing as needed.

- Fielding: Participate in training and inform command of capabilities. Assist in or perform installation. Provide feedback in trouble reports.

Enclosure(s):

Signature Page

1. Requirements Implementation Document (RID)
2. Evolutionary Phased Implementation Plan

# Signatures

| | |
|---|---|
| _____ | _____ |
| Deputy Director,<br>C4 and Intelligence Programs | J3 |
| _____ | _____ |
| Deputy Director,<br>Engineering and Interoperability | J6 |
| _____ | _____ |
| Deputy Director,<br>C4 Modeling, Simulation, and Assessment | DT/OT Senior Player in community |

_____
Director,
Defense Information Systems Agency

| | |
|---|---|
| _____ | _____ |
| ASD(C3I) | Joint Staff |

# REQUIREMENTS IMPLEMENTATION DOCUMENT (RID)

ENCLOSURE 1

# REQUIREMENTS IMPLEMENTATION DOCUMENT (RID) FOR THE GLOBAL COMMAND AND CONTROL SYSTEM

## PHASE II (Version 3)

1. Purpose. This Requirements Implementation Document provides a statement of functional requirements planned for incorporation into GCCS version 3.0. The major thrust of version 3.0 is a baseline change to move GCCS COE version 2.2 to DII COE version 3.1. Subsequent fielding of applications and new functionality will be implemented as necessary.

2. Background. Following the initial phase, consisting of versions 2.1,2.2, 2.2.1, and 2.2.2, version 3.0 is the second evolutionary phase of the secret-level Global Command and Control System.. The baseline changes will support and enhance functional capabilities and planned functional requirements. In general, requirements planned for this phase of GCCS include the following:

- performance improvement to JOPES.
- introduction of the Joint Force Requirements II Generator (JFRG II)
- prioritized functional fixes to various JOPES applications,
- introduction of the Joint Planning & Execution Toolkit (JPET) to support crisis action planning,
- increased intelligence functionality to include access to a wider range of intelligence data and improved interoperability with and display on the Common Operational Picture (COP) display,
- provides upgrades to some SORTS data functions,
- increased platform independence with improved capabilities for (Windows NT) PC clients,
- introduction of Joint Total Asset Visibility (JTAV) client
- introduction of Joint Personnel Asset Visibility (JPAV) client
- increased interoperability with Service applications through compliance with Defense Information Infrastructure/Common Operating Environment (DII/COE) standards.
- introduction of FOCAL POINT capability
- migration to the Joint Tactical data standard—TADIL J/LINK 16
- introduction of a C4I interoperability data base for joint use
- embedded training for COP

This statement of requirements for the second evolutionary phase of GCCS forms the basis of user expectations for GCCS version 3. It also provides the requirements based foundation for development of the Evolutionary Phase Implementation Plan (EPIP). The EPIP for GCCS Phase II will articulate programmatic topics associated with this evolutionary build. Those topics to include training, logistics support, risks, testing, economic analysis, and schedule.

3. Description of functional requirements. Unless specifically noted, functionality in GCCS version 2.2.X will be carried over into version 3.0. For ease of reference, functional requirements for this phase are categorized into the following sub-sections: JOPES, Common Operational Picture, Intelligence, SORTS, miscellaneous requirements, Security, and DII/COE.

a. Joint Operations Planning and Execution System (JOPES):

1) Improved timeliness (performance) of common Requirements Development & Analysis (RDA), Scheduling and Movement (SM), Ad Hoc Query and related applications.

2) Includes fixes to some GCCS problem reports.

3) Addition of the Joint Planning & Execution Toolkit (JPET)[1]. A product of a USACOM sponsored Advanced Concept Technology Demonstration, JPET is comprised of three distinct applications; TARGET, TPEDIT, and FMEDIT that enhance the crisis action planning and collaborative planning capabilities of GCCS.

a) TARGET version 2.3.1 replacing existing version of TARGET fielded in GCCS version 2.2. Newer version provides user identified enhancements plus software capability to conduct voice with limited video conferencing between two or more workstations. Site hardware, and possibly, communications upgrades are likely required to take advantage of voice/video conferencing.

b) TPEDIT (TPFDD Edit) version 6/96 replacing DART version currently on GCCS. New version includes user identified enhancements.

c) FMEDIT (Force Module Edit) version 3.0.7, provides capability not previously available on GCCS. As the title implies, FMEDIT provides the user with ability to manipulate TPFDD force modules. Application provides the planner with greater flexibility in building new, as well as modifying existing, TPFDDs.

4) Improved 'Airfields' application. A new version of the Airfields application allowing user access from any workstation using the web browser tool (NETSCAPE) on the SIPRNET. This will be one of the first browser-based applications in GCCS that provides a more familiar user interface, better support for low-bandwidth GCCS users, and support for any workstation capable of hoisting a web browser.

5) Adds Global Transportation Network (GTN) application. With an integrated view of transportation data, GTN provides the ability to query and review results of GTN database information permitting in-transit visibility of Transportation Component Command cargo and personnel movements. The GTN client will be identical (in functionality) to its' unclassified counterpart; providing users with the same

[1] Addition of JPET in its' entirety remains tentative as of this writing; TPEDIT, one of the three applications comprising JPET will be available. TARGET and FMEDIT are the tentative portions.

capability to conduct complex retrievals and information display. The GTN database will support historical, operational, and exercise data.

6) JFRG II. Moves JFRG I to a windows based environment that allows Army, Navy, Air Force TUCHA import capabilities, develops and refines interfaces to the JOPES data base, and allows the addition, modification, and deletion of transactions.

a. Common Operational Picture (COP).

1) Theater Ballistic Missile Display (TBMD). With TRAP data feed, TBMD provides ability to display threat ballistic missile indications and warnings; specifically: launch/impact points, and related information in near real-time.

2) Air Tasking Order Overlay. Provides ability to selectively view an ATO message in a variety of different ways, and displays tasked units and targets on a COP overlay. GCCS will also be able to visually link actual tracks to ATO plans, aiding commanders in monitoring the status of mission execution.

3) Enhanced track correlation. Provides enhanced automated capability to distinguish and correlate COP tracks; reducing potential ambiguity.

4) Track Display. Track display permitted from several receive-only interfaces to provide a more comprehensive COP. Specifically permits feeds from TIBS, TADIL B, PLRS, and ELPRS.

5) Imagery display. Access and display of imagery products made available in National Imagery and Mapping Agency's Imagery Product Library.

6) Display of selected data available from Defense Intelligence Agency's Modernized Integrated Database.

7) C2PC. Adds the 'C2PC' (Command & Control for Personal Computer) application providing users with a dynamic COP display available on Windows NT-based clients; providing users on this platform with capabilities previously available only on Sun or Hewlett Packard workstations. While not supporting all of the Unix-based COP capabilities. C2CPC provides users with more capability than Enhanced Linked Visual Information System (ELVIS). ELVIS will continue to evolve in GCCS, however, as it provides low-bandwidth users with the only capability to view the COP..

c. Intelligence.

1) Client software will extend access to available National Imagery and Mapping Agency's Imagery Product Libraries providing imagery and geospatial information. This includes image viewer and basic imagery manipulation tools to enhance situational awareness using images, maps, and geospatial information.

2) Access to available Modernized Integrated Databases through DIA client software to provide general military intelligence.

3) Adds the COLISEUM application allowing users to document and submit intelligence 'Requests for Information' (RFIs).

d. Status of Resources and Training System (SORTS).

1) Reference table updating. Modify SORTS to link currently existing GCCS reference tables to eliminate multiple variants of key reference file data within GCCS. Previously, SORTS obtained TUCHA and GEOFILE data via a special mainframe

retrieval. This resulted in a SORTS view of data that was consistently different than the JOPES view. This change will use the Information Management Services/Reference File Manager (IMS_RFM) segment within GCCS as the common source for key reference file data for both TUCHA and GEOFILE purposes. Using this change, both the JOPES and SORTS applications obtain the same data from the same source, using the GCCS segment designed and fielded for that purpose.

2) Navy Ship Locations. Modify SORTS to utilize Navy ship location data found in JMCIS. The software change will allow timely update of Navy ship locations while eliminating the requirement for Navy ships to submit location data in separate reports.

e. Miscellaneous Requirements.

1) C4I Interoperability data base (tentative). While the final selection of a technical solution for this requirement is pending, the small size of this application and requirement may allow of implementation of this requirement in this phase. This data base application will provide interoperability information on C4I systems, circuits, and leased services with near-real-time access to a wide variety of users and will include system characteristics, uses, and other information necessary to evaluate interoperability requirements. This requirement will fulfill the requirements of CJCSI 6112.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems. Although no single application is designated at the lead, this data base should be fielded in later version of 3.X.

2) FOCAL POINT Capability. The implementation of FOCAL POINT must provide a mechanism that will ensure that the communications are made private between the designated individuals know as Focal Point Systems Control Officers (FPSCOs). The mechanism that provides these privacy is commercial-off-the-shelf software (COTS) product known as SecretAgent.

3) Security. GCCS 3 will provide improved security over version 2.0, and will provide security administrators with a wider range of tools to help administer and secure GCCS.

4) Defense Information Infrastructure, Common Operating Environment (DII COE). GCCS 3 will replace the GCCS Common Operational Environment (COE) with the DII COE, increasing interoperability with other systems, particularly between applications.

5) Upgraded COTS web browser (NETSCAPE COMMUNICATOR) for UNIX, HP, and NT platforms. Communicator expands the capabilities of the current version, to include addition of whiteboard and collaborative tools.

6) Newer versions of the Solaris and HP/UX operating systems. GCCS 3 use the DII COE versions supporting Solaris 2.5.1 & HP/UX 10.20. These operating systems both improve the performance and reliability of GCCS platforms. The new version of HP/UNX will also incorporate several US Navy-specific additions as part of the commercial Operating System, eliminating the vulnerabilities of Navy configurations.

7) Replaces the current Executive Manager segments with a common desktop environment providing user with a more open and intuitive desktop/human-machine interface.

8) Upgraded COTS office automation suite (Applixware 4.3) providing improved import/export interoperability with common PC-based office automation suites (e.g. MS Office), providing the full range of applications for all GCCS users, and providing the flexibility to run these applications via a web-browser..

9) Provides improved capability for UNIX workstation users to access applications running on Intel X86 workstations.

10)Improved interoperability with Service feeder systems. In addition, new DII/COE-compliant Service applications can be made available to users. Examples are expected to include:

a) Tactical METOC (Meteorological and Oceanographic) capability available from USN's Joint METOC application.

b) Selected USAF TBMCS (Theater Battle Management Control System) segments.

c) Provides a limited interoperability with WINDOWS NT 4.0 clients to support available NT PC-based applications (e.g. C2PC, and MS Office).

# ENCLOSURE 2

# EVOLUTIONARY PHASED IMPLEMENTATION PLAN (EPIP) PHASE II

# GCCS VERSION 3.0

# ENCLOSURE 2

## EVOLUTIONARY PHASED IMPLEMENTATION PLAN (EPIP)

### Table of Contents

**EPIP Executive Summary** **2-1-thru 2-14**

**ANNEXES**

**A Requirements Implementation Summary Matrix**

**B Key POC List**
**(by duty, organization, location, office, phone, fax, email, then alphabetically)**

**C Functional Description**

**D System Architecture**

**E Security Plan CONOPS**

**F TEMP CONOPS**

**G Training Plan CONOPS**

**H Production Operations Transition Plan CONOPS**
**(Fielding, Transition Responsibilities, and Steady-State CONOPS)**

**I Integrated Logistics Support Plan**

**J Economic Analysis**

**K Risk Analysis**

**L Acronyms and Definitions**

**EPIP PHASE II**
**GCCS Version 3.0**
**EPIP EXECUTIVE SUMMARY**

The executive summary is divided into three parts: Part 1 is a general overview of the implementation and background. Part 2 is the details of each major part of the implementation, assumptions, risks, and an overview cost analysis. Part 3 is a list of responsibilities.

## PART 1 GENERAL OVERVIEW

**1. General**. GCCS 3.0 will be completed in two stages. Stage 1 of GCCS Release 3.0 will target the DII COE Release 3.1 with existing baseline capabilities, including the (TPFDD - Edit (TPEDIT) portion of Joint Planning and Execution Toolkit (JPET) which will replace the DART functionality, and four security segments. Stage 2 will provide additional application releases and high priority fixes. The second stage applications include Modernized Integrated Database/Imagery Product Archieve/Imagery Product Library for GCCS (MIG), Meteorology and Oceanography (METOC), JPET, and Joint Force Requirements Generator (JFRG II). A current schedule for GCCS 3.0 is shown in Figure A-3. Since the plan calls for a parallel installation, there will be little to no impact on operations as long as the major assumptions concerning backward compatibility are tested to be true. This transition will require aggressive management from the Joint Staff, DISA, and CSAs to ensure all GCCS components are moved in a timely manner for a total system upgrade. The requirements management process, overall testing approach, and issue resolution process are maturing. As they mature user inputs will drive much of the requirement prioritization based on "operational utility."

a. Overview. The Global Command and Control System (GCCS), Release 3.0, represents a maturation of the evolutionary process. The immediate goal of replacing an outdated and expensive system to maintain, control, and operate has occurred. We are now reinvesting those maintenance dollars into targeted improvements. We are also refining the requirement prioritization, testing, training, and guidance processes.

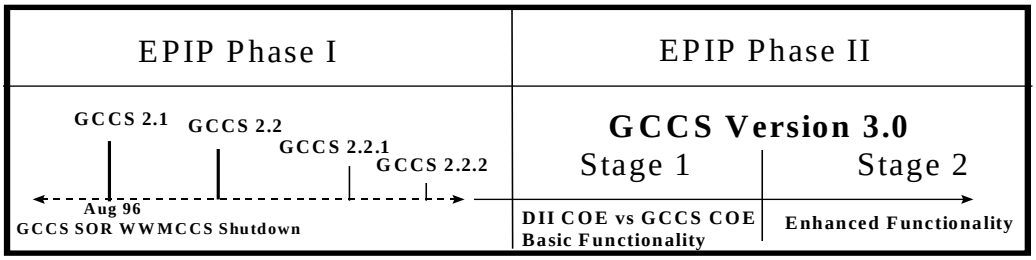



**Figure A-1. EPIP Phases and GCCS**

b. EPIP Phase Description and Relationship to GCCS. GCCS is being implemented in an evolutionary manner through distinct phases to provide the C2 capabilities needed from the foxhole to the National Command Authority (NCA). The objective of EPIP Phase I was for DOD to replace the SECRET and below functionality of the World Wide Military Command and Control System (WWMCCS) with a modern distributed environment (see Figure A-1). The next step, Phase II, is to move that baseline functionality onto the Defense Information Infrastructure (DII) Common Operating Environment (COE) and add additional functionality. Future phases will address opportunities that arise through new major technology and operating environment improvements.

c. The Goal. There are several goals with this implementation, the key goal is to provide a more stable and manageable system with the intoduction of some new functionality. As a pont of performance measurement, users should perceive increases in system reliability, user performance, system response time, and ease of use. Once this implementation is completed, users will be asked for their respective measures relating to these performace areas. To accomplish the foxhole to NCA interoperability, GCCS must grow to a set of fully integrated segments that incorporate the best of many existing C2 systems, and even provide additional capabilities that do not exist today. Therefore GCCS must address three key compatibility issues:

- Incompatible hardware and software platforms
- Incompatible data formats

- Incompatible applications (similar C2 systems collect and use similar data but on different schedules or grouped by different categories).

d. Five Major Functions of Command and Control (C2). The Command and Control arena can be viewed from the Commander's perspective at three levels (Strategic, Operational, and Tactical) to consist of five major functions: 1) Force Development, 2) Intelligence, 3) Sustainment, 4) Mobility & Survivability/Protection, and 5) Employ Forces/Firepower. (These C2 functions are identified in C2 Framework, draft Version 2.1, 7 Apr 95, an ASD(C3I) Functional Information Manager initiative. Each of these five Functional Areas/Communities has a Strategic, an Operational, and a Tactical C2 component. These are the categories used in the EPIP to describe the Mission Application segment functions. Figure A-2 illustrates how the C2 functional areas integrate with GCCS functions.

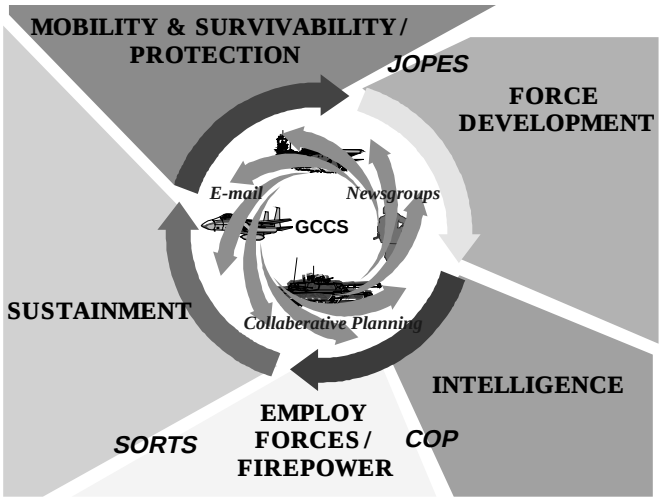



**Figure A-2 C2 Functional Areas**

e. Functional Community Responsibilities. The five C2 Functional Communities, listed above, are responsible for identifying requirements, establishing a Functional Economic Analysis for the required work, and implementing data element standardization efforts. Data standardization references for this work are DOD 8020.1-M Change 1, and DOD 8320.1-M, both initiatives sponsored by the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, OASD (C3I). The five C2 Functional Communities will need to engage User Working Groups and Subject Matter Experts (SMEs) representing these Working Groups to accomplish these tasks. Once the requirement's definitions, justification, and funding have been identified and prioritized, the functional community will continue to be involved in the process as necessary to ensure functional requirements are met.

f. Up Front Development/Testing. The functional community will become involved up-front in the development and prototype efforts, and participate in the testing efforts. All requirements identified by the user community, during the testing, that are really beyond the immediate release will be captured for input into the requirements identification process.

g. Functions, Applications, and Segments. Users should be careful to make a distinction between functions, applications, and segments. A function is a user-defined capability that an application or several applications may provide. Each application, to reside on the COE, is divided up into modular segements according to the DII COE specifications. Build lists usually are a listing of segments and not easily translated into applications or functions. Further, not all applications are segemented the same way so it is not recommended to use the build list a reference to determine applications or functionality. In Stage 1 there are more Solaris segments than HP segments on the build list this does not mean that HP will have less functionality. By the completion of stage II of this implementation plan equal functionality will reside on Solaris and HP.

## PART 2 IMPLEMENTATION SUMMARY

1. Key Assumptions:

a. Management.

1) Assumption M.1 **(validated)**: Testing strategy includes doing a Modified Developmental Test with distinct stages (MDT Stages I, II, and III) at developer sites, at the Operational Support Facility (OSF) and at additional laboratory sites to build confidence before introducing software at operational sites.

2) Assumption M.2 **(validated)**: Video hardware will be provided by Services as needed for applications that require video functionality.

3) Assumption M.3: Enterprise licensing requirements are identified early enough for the Services to purchase necessary software licenses.

4) Assumption M.4: Sites have the necessary support equipment and hardware on site (application servers), or server space for the installation plan.

5) Assumption M.5: Database compatibility between versions will be maintained throughout the implementation.

b. Developmental.

Assumption D.1: Developers or Executive Agents will provide segments and documentation on time. The documentation will be correct and complete (e.g. high-quality).

c. Technical.

Assumption T.1: There are three levels of compatibility assumed: data base, application server, and clients. There will be backwards compatibility between GCCS Release 3.0 and GCCS Release 2.2.x databases. Application servers will work with same release databases and even between UB applications if using MDX to transfer track information (NOT a mix of application servers on the same LAN). Clients only talk to servers, not to each other. Expect 2.2 clients to be able to work with 3.0 servers; but 3.0 clients will not be expected to work with 2.2 servers.

d. Security.

1) Assumption S.1: DII COE is available for developers in April 1997, and will have appropriate security mechanisms.

e. Transition.

1) Assumption X.1: Even though the move to GCCS 3.0 is a "complete rebuild" we will have procedures in place to save accounts, along with associated authorizations and privileges, then restore that information once the install is done -- estimate 2 to 3 weeks per server site to do the full install and restore work but exact time is currently unknown.

2) Assumption X.2: Services are aware of GCCS Release 3.0 fielding schedule and are planning to handle their own server sites, remote clients (regardless of server site), and Service Unique system and interface upgrades.

**2. Section Summaries.**

a. Functional Description. In Stage 1 of this release GCCS will move from GCCS COE version 2.2 to DII COE version 3.1. The DART application will be deleted but functionality will be replaced with the TPEDIT capabilities from JPET. Also, there will be 3 security segments introduced in Stage 1 for the Solaris and HP-UX systems:

- Audit Segment
- Security Alignment Segment
- Security Monitoring and Reporting (SeMORe) tool Segment

Additonally, two commercial audit analysis and management product segments will be available for site purchase:

- Computer Misuse and Detection System (CMDS)
- Stalker

Under Stage 2 the following major new components for Solaris and HP will include:

.
- Integrated Intelligence Capabilities
- Joint Planning and Execution Toolkit (JPET)
- Joint Total Asset Visibility (JTAV)
- Joint Personnel Asset Visibility (JPAV)
- Meteorology and Oceanograpy (METOC)
- Web-Based Access to Mission Applications
- Theater Battle Management Core System (TBMCS)
- Joint Force Requirements Generator (JFRG)

The GCCS Release 3.0 Functional Description, Annex C, will describe the baseline capabilities provided by the segments (mission applications) within GCCS Release 3.0.

One additional security segment will be provided in Stage 2 for the Solaris, HP-UX, and NT platforms:

- Secret Agent

b. Systems Architecture. The basic system architecture remains the same with the exception of the replacement of the current Executive Manager segments with a common desktop environment. The GCCS Release 3.0 System Architecture, Annex D, describes the system structures and interfaces (hardware and software related). It also describes technical requirements, system operations, and the GCCS 3.0 build list.

c. Security. There is not a major change in the security requirements in this version except for the JAVA and NT applications. Testing lessons learned from GCCS(T) will be applied to the approach for ST&E for this version. The Security CONOPS, Annex E, lays out Security responsibilities and major security considerations (e.g. JAVA and NT technology) for GCCS as a critical system using a distributed environment.

d. Master Schedule (Preparation, Execution and Milestone Highlights). Figure A-3 below, outlines a notional master schedule for GCCS 3.0 efforts.

Unclassified

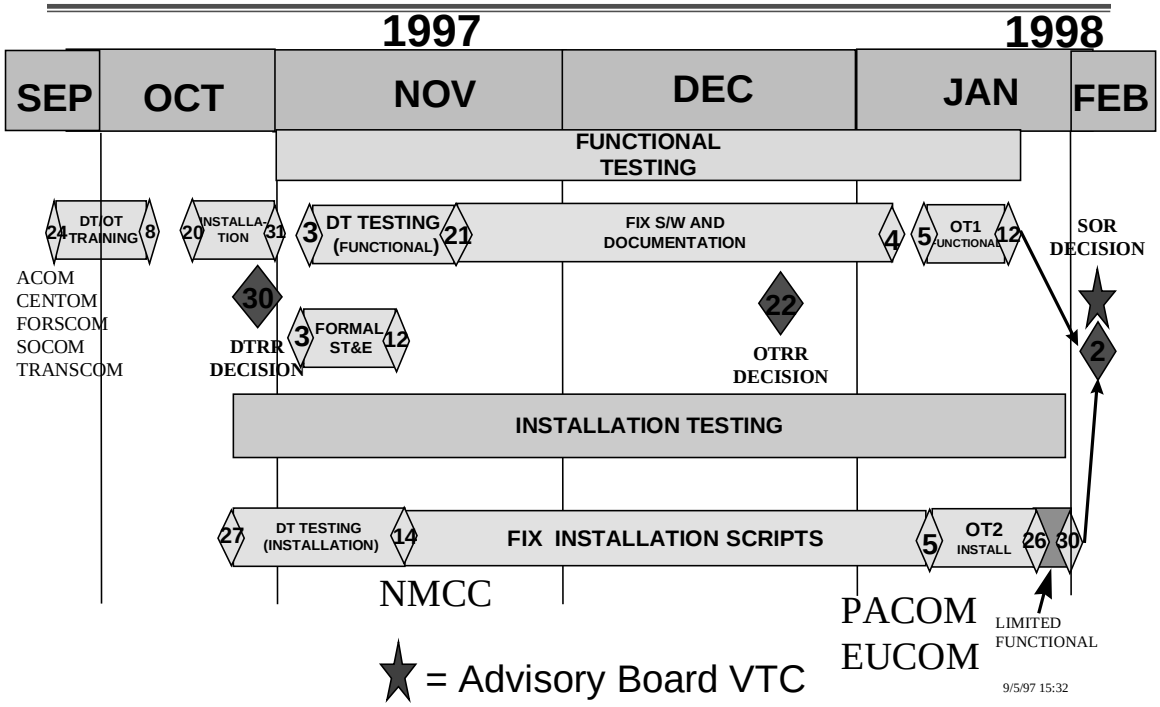



**Figure A-3 GCCS 3.0 Schedule**

e. Training. There will be no major changes of the training concept. New equipment training will be handled by DISA. Application training will be handled by one of these ways:

- JTO/AETC
- NAVY (COP)
- Scenario Based
- Contractor
- Train the Trainer

f. Integrated Logistics Support Plan. Two key points are presented here. The first point addresses hardware and operating system maintenance. The recommended maintenance aproach for equipment hardware and operating software for GCCS Release 3.0 is contract support. The maintenance support and coverage related to equipment hardware and Sun Solaris operating system software is available to CINCs, Services, and Agencies (C/S/As) under the DISA GCCS Omnibus maintenance contract. The second key point addresses the C2 mission application software life-cycle. The ILS Plan, Annex

I, addresses software from three perspectives: 1) licenses, 2) maintenance, and 3) configuration management and control.

g. Economic Analysis. This section summarizes the costs and benefits of the incremental changes associated with GCCS version 3.0. It is important to understand the scope of the costs contained in this cost analysis. Only the *incremental* costs associated with changes in GCCS functionality are addressed herein. The costs associated with the existing GCCS baseline (e.g., operation and maintenance of existing hardware and software packages) are not included even if updates to components of the baseline are covered under this EPIP. The rationale for this is that the cost analysis of the existing baseline accounts for "refreshes" to existing hardware and software.

Given this costing strategy, the cost of enhancements to existing mission applications (e.g., GCCS System Problem Report fixes for JOPES applications) are not included because they are considered maintenance of the existing baseline. This same rationale applies to updates of existing operating systems (e.g., Solaris 2.5.1) and database management systems (e.g., Oracle 7.3.2).

Note that the existing baseline also includes a funding "wedge" that covers the recurring costs of releasing current and future incremental changes.

Although, under this costing strategy, mission application development costs should be addressed in this EPIP, due to the timing of this document, most of these costs are now sunk and are no longer germane to the decision-making process. Thus, with the exception of JPET and JFRG (which have not yet been segmented for GCCS) development costs are not included herein. The following table summarizes the costs associated with GCCS 3.0 by Service or Agency.

**Table A-1: Cost Summary**
**(Figures in thousands of dollars)**

| Organization | FY97 | FY98 | FY99 | FY00 | FY01 | FY02 | FY03 | FY04 | FY05 | FY06 |
|---|---|---|---|---|---|---|---|---|---|---|
| DISA | 2841 | 821 | 821 | 1289 | 821 | 821 | 1289 | 821 | 821 | 1289 |
| Navy | 689 | 1917 | 1725 | 1587 | 1668 | 1507 | 1578 | 1657 | 1507 | 1670 |
| USMC | 679 | 44 | 44 | 255 | 44 | 44 | 255 | 44 | 44 | 255 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Army | 3850 | 2000 | 2000 | 2000 | 2200 | 2050 | 2050 | 2050 | 2050 | 2050 |
| Air Force | 1500 | 3826 | 887 | 1079 | 1270 | 1463 | 1655 | 1655 | 1655 | 1655 |
| JDISS PMO | 0 | 430 | 430 | 430 | 430 | 430 | 430 | 430 | 430 | 430 |
| NIMA | 0 | 535 | 535 | 535 | 535 | 535 | 535 | 535 | 535 | 535 |
| DIA | 0 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 |
| **TOTAL:** | 9559 | 11566 | 8435 | 9168 | 8961 | 8843 | 9785 | 9185 | 9035 | 9877 |

h. Risk. The risk for GCCS 3.0 implementation is medium, yet risks can be minimized if tight controls are maintained on scheduling, testing, and actual implementation. Major areas of concern are validating assumptions, ensuring resource availability and schedule credibility, and maintaining coordination amongst stakeholders. The table below summaries risk factor influences:

| **ADDS TO RISK** | **MINIMIZES RISK** |
|---|---|
| Exercise Schedule | Regional Implementation |
| Assumptions | Two Stage Approach |
| Resource Intensive Plan | Leverage MDT efforts |
| Lack of Funds Availability | Applying GCCS (T) lessons |
| New Baseline | Allow baseline to stabilize |
| Tight Fielding Schedule | More user input in testing |

Summary of the risk categories, specific risk, and relative risk level is given below:

**Table A-2. Relative Risk**

| | | |
|---|---|---|
| Management | Medium | Distributed Program Execution |

| | | |
|---|---|---|
| | | Overlapping Release Efforts<br>Event Driven Schedules<br>Requirement Creep |
| Technical | Medium | GCCS/DII COE<br>Interoperability<br>Technology Limits<br>Database synchronization<br>Interface Definitions<br>Capacity/Performance Issues |
| Development | Low | Schedule for testing<br>Operational test failures<br>Unmet User's expectations<br>Developer's capacity |
| Security | Medium | Security Accreditation |
| Transition | Low | Training<br>Maintenance |

## PART 3 RESPONSIBILITIES

1. Joint Staff, Functional Communities, Work Groups, & Subject Matter Experts (requirements definition/justification, and data element standardization)

Identify functional requirements.

Prioritize requirements and identify associated "operational utility" (across applications within a functional area, and across functional areas).

Develop Functional Economic Analysis (FEA) for new capabilities.

Define standardized data elements.

Register data elements via the C2 Functional Data Administrator.

Participate in prototype development (including MDT Stage I).

Participate in pre-production testing (as MDT Stage II).

Participate in MDT Stage III at laboratory facilities to strengthen confidence level in release.

Participate in Operational Testing.

2. Program Managers/Executive Agents (development)

Build applications/segments to meet the identified requirements.

Engage user community in prototype development efforts for rapid turnaround.

Provide segments to DISA for integration with DII COE and pre-production screening.

3. DISA (GCCS Program Management guidance, pre-production, security, and operational testing; NET; core fielding & site support)

Validate assumptions, minimize risks.

Train site personnel on implementation procedures.

Provide GCCS Programmatic oversight: develop strategies, and execute optimum strategy based on trade-off analysis, communicate strategy, engage the appropriate players and allocate funding to efforts.

Integrate and ensure compatible interfaces between mission apps and DII COE (Pre-Production testing).

Security Testing (ST&E).

Lead Modified Developmental Testing (MDT) in three "Stages" to involve users early and get their feedback into the process quickly (manage expectations on both sides) and keep list of additional functionality needed in future releases.

Field to 39 IOC server sites, and provide assistance/training to regions for installations on the remaining servers and clients.

Coordinate with and train local staff to transition their remote sites, within the timeframe directed by the Joint Staff.

Provide New Equipment Training for 39 IOC sites and special requests from CINCs/Services/Agencies.

Provide initial site support, immediately after transition as required by IOC sites.

Identify the appropriate resources needed for implementation to the C/S/As by Sep 97.

Monitor implementation efforts and provide periodic reports to the Joint Staff and C/S/As.

Maintain a master schedule of events, posting the current schedule, problems, and major activities on the GCCS homepage as available.

Identify appropriate software enterprise license requirements to the services NLT 15 Oct 97.

4. CINCs/Services/Agencies

Support Joint Staff, Functional Communities, and Working Groups by assigning subject matter experts to participate in GCCS requirements definition, prioritization, justification, and data element standardization efforts.

Support implementation efforts by identifying qualified site personnel for implementation and making them available for training.

Implementation of application servers, clients and remote sites below the 39 System of Record (SOR) sites.

Purchase site software enterprise licenses to support the implementation.

Engage in GCCS Review Board and GCCS Advisory Board activities as appropriate to ensure own Commander's perspectives are acknowledged in the requirements prioritization process (provide input to Functional Economic Analysis, and associated funding for new capabilities).

Schedule NET (new equipment training) with DISA as desired for own sites or wait for school house instruction.

# ANNEX A TO ENCLOSURE 2

## REQUIREMENTS IMPLEMENTATION SUMMARY MATRIX

1. The following matrix highlights what was addressed in Phase I and what still remains as a target for Phase II. As the requirements process identifies additional requirements, they will be added to the list for prioritization via an "operational utility rating." Requirements will be grouped by Functional Area to allow for trade-off analysis for funding and approval.

| REQUIREMENTS TEXT EPIP 3.0 | EPIP 1 | POST EPIP1 |
|---|---|---|
| **GCCS GENERAL REQUIREMENTS** | | |
| HAVE THE SAME "LOOK AND FEEL" AS GCCS USING SAME HARDWARE/SW. | X | |
| RELIABLE, NEAR REAL-TIME DATA | X | |
| DEPLOYABLE/MOBILE (INCLUDES ACCESS) | X | |
| ALL GCCS FUNCTIONALITY | X | |
| RELIABLE,REDUNDANT DISTRIBUTED DATABASES | X | |
| IMPROVED CONNECTIVITY | X | |
| POSSESS SECURITY SAFEGUARDS | X | |
| ADAPTABILITY - RESPONSIVE, SCALEABLE | X | |
| ACCURATE DATA/DATABASE SYNCHRONIZATION | X | |
| PERFORMANCE COMPARABLE TO GCCS 2.2 | X | |
| EASE OF ACCESS | X | |
| MISSION SUPPORT | X | |
| USE OF DOD STANDARD | X | |
| SUPPORT TO DEPLOYED FORCES | X | |
| LOCAL CAPABILITY TO PRIORITIZE COMMUNICATIONS/ACCESS REQ | | X |
| NETWORK RELIABILITY | X | |
| COMPATIBILITY WITH PROTOCOLS | X | |
| USE OF WIDE AREA NETWORK (WAN) | X | |
| SUPPORT CRISIS ACTION/DELIBERATE PLANNING - LIMITED EXECUTION | X | |
| SUPPORT CRISIS ACTION/DELIBERATE EXECUTION | X | |
| UNINTERRUPTABLE SERVICE | X | |
| INTEROPERABLE AMONG US SERVICES/ELEMENTS | X | |
| FOCAL POINT CAPABILITY | X | |
| **GCCS TECHNICAL REQUIREMENTS** | | |
| GCCS COE/DII 3.X | X | |

| | | |
|---|---|---|
| SOLARIS 2.5 & ORACLE 7.3 | X | |
| COMMON DESKTOP ENVIRONMENT TO REPLACE EXECUTIVE MANAGER | X | |
| APPLIXWARE UPGRADE (PC/UNIX) | X | |
| LINK 16/ TADIL J COMPATIBILITY | | X |
| **GCCS FUNCTIONAL REQUIREMENTS** | | |
| FILE TRANSFER CAPABILITY (FTP) | X | |
| TELECONFERENCING | X | |
| TELNET CAPABILITY | X | |
| JOINT OPERATION PLANNING AND EXECUTION SYSTEM (JOPES) | X | |
| JOINT RESOURCE ASSESSMENT DATA SYSTEM (JRADS) | X | |
| LOGISTICS FEASIBILITY ANALYSIS CAPABILITY (LOGFAC) | X | |
| MULTI-LEVEL SECURITY (MLS) | | X |
| SCI, CODEWORDS AND SPECAT | | X |
| NETSCAPE FOR JOPES NAVIGATION MENU/HYPERTEXT BROWSER | X | |
| REQUIREMENTS DEVELOPMENT AND ANALYSIS (RDA) | X | |
| SCHEDULING AND MOVEMENT (S&M) | X | |
| ADHOC QUERY (AHQ) | X | |
| PREDEFINED REPORTS (PDR) | X | |
| OFFICE AUTOMATION/REPORT GENERATION | X | |
| JOPES EXTERNAL SYSTEM INTERFACE (ESI) | X | |
| DYNAMIC ANALYSIS AND REPLANNING TOOL (DART) | X | |
| JOINT ENGINEERING PLANNING AND EXECUTION SYSTEM (JEPES) | X | |
| LOGISTICS SUSTAINMENT ANALYSIS AND FEASIBILITY ESTIMATOR (LOGSAFE) | X | |
| INFO MANAGER/REFERENCE FILE MGMT (IMS/RFM) | X | |
| REFERENCE FILE ADMINISTRATION (RFA) | X | |
| CHRONOLOGICAL LOG (CLOG) | X | |
| POSITION LOG (PLOG) | X | |
| CUI VERSIONS OF JOPES/JOINT FORCE REQ GENERATOR (JFRG) | X | |
| AMHS/DMS MESSAGE CAPABILITY | X | |
| PRINT CAPABILITY | X | |
| HIGH-SPEED, WIDE CARRIAGE PRINTER AT EACH LOCAL NODE | X | |
| AUTOMATIC DATA COMPRESSION BUILT INTO FILE TRANSFER AND PRINT ICONS | | X |
| GCCS INTERFACE W/ GCCS(T) MLS | | X |
| DIRECT CONNECT VICE DIAL-UP CAPABILITY | | X |
| GTN INTERFACE | X | |
| WARTIME AIRCRAFT ACTIVITY REPORT SYSTEM (WAARS) INTERFACE | X | |
| AMC DEPLOYMENT AND ANALYSIS SYSTEM (ADANS) INTERFACE | X | |
| AF CONTIN OPNS/MOB PLANNING & EXE SYSTEM (COMPES) INTERFACE | X | |
| MANPOWER/PERSONNEL MODULE (MANPER-M) INTERFACE | X | |
| JOINT STRATEGIC CAPABILITY PLAN (JSCP) INTERFACE | X | |
| JOINT DEPLOYABLE INTELLIGENCE SUPPORT SYSTEM (JDISS) | X | |
| IMAGE VIEWER | X | |
| AIRFIELDS | X | |

| | | |
|---|---|---|
| JOINT MAPPING TOOLKIT(JMTK) | | X |
| COMPUTERIZED MOVEMENT PLANNING AND STATUS SYSTEM (COMPASS) | X | |
| JOINT PLANNING & EXE TOOLKIT - TARGET /TPEDIT /FMEDIT | X | |
| ATO OVERLAY ON COP | X | |
| JPAV/JTAV CLIENTS (ACCESSIBLE THROUGH GTN) | X | |
| JAVA BASED AIRFIELDS SEGMENT | X | |
| C4I INTEROPERABILITY DATA BASE | | X |
| **GLOBAL RECONNAISSANCE INFORMATION SYSTEM (GRIS) REQUIREMENTS** | | |
| DII MIGRATION | X | |
| ON-OFF STATION TIMES | X | |
| JOPES TABLE STANDARDIZATION | X | |
| GRIS TABLE NORMALIZATION | X | |
| MIXED PLATE TRACK COMPLIANCE | X | |
| MESSAGE PLATE TRACK COMPLIANCE | X | |
| MESSAGE EDITING STANDARDIZATION | X | |
| REVISE GRIS SOFTWARE USERS MANUAL | X | |
| REVISE GRIS SYSTEM SEGMENT SPECIFICATIONS | X | |
| MODIFY HELP SCREENS | X | |
| DEVELOP GRIS USER TRAINING | X | |
| GRIS MESSAGE ADDRESSEE USE, REUSE, EDIT, AND DISPLAY | X | |
| GRIS AUTOMATED MESSAGE PROCESSOR | X | |
| GRIS CODES, ABBREVIATIONS, AND ACRONYMS | X | |
| CONSOLIDATED SRO SCHEDULE MESSAGE | X | |
| DAILY SCHEDULE MESSAGE | X | |
| MESSAGES | X | |
| MESSAGE LOCK | X | |
| MISSIONS | X | |
| MISSION INDEX MONITOR | X | |
| MONTHLY MISSION RECAP REPORT | X | |
| NICKNAMES | X | |
| SRO SUMMARY MESSAGE | X | |
| STATISTICAL SUMMARY MESSAGE | X | |
| STATISTICS | X | |
| STATUS LOG | X | |
| STATUS LOG MONITOR | X | |
| TRACKS | X | |
| **GLOBAL STATUS OF RESOURCES & TRNG SYSTEM (GSORTS) REQS** | | |
| PROVIDE THREE LEVELS OF INFORMATION | X | |
| USE GCCS HARDWARE/SOFTWARE/APPLICATIONS | X | |
| REFERENCE TABLE UPDATING | X | |
| NAVY SHIP LOCATIONS | X | |
| EASE OF ACCESS | X | |
| PRINT CAPABILITY | X | |
| PRINT FILE CAPABILITY | X | |
| FILE INPUT CAPABILITY | X | |
| FILE OUTPUT CAPABILITY | X | |
| SUPPORT OPERATIONAL TERMINOLOGY | X | |
| ADAPTABILITY | X | |
| DATA ACCURACY | X | |
| AUTOMATIC DATABASE COMPARISON | | X |
| PERFORMANCE COMPARABLE TO GIQS | X | |
| COMPATIBILITY WITH PERSONAL COMPUTERS | X | |
| MAXIMIZATION OF DATA THROUGHPUT | X | |

| | |
|---|---|
| COMPATIBILITY WITH PROTOCOLS | X |
| USE OF WIDE AREA NETWORK | X |
| CONNECTION WITH OTHER SYSTEMS (INTEGRATED WITH AJMRR & JMRR) | X |
| **JOINT METEOROLOGICAL AND OCEANOGRAPHIC (METOC) REQUIREMENTS** | |
| PRODUCE COLOR-CODED DISPLAYS OF METOC EFFECTS (PARA 5 a. (1)) | X |
| PROVIDE CURRENT WEATHER AT INCIDENT LOCATION (SAR MSN) (PARA 5 a.(2)) | X |
| ABILITY TO ACCESS METOC INFO FROM PRODUCTION DATABASES (PARA 5 b.) | X |
| ABILITY TO TRANSFORM AND COMMUNICATE METOC INFO (PARA 5 c.) | X |
| ABILITY TO CUSTOMIZE METOC OVERLAYS AND DISPLAY ON GCCS MAP IMAGERY | X |
| PRODUCE WEATHER SATELLITE IMAGERY (PARA 5 d. (1)) | X |
| STANDARDIZE WORLDWIDE WEATHER REPORTS (PARA 5 d. (2)) | X |
| DEPICT METOC ANALYSES AND FORECASTS AT 12/24/36/48/72/96/120/144 HRS | X |
| DEPICT SEVERE OR HAZARDOUS METOC CONDITIONS | X |
| DEPICT TROPICAL STORM TRACK INFORMATION IN GRAPHICAL FORM | X |
| DEPICT ELECTRO-OPTICAL EFFECTS | X |
| DEPICT FORECAST AREAS OF MISSION-IMPACTING RADAR REFRACTIVE EFFECTS | X |
| DEPICT FLIR FORECASTS | X |
| DEPICT WIND DIRECTION/SPEED | X |
| DEPICT CLOUD COVER OVER AREA OF RESPONSIBLITY (AOR) | X |
| DEPICT MARGINAL VISUAL FLIGHT RULES AND INSTRUMENT FLIGHT RULES | X |
| DEPICT FRONTAL AND PRESSURE SYSTEMS | X |
| DEPICT WEATHER PHENOMENA/RESTRICTIONS TO VISIBILITY | X |
| DEPICT SOIL MOISTURE | X |
| DEPICT PRECIPITATION TOTALS | X |
| DEPICT SNOW DEPTH RESOLVED TO 1 INCH | X |
| DEPICT TEMPERATURE/HUMIDITY PROFILES | X |
| DEPICT HEIGHTS OF PRESSURE SURFACES | X |
| DEPICT VOLCANIC PLUME TRACKING AND PREDICTION | X |
| OUTPUT FROM MODELS DEPICTING TRANS, DISPERSION, AND NBC FALLOUT | X |
| DEPICT CHAFF FORECASTS | X |
| DEPICT BALLISTIC WIND AND DENSITY FORECASTS | X |
| DEPICT SIGNIFICANT WAVE HEIGHTS | X |
| DEPICT ICE EDGE ANALYSIS AND POLYNA ANALYSIS | X |
| DEPICT BATHYMETRY | X |
| DEPICT OCEAN CURRENTS | X |
| DEPICT SURF | X |
| DEPICT TIDAL CURRENTS | X |
| DEPICT TIDAL CYCLE | X |
| DEPICT OCEAN FRONTS AND EDDIES | X |
| DEPICT LAYER DEPTHS | X |
| DEPICT SOUND CHANNEL | X |
| DEPICT TOPOGRAPHIC NOISE STRIPPING POTENTIAL | X |
| DEPICT AMBIENT NOISE | X |
| DEPICT BIOLUMINESCENCE | X |
| DEPICT BIOLOGICS | X |
| DEPICT SOUND VELOCITY PROFILES | X |
| DEPICT REVERBERATION ASSESSMENT | X |
| DEPICT UNFAVORABLE ASW CONDITIONS | X |
| DEPICT SALINITY | X |
| DEPICT GRAPHIC AND ALPHANUMERIC CHARTS AND TABLES | X |
| DEPICT SPACE WEATHER PRODUCTS - AREAS OF SATCOM AVAILIBILITY | X |
| DEPICT HF, UHF, VHF PREDICTED RANGES | X |
| DEPICT SOLAR FLUX VALUES | X |
| DEPICT GEOMAGNETIC INDICES | X |

| | | |
|---|---|---|
| DEPICT SUNSPOT NUMBER | X | |
| DEPICT REFRACTIVE INDICES (IONOSPHERIC AND TROPOSPHERIC) | X | |
| DEPICT ADVISORIES AND WARNINGS FOR SOLAR FLARE BURST EVENTS | X | |
| DEPICT ADVISORIES AND WARNINGS FOR SHORT WAVE FADES | X | |
| DEPICT ADVISORIES AND WARNINGS FOR PROTON EVENTS | X | |
| DEPICT ADVISORIES AND WARNINGS FOR GEOMAGNETIC STORMS | X | |

**INTELLIGENCE FUNCTIONALITY REQUIREMENTS**

| | | |
|---|---|---|
| APPLICATIONS RUN ON GCCS HW/SW/DII/COE | X | |
| USE DOD STANDARD | X | |
| ADAPABLE | X | |
| ACCURATE/RELIABLE DATA | X | |
| PERFORMANCE MUST SUPPORT COMMANDER'S REQUIREMENTS | X | |
| SCALEABLE | X | |
| SUPPORT CRISIS ACT PLANNING, EXECUTION, DEPLOYMENT/REPLOYMENT | X | |
| PROVIDE COLLATERAL LEVEL INFORMATION | X | |
| ACCESS TO IMAGERY AND GEOSPATIAL DATA | X | |
| ACCESS TO GENERAL MILITARY INTELLIGENCE | X | |
| CORRELATED, NEAR-REAL-TIME RED FORCE DATA | X | |
| ACCESS TO FINISHED TEXTUAL ANALYSIS FROM INTEL CENTERS | X | |
| ACCESS TO TARGETING DATA, INCLUDING TARGET SYSTEMS, BDA, FAC DATA | X | |
| ACCESS TO TARGETING DATA, INCLUDING TARGET IMAGERY, & TARGET FOLDER | X | |
| CAPABILITY TO REQUEST ADDITIONAL COLLATERAL INTEL | X | |
| RED TRKS LINKED TO GEN MIL INTEL DATA TO PROVIDE FUSED JOINT PICTURE | X | |
| EXTRNAL INTERFACES: TBMCS/JMCIS/ASAS/MAGTAF II/IAS/SOF IV/BROADCASTS | X | |
| IMAGERY PRODUCT LIBRARY (IPL) ACCESS & DISPLAY | X | |
| IMAGE VIEWER AND BASIC IMAGERY MANIPULATION TOOLS | X | |
| MODERNIZED INTEGRATED DATABASE (MIDB) ACCESS & DISPLAY | X | |
| CORRELATION APPLICATION | X | |
| INTELINK-S | X | |
| THEATER BALLISTIC MISSILE DEFENSE (TBMD) SEGMENT WITH INTERFACE | X | |
| REQUEST FOR INFORMATION (COLISEUM) | X | |
| INTEROPERABLE | X | |
| COLLECTION MANAGEMENT | | X |
| 3D TERRAIN AND SENSOR DEPICTION | | X |
| COLLABORATION TOOLS | | X |
| RECEIVE AND PROCESS DATA FROM GBS AND IBS | | X |
| ACCESS TO FORCE PROTECTION DATABASES | | X |
| IMPORT AND CORRELATE SANITIZED SCI INFORMATION | | X |
| GCCS AS FUSION NODE FOR AIR, GROUND, MARITIME, & SOF INTEL PICTURES | | X |
| PRODUCTION QUALITY RECEIVE ONLY INTERFACES - TIBS/TADIL B/PLRS/EPLRS | X | |

(INTENTIONALLY BLANK)

ANNEX B TO ENCLOSURE 2

KEY POC LIST

**Table 1: Key POCs Listed by Area of Responsibility**

## GCCS Program Manager Office and Related PM/EA Offices

| | | | | |
|---|---|---|---|---|
| GCCS PM | DISA/OSF | D2 | LtCol Dave Scearse | 703-735-8281 |
| Engr POC | DISA/OSF | D2 | LTC Marc Withers | 703-735-8185 |
| Resource Lead | DISA/OSF | D2 | LtCol Herb Diew | 703-735-8824 |
| Risk/Y2K POC | DISA/OSF | D2 | Maj Brian Eleazer | 703-735-8283 |
| Training POC | DISA/OSF | D2 | Maj John Sisk | 703-735-8936 |
| Resource POC | DISA/OSF | D2 | Maj Paul Taylor | 703-735-8281 |
| ILS | DISA/OSF | D4 | Berk Jeffries | 703-735-8629 |
| COP PM/EA | | | | |
| MIG PM/EA | | | | |
| JFRG PM/EA | HQMC | LPS | Mr. Carl Marchetti | 703-696-1073 |
| METOC PM/EA | | | | |
| JPET PM/EA | | | | |
| JOPES PM/EA | | | | |
| SORTS PM/EA | | | | |
| xx PM/EA | | | | |
| xx PM/EA | | | | |
| xx PM/EA | | | | |
| xx PM/EA | | | | |
| xx PM/EA | | | | |
| xx PM/EA | | | | |

## C2 Functional Communities

| | | | |
|---|---|---|---|
| C2 Functional Area Lead | Pentagon | J3 | LTC Thigpan |
| COP WG Chair | | AIR STAFF | |
| INTELLWG Chair | | | |
| JOPES WG Chair | | J-3 | |
| METOC WG Chair | | J-38 | |
| SIWG WG Chair | | J-6V | |
| READINESS WG Chair | | J-34 | |
| TRAINING WG Chair | | J-33/J-6V | |
| CRISIS ACTION WG Chair | | J-3 | |
| TBM WG Chair | | BMDO/J-3 | |
| COALITION INTEROPERABILITY WG Chair | | J-6V | |
| xx WG Chair | | | |
| xx WG Chair | | | |
| xx WG Chair | | | |
| xx WG Chair | | | |
| xx WG Chair | | | |
| xx WG Chair | | | |

## Segment Development

| | | | | |
|---|---|---|---|---|
| GCCS System Engineer DISA | DISA/OSF | D68 | LtCol Intae Kim | 703-735-8712 |
| Alt GCCS System Engineer | DISA/OSF | D68 | Cookie Carlson | 703-735-xxxx |
| Release 3.0 | DISA/OSF | D68 | Maj. Jim Quetsch | 703-735-8513 |
| Security | DISA/OSF | D68 | CAPT Viersen | |
| xx Developer | | CSC | | |
| xx Developer | | SRA | | |
| DII COE Developer | | INRI | | |
| xx Developer | | SAIC | | |
| xx Developer | | | | |
| xx Developer | | | | |
| xx Developer | | | | |

## Modified Development Test (MDT): Stage I

| | | | |
|---|---|---|---|
| Stage I Lead | DISA/VASQ | JITC | Luanne Overstreet |

| | | | | |
|---|---|---|---|---|
| Developer | Dev. site | INRI | | |
| Developer | Dev. Site | CSC | | |
| Developer | Dev. Site | PRC | | |
| Developer | Dev. site | SAIC | | |

## Pre-Production Efforts at OSF

| | | | | |
|---|---|---|---|---|
| Configuration Management | DISA/OSF | JIEO/JEJ | Jo Tate | 703-735-8246 |
| Integration | DISA/OSF | JIEO/JEJ | Ms. Susan Warshaw | 703-735-8644 |
| Product Assurance | DISA/OSF | JIEO/JEJ | Mr. Dan Lewis | 703-735-8506 |
| Product Support | DISA/OSF | JIEO/JEJ | Mr. Mike DiAndrea | 703-735-8503 |
| Director of Operations | DISA/OSF | JIEO/JEJ | Mr. Larry Long | 703-735-8502 |
| GCCS Product-Line Manager | DISA/OSF | JIEO/JEJ | LTC Hayward Hull | 703-735-8148 |
| OSF Deputy | DISA/OSF | JIEO/JEJ | Mr. John Bridger | 703-735-8647 |
| OSF Chief | DISA/OSF | JIEO/JEJ | Ms. Joanne Arnette | 703-735-8500 |

## MDT Stage II

| | | | |
|---|---|---|---|
| Stage II Lead | DISA/VASQ | JITC | Luanne Overstreet |
| Developer | DISA/OSF | INRI | |

| | | | | |
|---|---|---|---|---|
| Developer | DISA/OSF | CSC | | |
| Developer | DISA/OSF | PRC | | |
| Developer | DISA/OSF | SAIC | | |

## Baseline Freeze

| | | | | |
|---|---|---|---|---|
| PM | | | LtCol Dave Scearse | |
| GCCS System Engineer | | | LtCol Intae Kim | |
| C2 Functional Area Lead | Pentagon | J3 | LTC Thigpen | |
| CDR, JIEO | DISA/HQ | D6 | BG Salisury | |

## DTRR

| | | | | |
|---|---|---|---|---|
| Stage III Lead | DISA/FTH | JITC | Mr. Sam Assi | |
| Stage I & II Lead | DISA/VASQ | JITC | Ms. Luanne Overstreet | |
| OSF POC | DISA/OSF | JIEO/JEJ | Mr. Dan Lewis | 703-735-8506 |
| GCCS System Engineer | DISA/OSF | D68 | LtCol Intae Kim | |
| PM GCCS | DISA/OSF | D2 | LTC Marc Withers | |

## MDT Stage III

| | | | |
|---|---|---|---|
| Stage III Lead | DISA/FTH | JITC | Mr. Sam Assi |
| FTH Lead | | | |
| OSF Lead | | | |
| EDS (AF) Lead | | | |
| xx (Navy) Lead | | | |
| xx (Army) Lead | | | |
| JDEF Lead | | | |
| SME | | | |
| SME | | | |
| SME | | | |
| SME | | | |
| SME | | | |
| SME | | | |

## ST&E

| | | | | |
|---|---|---|---|---|
| Security Lead | DISA/SKY | D25 | Mr. Jack Eller | |
| OSF Lead | | | | |
| NMCC Lead | | | | |
| DII COE POC | | | | |
| App Expert | | | | |
| App Expert | | | | |
| App Expert | | | | |
| App Expert | | | | |
| App Expert | | | | |
| App Expert | | | | |
| App Expert | | | | |

## New Equipment Training (NET)

| | | | | |
|---|---|---|---|---|
| NET Lead | DISA/OSF | D2 | Maj John Sisk | 703-735-8936 |
| Army NET Lead | | | | |
| AF NET Lead | | | | |
| Navy NET Lead | | | | |
| Marine Corps NET Lead | | | | |
| Region 1 NET Lead | | | | |
| Region 2 NET Lead | | | | |
| Region 3 NET Lead | | | | |
| Region 4 | | | | |

NET Lead
Region 5
NET Lead

## Operational Test Readiness Review (OTRR)

| | | | |
|---|---|---|---|
| OT&E Lead | DISA | JITC | LCDR Thompson |
| ST&E Lead | DISA/SKY | D25 | Mr. Jack Eller |
| Stage III Lead | DISA/FTH | JITC | Mr. Sam Assi |
| PM | DISA/OSF | D2 | LTC Marc Withers |
| C2 Functional Area Lead | Pentagon | J3 | LTC Thigpen |
| CDR, JIEO | DISA/HQ | D6 | BG Salisbury |

## Operational Test & Evaluation (OT&E)

| | | | |
|---|---|---|---|
| OT&E Lead | DISA/ | JITC | LCDR Thompson |
| Army OT&E Lead | | | |
| AF OT&E Lead | | | |
| Navy OT&E Lead | | | |
| Marine Corps OT&E Lead | | | |
| Region 1 OT&E Lead | | | |
| Region 2 OT&E Lead | | | |
| Region 3 OT&E Lead | | | |
| Region 4 OT&E Lead | | | |
| Region 5 OT&E Lead | | | |
| SME | | | |
| SME | | | |
| SME | | | |

SME
SME
SME
SME
SME
SME
SME

## SOR (System Of Record) Decision

| | | | |
|---|---|---|---|
| C2 Functional Area Lead | Pentagon | J3 | LTC Thigpen |
| PM GCCS | DISA/OSF | D2 | LtCol Dave Scearse |
| GCCS System Engineer | DISA/OSF | D68 | LtCol Intae Kim |
| CDR, JIEO | DISA/HQ | D6 | BG Salisbury |

## Field to IOC Sites (use five region construct)

| | | | | |
|---|---|---|---|---|
| Core Installation Lead | DISA/OSF | JIEO/JEI | Mr. Bob Marchese | 703-735-8661 |
| Region 1 POC | | | TBD | |
| Region 2 POC | | | TBD | |
| Region 3 POC | | | TBD | |
| Region 4 POC | | | TBD | |
| Region 5 POC | | | TBD | |

## Other Sites

AF Lead
AF Unique Segment Developme nt POC
AF OT&E POC
AF Installat ion POC
AF NET POC
AF Site A
AF Site B
AF Site C

Navy Lead
Navy Unique Segment Developme nt POC
Navy OT&E POC
Navy Installat ion POC
Navy NET POC
Navy Site A
Navy Site B
Navy Site C

| | | | | |
|---|---|---|---|---|
| Army Lead Army Unique Segment Development POC | | | | |
| Army OT&E POC | | | | |
| Army Installation POC | | | | |
| Army NET POC | | | | |
| Army Site A | | | | |
| Army Site B | | | | |
| Army Site C | | | | |
| Marine Corps GCCS Functional Manager | HQMC | PP&O | Action Officer Maj John Gambrino | DSN 224-5212 |
| Marine Corps GCCS Program Manager | COMMARCOR-SYSCOM | PMCIS | Action Officer Maj Keith Davis | DSN 278-2645 x 2591 |
| Marine Corps Network Operations Center | COMMARCOR-SYSCOM | NOC | Action Officer Maj John Burnette | DSN 278-3418 |
| Marine Corps Software Configuration Manager | MTCSSA | GSD | Action Officer Maj Sam Kirby/Maria Hahn | DSN 365-3073/2158 |

DIA Lead
DIA Unique Segment Developme nt POC
DIA OT&E POC
DIA Installat ion POC
DIA NET POC
DIA Site A
DIA Site B
DIA Site C

NSA Lead
NSA Unique Segment Developme nt POC
NSA OT&E POC
NSA Installat ion POC
NSA NET POC
NSA Site A

| | | | |
|---|---|---|---|
| NSA Site B | | | |
| NSA Site C | | | |
| DLA Lead | HQ DLA | Lt Col Kelly | DSN 427-3708<br>703-767-3708 |
| DLA Unique Segment Development POC | | | |
| DLA OT&E POC | | | |
| DLA Installation POC | | | |
| DLA NET POC | | | |
| DLA Site A | | | |
| DLA Site B | | | |
| DLA Site C | | | |
| MTMC Lead | | | |
| MTMC Unique Segment Development POC | | | |
| MTMC OT&E POC | | | |
| MTMC Installation POC | | | |
| MTMC NET POC | | | |
| MTMC Site | | | |

| | | | | |
|---|---|---|---|---|
| A MTMC Site B MTMC Site C | | | | |
| DSWA Lead | HQ DSWA | OPOM | Mrs. Sandra Tewell | 703-325-1007 |
| DSWA Unique Segment Development | HQ DSWA | OPOM | MAJ Robert Lovett | 703-325-7044 |
| DSWA OT&E | HQ DSWA | OPOM | MAJ Robert Lovett | 703-325-7044 |
| DSWA DSWA Installation | HQ DSWA | OPOM | MAJ Robert Lovett | 703-325-7044 |
| DSWA NET | HQ DSWA | OPOM | MAJ Robert Lovett | 703-325-7044 |
| DSWA Site A | HQ DSWA | OPOM | Mrs. Sandra Tewell | 703-325-1007 |
| DSWA Site B | FCDSWA | FCPC | Mrs. Mary Garcia | 505-846-8558 |

(INTENTIONALLY BLANK)

ANNEX C TO ENCLOSURE 2

FUNCTIONAL DESCRIPTION

**TABLE OF CONTENTS**

EXECUTIVE SUMMARY
1.0 INTRODUCTION
2.0 BACKGROUND
3.0 REFERENCE DOCUMENTS
4.0 GENERAL OPERATIONAL REQUIREMENTS
5.0 SYSTEM CONSTRAINTS
6.0 FUNCTIONAL CAPABILITIES
6.1 FUNCTIONAL AREAS UNDER THE SUN SOLARIS UNIX OPERATING SYSTEM
6.1.1 Force Development and Deployment
6.1.1.1 Joint Operation Planning and Execution System (JOPES)
6.1.1.2 Evacuation File Maintenance and Retrieval System (EVAC)

6.1.1.4 Joint Planning and Execution Toolkit (JPET)
6.1.1.5 Transportation Component Command External System Interface (TCCESI)
6.1.1.6 Navy Reserve Unit Data Resource System (RUDRS)
6.1.1.7 Global Transportation Network (GTN)
6.1.2 Intelligence
6.1.2.1 Global Reconnaissance Information System (GRIS)
6.1.2.2 Joint Deployable Intelligence Support System (JDISS)
6.1.2.3 Modernized Integrated Database/Image Product Archive/GCCS (MIG)
6.1.2.4 Meteorology and Oceanography (METOC)
6.1.2.5 Naval Intelligence Processing Services (NIPS)
6.1.2.6 StrikePlot (STRIKE)
6.1.2.7 Coliseum (COLSM)
6.1.3 Sustainment
6.1.3.1 Joint Personnel Asset Visibility (JPAV)
6.1.3.2 Joint Total Asset Visibility (JTAV)
6.1.4 Mobility & Survivability/Protection
6.1.4.1 Theater Ballistic Missile Defense (TBMD)
6.1.4.2 TBMD Shared Early Warning (TSEW)
6.1.5 Employ Forces/Firepower
6.1.5.1 Automated Message Handling System (AMHS)
6.1.5.2 Common Operational Picture (COP)

6.1.5.3 Air Tasking Order (ATO) Review Capability
6.1.5.4 Theater Battle Management Core Systems (TBMCS)
6.1.6 System Administration Tools
6.1.6.1 GCCS System Tools
6.1.6.2 DII COE Tools 1
6.1.6.2.1 Database Tools
6.1.6.2.2 Security Tools
6.1.6.2.3 Web/Teleconferencing Tools
6.1.6.2.4 Network Administration Tools
6.1.6.2.5 Office Automation Tools
6.1.6.2.6 Unified Build (UB)
6.1.6.2.7 Joint Mapping Toolkit (JMTK)
6.1.6.2.8 Character Based Interface (CHARIF)
6.1.6.2.9 MAILX For CBIF (MAILX)
6.1.6.2.10 Mail Services (MSVCS).
6.1.6.2.11 PERL (PERL)
6.1.6.2.12 Printer (PRINTER)
6.1.6.2.13 Point-To-Point Protocol (PPP)
6.1.6.2.14 Remote Access (REMOTE ACCESS)
6.1.6.2.15 Remote Install (REMOTE INST)
6.1.6.2.16 Remote Printing (REMOTE PRINTING)
6.1.6.2.17 System Maintenance (SYSTEM_BACKUP)
6.1.6.2.18 Tools Command Language (TCL)
6.1.6.2.19 Volume Manager (VOLUME MANAGER)
6.1.6.2.20 TELNET
6.1.6.2.21 File Transfer Protocol (FTP)
6.2 FUNCTIONAL AREAS UNDER THE HEWLETT PACKARD (HP) OPERATING SYSTEM
6.2.1 Force Development and Deployment
6.2.1.1 JOPES Planning and Execution Applications
6.2.1.2 Navy Reserve Unit Data Resource System (RUDRS)
6.2.2 Intelligence
6.2.3 Sustainment
6.2.4 Mobility & Survivability/Protection
6.2.5 Employ Forces/Firepower
6.2.5.1 Automated Message Handling System (AMHS)
6.2.5.2 Common Operational Picture (COP)
6.2.6 System Administration Tools
6.2.6.1 GCCS Tools
6.2.6.1.1 GCCS Security Tools
6.2.6.2 DII COE Tools
6.2.6.2.1 Database Tools
6.2.6.2.2 Security Tools
6.2.6.2.3 Web/Teleconferencing Tools

6.2.6.2.4 Network Administration Tools
6.2.6.2.5 Office Automation Tools
6.2.6.2.6 Unified Build (UB)
6.2.6.2.7 File Transfer Protocol (FTP)
6.2.6.2.7 Motif 1.2.4
6.2.6.2.9 DII COE Remote Installer
6.2.6.2.10 Joint Mapping Tool Kit (JMTK)
6.2.6.2.11 Mail Services
6.2.6.2.12 X-Windows
6.2.6.2.13 Printer (PRINTER)
6.2.6.2.14 Point-To-Point Protocol (PPP)
6.1.6.2.15 PERL (PERL)
6.3 FUNCTIONAL AREAS UNDER THE NT OPERATING SYSTEM
6.3.1 Force Development and Deployment
6.3.1.1‘ JFRG II
6.3.1.2 Smart Thin Clients
6.3.2 Intelligence
6.3.3 Sustainment
6.3.4 Mobility & Survivability/Protection
6.3.5 Employ Forces/Firepower
6.3.5.1 Common Operational Picture (COP)
6.3.6 NT System Tools
6.3.6.1 GCCS Tools
6.3.6.2 DII COE Tools
6.3.6.2.1 Database Tools
6.3.6.2.2 Security Tools
6.3.6.2.3 Web/Teleconferencing Tools
6.3.6.2.4 Network Administration Tools
6.3.6.2.5 Office Automation Tools
6.3.6.2.6 DII COE Kernel
7.0 OPERATIONAL EMPLOYMENT
7.1 OVERVIEW
7.2 DELIBERATE PLANNING
7.2.1 JOPES AUTOMATED DATA PROCESSING (ADP)
7.2.2 GSORTS
7.2.3 E-MAIL, FTP
7.2.4 RESOURCE AND UNIT MONITORING
7.3 CONVENTIONAL PLANNING AND EXECUTION
7.4 CRISIS ACTION PLANNING (CAP)
7.4.1 TELECONFERENCING
7.4.2 COA Time-Phased Force and Deployment Data (TPFDD)s
7.4.3 COP
8.0 SUMMARY

**Executive Summary**. GCCS 3.0 will provide increased reliability, stability, and performance, and will extend support for NT platforms and web browser-based access. It also becomes the first major program to fully implement the concept of the DII COE. The DII COE will replace the GCCS COE used in GCCS 2.2 and earlier versions.

**1.0 Introduction.** This Functional Description (FD) document describes the functional capabilities of the Global Command and Control System (GCCS) version 3.0, providing users with a high level description of how GCCS can be used to support the warfighter.

**2.0 Background.** GCCS is a program designed to implement the concept of C4IFTW to provide critical automation capabilities to the Joint Staff (JS) and warfighting Commanders in Chief (CINCs). GCCS version 3.0 implements DII COE version 3.1. It is an incremental step in ultimately satisfying the requirement of the Joint Staff, CINCs, and Services for a single Department of Defense (DOD)-wide suite of integrated C2 information systems. The use of the DII COE will eventually allow users to host GCCS or Global Combat Support System (GCSS) applications on the same platform, eliminating the need for a separate hardware platform for C2 and combat support functions.

**3.0 Reference Documents**

The following documents were used to develop the GCCS 3.0 Functional Description:

- US GCCS User Concept of Operations (CONOPS), 1 December 1995.
- GCCS Common Operating Environment Requirements, 15 August 1994.
- GCCS Operational Evaluation Master Plan, 7 December 1995.
- GCCS Operational Evaluation Plan, 7 March 1995.
- [JS] J33 Message RUEKJCS6229 252148Z AUG 95.
- GCCS Joint Integrated Logistics Support Plan, 30 September 1995.
- GCCS Version Description Document for Version 2.2, 11 December 1996.
- DII COE Integration and Run-Time Specification, Draft, 1 January 1997.
- MIL-STD-498, Software Development and Documentation, 5 December 1994.
- JOPES Software Users Manual: JOPES Users Guide, 18 August 1995.
- OSF GCCS Software Segment Information Files, December 1996.
- Netscape News Server 2.01 Data Sheet, Netscape Communications Corporation, 1997.
- CONOPS for GCCS Common Operational Picture (COP), COP Working Group, 14 April 1997.

**4.0 General Operational Requirements.** The GCCS User CONOPS document defines eight objectives for GCCS. These objectives, considered as operational requirements, are to:

- Be configurable to achieve optimum crisis response.
- Support unity of effort and command dominance.
- Support deliberate and crisis action planning.
- Provide for joint TPFDD development and updating.
- Provide the Commander, Joint Task Force (CJTF), with global access to current intelligence and tactical information in support of joint and coalition missions.
- Support decision and execution cycles faster than those of the enemy.
- Provide interoperability for joint and multinational force C2 systems.
- Facilitate use of commercial off-the-shelf (COTS) products.

**5.0 System Constraints**. As an upgrade to an operational system, GCCS 3.0 must not degrade current levels of performance or functionality. Transition to version 3.0 (detailed in the GCCS Transition Plan) must not involve an unacceptable amount of downtime for the sites.

**6.0 Functional Capabilities**. The functional capabilities and the GCCS applications attributed to each capability below are not absolute. Many other mission area definitions and functional partitions can be used and many GCCS applications may contribute to several functional areas. The descriptions below are intended to show the utility of selected GCCS applications in the given C2 construct. Nor is the list exhaustive. A complete list of GCCS 3.0 Build segments is dynamic. Additional current information on GCCS 3.0 segments can be found on the GCCS Home pages.

### 6.1 Functional Areas Under the Sun Solaris UNIX Operating System

#### 6.1.1 Force Development and Deployment

##### 6.1.1.1 Joint Operation Planning and Execution System (JOPES)

JOPES contains a variety of applications used for deliberate and crisis planning, as well as controlling execution of joint operations. GCCS 3.0 will allow users to navigate among the various JOPES applications using the JOPES Navigation (JNAV) graphical interface. JNAV allows users to easily start GCCS applications and switch between them. The JOPES applications are described below. In the descriptions below, "OPLAN" refers to OPLAN-related data in the JOPES database which includes TPFDD data.

#### 6.1.1.1.1 GCCS Synchronization Tool (SYNCTOOLS)

The Synchronization Tool is intended for use at the National Military Command Center (NMCC). The tool provides visibility of the synchronization status of requirements information (Time-Phased Force Deployment Data) within the network of GCCS JOPES databases worldwide.

#### 6.1.1.1.2 Reference File Manager (RFM)

RFM is a TIP software package that has been incorporated into GCCS. The RFM is a tool used to download standard reference files such as ASSETS, CHSTR, TUCHA, GEOFILE, etc., from the mainframe of the GCCS server. The RFM application is initiated by operator action to download Reference Files from the WWMCCS mainframe to the various TIP applications.

#### 6.1.1.1.3 Real Property Inventory

Real Property Inventory (RPI) is a subsystem of the Joint Engineering Planning and Execution System (JEPES) that processes real property asset information from the Services. RPI validates the Service data, converts Service category codes to DOD standard facility category codes, aggregates the quantities by category code and location, and provides an Oracle export file of combined assets for use by all JEPES sites. RPI allows users to extract engineering asset information from the JEPES Combined Asset file. Errors can then be corrected. JS Directorate for Logistics staff are the primary users of RPI.

#### 6.1.1.1.4 Ad Hoc Query (AHQ)

AHQ is part of the Scheduling and Movement (S&M) application. AHQ allows Operations Plan (OPLAN) end users to query S&M on scheduling and movement requirements for a given OPLAN. A toolkit allows users to build queries and reports, thus minimizing the need for specialized knowledge of the database. For GCCS 3.0 AHQ will support a new web-browser front end, greatly enhancing the simplicity and familiarity of database queries.

#### 6.1.1.1.5 Ad Hoc Query Character (AHQCHAR)

AHQCHAR is the client/server replacement for JOPES Subsystem E. This character-based segment of S&M is called by a remote machine, such as a remote PC or SPARCstation , for execution over a small bandwidth serial or satellite line.

#### 6.1.1.1.6 External System Interface (ESI)

The ESI application comprises the Transportation Component Command (TCC) ESI for the migration of JOPES validation functionality to GCCS. The ESI provides an interface between JOPES and the software systems of the TCC for the United States Transportation Command (USTRANSCOM). This software provides users with the capability to identify and manage the force requirements that should be scheduled for transportation. Depending on the characteristics of the users' access userid, ESI provides specific functional access for users in the Commander-in-Chief (CINC) Site Validator, USTRANSCOM, Air Mobility Command (AMC), and Military Sealift Command (MSC) user classes.

#### 6.1.1.1.7 GSORTS Oracle Server (GORA)

GSORTS Oracle Server, segment creates the ORACLE table space, GSORTS_DATA to allow creation of the Status of Resources and Training System (SORTS) table definitions. ORACLE constraints, views, and indexes are also created during installation of this segment. The segment provides the structure for GSORTS Update engine from GUPD segment and General Interactive Query System (GIQS) from GSORTS segment. The segment is part of the Global Command and Control System (GCCS) Oracle database. The ORACLE database manager should grant SORTS access to only authorized users.

#### 6.1.1.1.8 Global Status of Resources and Training System (GSORTS)

GSORTS is an output application providing general service data, basic identity information (including unit location) on all units and resource status of operational units listed on TPFDDs/TPFDLs. It is the central registry of all units. Unit location can be plotted onto DMA digital map products. GSORTS currently has all Joint data elements and service-unique elements. GSORTS' Generalized Interactive Query (GIQ) allows data retrieval by a series of user-defined SQL type statements.

#### 6.1.1.1.9 GSORTS Update Engine (GUPD)

This segment is an aggregate segment to the GORA segment. GUPD 3.0 SORTS Update Engine segment loads the Status of Resources and Training System (SORTS) reference and lookup tables in the Global Command and Control System (GCCS) ORACLE database. The update portion processes United States Message Text Format (USMTF) information to update the SORTS portion of the GCCS database at any site and provides the ability to reload the SORTS portion of the GCCS site from another GCCS site. The ability exists to do counts of the SORTS update, reference and lookup table contents. The primary user is GSORTS Operations at the Pentagon. GSORTS Operations receives USMTF traffic from GCCS Automatic Message Handler and processes for distribution to the GCCS sites. The segment connects to GORA table definitions through the ORACLE LISTENER.

**6.1.1.1.10 GSORTS World Data (GWORLD)**

GSORTS World Data, segment contains the Defense Mapping Agency vector map files for use with the GSORTS application. The Maps provide additional features and detailed scaling as the user zooms into the map. Map details and features may be modified using the GSORTS application segment. Boundaries, rivers, roads, ports, cities, and labels appear as the maps expand. The maps are used as background for overlaying Status of Resources and Training System (SORTS) location data.

**6.1.1.1.11 JOPES Oracle PDRPT (JOPES ORA PDRPT)**

The JOPES_PDRPT database segment (JOPES_ORA_PDRPT) is necessary in order to create an application specific schema which supports the processing of report data and to grant select privileges to various table_master tables.

**6.1.1.1.12 JOPES Pre-Defined Reports (PDRPT)**

The JOPES PDRPT required for migration to GCCS are delivered in six sets. The reports access the S&M GCCS Core Database via the JOPES navigation segment and are dependent on that segment. The PDR product includes:

- Client application software segment for user interface and report generation;

- Database server segment used to create tables, views, and roles required to operate JOPES; reports;

- Database server segment for Gain Momentum Net Daemon needed to access the JOPES Core; and

- Database from user interface.

**6.1.1.1.13 JOPES System Level Navigation**
JOPES consists of a number of applications that are traditionally divided into three categories: Requirements Planning and Execution, Deliberate Planning tools, and Functional Management. The application described manifests itself as an icon on the desktop. Opening the JOPES icon brings up a window pre-loaded with a form provid ing instructions to launch the application. The JNAV Client Segment consists solely of H yperText Markup Language (HTML) documents and UNIX scripts.

**6.1.1.1.14 Information Management Subsystem (IMS)**
IMS is a tool for centralized management of TPFDDs. IMS can move and translate TPFDD information between the various GCCS applications and databases.

**6.1.1.1.15 Joint Engineer Planning and Execution System (JEPES)**
JEPES provides GCCS users with a capability to determine requirements and adequacy of engineering support provided in OPLAN courses of action (COAs). JEPES allows planners to develop the Civil Engineering Support Plan (CESP) for an OPLAN. Using pertinent TPFDD data, JEPES can compute facility requirements and determine if adequate facilities exist to support deployed forces.

**6.1.1.1.16 Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE)**
LOGSAFE uses logistics related attributes, such as unit consumption factors, to calculate time-phased requirements for non-unit related supplies. LOGSAFE can also receive data from the Joint Engineer Planning and Execution System (JEPES. Strategic movement requirements can be grouped to optimize transportation needs.

**6.1.1.1.17 Predefined Reports (PDR)**
PDR provides users with a report generation capability that supports planners in determining force and non-unit requirements during deliberate or crisis action planning. PDR allows users to analyze COAs in relation to asset allocations and TPFDD modifications.

**6.1.1.1.18 Requirements Development and Analysis (RDA)**
RDA allows editing of TPFDDS and graphical analysis of COAs with respect to TPFDD modifications. RDA also provides a capability for creating and modifying force and non-unit requirements associated with OPLANs.

**6.1.1.1.19 Reference File Administration (RFA)**
RFA is used in a centralized location by database analysts to accept Joint Reporting Structure (JRS) input transactions and update reference files.

**6.1.1.1.20 Scheduling and Movement (S&M)**
S&M handles C2 information on deployment activity and status. S&M tracks and reports on TPFDD requirements. S&M allows GCCS users to work with Transportation Component Command (TCC) carrier and organic movement data before and during deployment. S&M can provide carrier support for more than one OPLAN. S&M allows user Ad Hoc Queries (AHQs).

**6.1.1.1.21 Scheduling and Movement Interface (SMINT)**
SMINT provides external systems with an interface to the S&M Client/Server (C/S) system. This interface provides the Global Transportation Network (GTN) with a means through which it can pass transportation data to the C2 and in transit visibility segments of S&M.

**6.1.1.1.22 System Services Client (SSC)**
(SSC) is the Client software that enables System Services to be run remotely from a client machine. SSC runs on a local Client, providing access via a remote shell to the System Services portion of the Scheduling and Movement segment running on the Database Server. A launch button is provided on the local client to initiate SSC.

**6.1.1.1.23 Transportation Component Command External System Interface (TCC ESI)**
TCCESI allows users to identify source requirements for validation and scheduling of movement assets. Transportation relevant data elements can be protected once an OPLAN is locked. The supported CINC can invalidate previously validated.

**6.1.1.1.24 External Transaction Processor (XTP)**
The XTP segment is designed to support transaction processing on a machine running System Services without the S&M program loaded. This requirement supports execution of other GCCS segments such as RDA.

**6.1.1.1.25 Non-Unit Personnel Generator (NPG).**
NPG allows the planner to generate Personnel Increment Numbers (PINs) through the construction of TPFDD records. The planner will incorporate the PINs into OPLAN movement requirements as the basis for lift analysis and allocations.

**6.1.1.1.26 Airfields**
Web based Airfields provides GCCS users with comprehensive information on over 40,000 free world airfields. This information is supplied by the National Imagery and Mapping Agency (NIMA). Reports provide one line summaries for each listed airfield. The database is updated monthly.

**6.1.1.1.27 AirFields Remote (AFSC)**
The AirFields application provides information on airfields worldwide. This segment contains a script to launch the AirFields application in a Remote Shell (RSH) running on the application server.

**6.1.1.1.28 Web Based Ad Hoc Query (DARWIN)**
Provides web based front end query capability for Scheduling and Movement database queries.

**6.1.1.2 Evacuation File Maintenance and Retrieval System (EVAC)**
EVAC is a JS and State Department automated computer database and retrieval system used to identify the number of potential evacuees located at each reporting foreign service post worldwide. Retrieval is allowed by country and districts within a country. Information is received from "F77" reports from the AMHS.

**6.1.1.3 Joint Planning and Execution Toolkit (JPET)**
Provides for a combination of Advanced Concept Technology Demonstration (ACTD) applications that dramatically improve crisis management planning capabilities.

**6.1.1.3.1 Enhanced Theater Analysis and Replanning Graphical Execution Toolkit (TARGET)**
Theater Analysis and Replanning Graphical Execution Toolkit (TARGET)/DCP aids the planner in all phases of crisis action planning, including Situation Assessment and Development, Course of Action (COA) Development and Selection, Execution Planning, and Execution. It facilitates simultaneous access to a distributed network of graphic planning cells sharing a common reasoning infrastructure. These tools facilitate rapid planning and COA development and analysis among the

Joint Planning and Execution Community (JPEC) sites in a distributed, collaborative mode. This enables current assessment of plan generation, scheduling, and analysis processes between the Joint Staff, supported and supporting CINCs, their components and the deployed JTF.

TARGET and DCP together comprise a system of software applications and tools that can be applied to operational, crisis action planning. TARGET is designed as an object-oriented system comprised of various tools to assist in crisis planning and to stimulate user ideas and creativeness. TARGET supports:

- Operational Planning Team
- Deployment Management Team
- Logistics Readiness
- Joint Intelligence
- Supporting Commands
- Service Components.

The TARGET Workbench has a medical forms tool to plan, organize, and provide deliveries to medical teams. TARGET and DCP are associated with the Integrated Feasibility Demonstration (IFD), and support the Advanced Research Projects Agency (ARPA) and Rome Laboratory Planning Initiative (PI).

**6.1.1.3.2 Force Module Edit (FMEDIT)**
Provides the user with ability to manipulate TPFDD force modules. Generates force "capability sets" for initial deployment analysis.

**6.1.1.3.3 TPFDD Edit (TPEDIT)**
Provides TPFDD development and analysis capability. Replaces DART version currently on GCCS.

**6.1.1.4 Transportation Component Command External System Interface (TCCESI**). TCCESI will be used for the migration of JOPES validation functionality to GCCS. The ESI provides an interface between JOPES and the software systems of the TCC for the USTRANSCOM.

**6.1.1.5 Navy Reserve Unit Data Resource System (RUDRS)**

RUDRS provides an automated means through which the Commander, Naval Reserve Force (COMNAVRESFOR) can provide Naval Reserve Force (NRF) unit data to Fleet Commanders in Chief (FLTCINCs) for reserve commissioned and reserve augmentation units to use in both deliberate and crisis action planning. RUDRS accepts data maintained in the COMNAVRESFOR Reserve Training Support System (RTSS) and makes that NRF data available via a database structure. It provides an automated means of updating JOPES TPFDD files with Naval Reserve data to source OPLANS. The interface provides the capability for FLTCINCS to generate Reserve Geographic Location (GEOLOC) and type-unit characteristics (TUCHA) files for NRF data validation.

#### 6.1.1.6 Global Transportation Network (GTN)

GTN provides a communications interface based on the HYPERchannel NETwork Executive (NETEX) application program. GTN is a transportation system and a command and control system that provides the JS and CINCs with transportation information. It provides a transaction-oriented, event-driven, data transfer capability. It focuses on providing the United States Transportation Command (USTRANSCOM) with the information necessary to carry out its mission of global transportation management.

### 6.1.2 Intelligence

#### 6.1.2.1 Global Reconnaissance Information System (GRIS)

GRIS provides automated support planning, scheduling, reporting, and monitoring of reconnaissance activities under the Sensitive Reconnaissance Operations (SRO) program. GRIS maintains a near real-time status of all SRO missions and provides immediate on-line retrieval of mission, track, and message data. To accomplish this, GRIS provides automatic real-time capture and processing of Reconnaissance Information Processing System (RIPS) format messages, and maintains a mission and track database containing schedule and resultant information. GRIS is used to generate and release outgoing SRO messages to AUTODIN and provides on-line query and report capabilities detailing message, mission status, and scheduling information. It is also used to maintain current track dictionary data and to generate the master copy of each new dictionary or set of change pages.

#### 6.1.2.2 Joint Deployable Intelligence Support System (JDISS)

JDISS provides connectivity and interoperability with the intelligence systems required to support forces in garrison and deployed in peacetime, crisis, and wartime. It provides the Joint Intelligence Center

(JIC), Joint Task Forces (JTF), and operational commanders with on-site automation support and the connectivity necessary to execute the intelligence mission. It is the technical baseline for the DoD Intelligence Information System (DoDIIS) client/server environment.

#### 6.1.2.3 Modernized Integrated Database/Image Product Archive/GCCS (MIG)

Modernized Integrated Database (MIDB) Imagery Product Archive/ Imagery Product Library for GCCS (MIG): MIG provides near real time display of the locations of friendly, neutral, and enemy ground, maritime, and air units on a map on a GCCS terminal with applicable overlay enhancements. The integration of C4I systems into the GCCS common operational picture provides the CJTF, components, theater CINC, and supporting forces with a common awareness of the JTF area of responsibility. Commanders see representations of the data and can support mission execution without requesting situational information. The MIG application for GCCS consists of 26 segments.

##### 6.1.2.3.1 Automated Image Import Module (AIIM)

The mission of the Automated Image Import Module (AIIM) is to provide automated services for importing imagery from local and remote file systems into the ITS Server and to provide management of the ITS Server search profiles and standing queries. AIIM provides an automated ability to import imagery from various sources, such as GBS/JBS broadcast, into the ITS Server, to maintain a log of the received data, and to optionally notify the user when new data is received. AIIM also provides the ability to configure and manage the retrieval of imagery from remote servers such as IPA/IPL by providing set-up tools for the ITS Server data search profiles and standing queries. AIIM includes a specialized interface for Netscape image import to optionally import imagery downloaded to the ITS Server.

##### 6.1.2.3.2 ICS (ICS)

The mission of the ICS Client is to provide a user application for sending and receiving imagery over synchronous and asynchronous communication channels. The ICS client provides the ability to disseminate imagery which is stored on the ITS server using the TACO2 protocol and to push imagery which is received via TACO2 into the ITS server.

##### 6.1.2.3.3 Image Composition Tool (ICT)

This Image Composition Tool provides the imagery user with the ability to create and manipulate National Imagery Transmission Format imagery.

Users can pull in multiple images and chips, move them around, and add annotations and symbols for producing a final imagery product.

#### 6.1.2.3.4 Image Exploitation Services (IES)

The mission of the IES is to provide the image analyst with advanced imagery exploitation capabilities. The IES application provides the ability to display, manipulate, enhance, and register imagery. IES can display and process any size image up to and including NITF Level 6.

#### 6.1.2.3.5 Image Manager (IMGR)

The mission of the IMGR tool is to provide the capability to integrate imagery into the Joint Mapping ToolKit (JMTK). The analyst can use Image Manager to query ITS for all of the images that are within the current area of the world that JMTK is focused on. The analyst can then display a footprint on JMTK of where the selected images would be located and then finally the analyst can have Image Manager draw the selected images onto the JMTK map.

#### 6.1.2.3.6 Imagery Product Archive (IPA)

The purpose of the IPA program is to establish standard servers in all theaters that can obtain and archive imagery files and/or imagery products from multiple sources. These files and products are then made available to imagery customers throughout the world. The mission is expanding to include the storage of maps and video files as well. IPA servers are currently on-line in several theaters. These servers can be accessed from clients anywhere in the Wide Area Network (WAN) using this segment. The IPA program provides both the server and client software necessary to implement the IPA mission. The Joint Deployable Intelligence Support System (JDISS) Program Management Office (PMO), which is a "clearing house" of integrated intelligence applications, currently packages the IPA Client to operate successfully in joint systems that have an intelligence mission. To date this includes JDISS itself, COP, and GCCS.

#### 6.1.2.3.7 Image Print Services (IPS)

The mission of the Image Print Services(IPS) is to provide an image printing capability and a standard interface for accessing image from the ITS server catalog and to print the image on a Kodak high resolution imagery printer, or on a plain paper Laser-Jet printer. Also noteworthy for this release is the ability to print color images to the Kodak printers provided that color print cartridges are installed in the printer.

#### 6.1.2.3.8 Image Transformation Services (DPSSRV)

The mission of ITS is to provide archiving, cataloging, and retrieval of digital products and related data. ITS is a scalable client/server based system. The ITS Segment provides a client interface to other segments which allows data entry, catalog query/selection, and data retrieval. Additional functions provided by ITS include file format translations, image scaling, and backup/restore.

#### 6.1.2.3.9 Image Viewer (IVWR)

The mission of the Image Viewer (IVWR) is to provide a basic image viewing application for all imagery users. IVWR provides the ability to display any image cataloged by the ITS Server and to perform simple image manipulations such as magnify, filter, and adjust brightness/contrast. IVWR does not allow modification of the original imagery file, only the displayed data.

### 6.1.2.4 Meteorology and Oceanography (METOC)

METOC applications will provide capabilities to obtain meteorological and oceanographic data for joint operations. Information on ocean currents, seawater temperatures, rainfall, storm locations, typhoon and hurricane prediction data, drought prediction data, and other weather-related phenomena will permit better scheduling and afford greater precision in decisions affecting transportation and deployment of forces.

### 6.1.2.5 Naval Intelligence Processing Services (NIPS)

The NTCS-A Intelligence Processing Services segment (NIPS) allows analysts to access a world-wide intelligence database for retrieval of military intelligence data. The database of information can be accessed directly by other segments or by user query from a workstation using NIPS applications.

#### 6.1.2.5.1 Naval Intelligence Processing Services (NIPS) (SINBAD)

NIPS SINBAD enables the operator to access any data contained in the Naval Intelligence Database (NID) by using real-world relationships between objects rather than requiring a user to know exactly where the data is located within the database structure. In future versions, SINBAD will be able to query from all databases.

#### 6.1.2.5.2 NID Editors (NID)

Primary entities available are aircraft, helicopters, missiles, merchant ships, ship classes, and submarine classes.

#### 6.1.2.5.3 NIPS System Administrator Applications (NIPSSA)

The NTCS-A Intelligence Processing Services (NIPS) System Administrator Applications segment (NIPSSA) provides software that controls and maintains certain NIPS functions such as profiling and message catalogue access. NIPSSA applications also include database backup and restore functions used to manage the Central Database Server (CDBS) data. NIPS also provides applications to view and manipulate system error logs and maintain GCCS analyst message privileges.

#### 6.1.2.5.4 NITF Services (NITFS)

The mission of the NITF Services is to supply a standardized set of software libraries which can be used by imagery applications for processing NITF formatted imagery files. The NITF Services libraries include tools to parse an NITF file into its components, as well as to assemble a valid NITF file from individual components. Tools are also provided to access, edit, create, and delete each component of an NITF file.

#### 6.1.2.6 StrikePlot (STRIKE)

The STRIKE segment allows graphical plotting and geographical display of national and tactical land pictures by bringing together NTCS-A Intelligence Processing Services (NIPS) site/unit data, Tactical Data Base Managers (TDBM) wet or dry track data, and ELINT data. STRIKE provides GCCS with geographical land displays and easy access to information associated with land displays. When combined with other GCCS tools, STRIKE is designed to assist force projection, strike planning, and intelligence/threat analysis.

#### 6.1.2.7 Coliseum (COLSM)

This is a client/server database application designed to support the national intelligence community for the registration, validation, tracking, and management of crisis and non-crisis intelligence requirements. It was developed with COTS technology to provide a GUI for interaction with the database host at Defense Intelligence Agency (DIA). Control functions and relational features are built-in to provide automatic checks and data element field completion. Specific functional requirements and data element descriptions leading to product delivery are listed in the COLISEUM Requirements Definition Document (RDD).

### 6.1.3 Sustainment

#### 6.1.3.1 Joint Personnel Asset Visibility (JPAV)

JPAV is an application from the Global Combat Support System (GCSS) that integrates and analyzes Joint and service-specific processes and data requirements relating to force conversion, mobilization, deployment,

and sustainment operations in support of Joint Task Forces. JPAV functionality includes tracking of military personnel movements into, within, and out of the area of operations. The client portion of this application will be included in GCCS 3.0 to allow users to access functionality hosted on JPAV sources.

#### 6.1.3.2 Joint Total Asset Visibility (JTAV)

JTAV is an application from the GCSS. The client portion of this application will be included in GCCS 3.0 to allow users to access JTAV functionality. JTAV is used by logistics asset managers to retrieve logistics information on joint force resources and status. JTAV contains general supply assets data, including petroleum, oils, and lubricants (POL), supplies, transportation, requisition status, war reserves, unit equipment, bulk fuel, and munitions. JTAV receives information from a variety of sources.

### 6.1.4 Mobility & Survivability/Protection

#### 6.1.4.1 Theater Ballistic Missile Defense (TBMD)

TBMD provides capability for monitoring the launch, detection, trajectory tracking, and dynamic display of TBMD events. I t allows the operator to display TBM launch points, view tracks with time-to-impact information, and produce and further display TBM tactical information that is needed for related defensive or mission-critical uses.

#### 6.1.4.2 TBMD Shared Early Warning (TSEW)

The TSEW (Theater Ballistic Missile Shared Early Warning) segment provides Ballistic Missile Launch alert, launch point plotting, and projected point of impact plotting for US Allies. It is currently loaded onto GCCS 2.2 suites, and it requires full up UB/COP functionality be present on the machine that it is loaded on. Certain data feeds (TRE) are required in order for alerts to occur.

### 6.1.5 Employ Forces/Firepower (Common Operational Picture)

#### 6.1.5.1 Automated Message Handling System (AMHS)

The GCCS AMHS provides GCCS users with the capability to receive (via profiles) and transmit with Automatic Digital Network (AUTODIN) messages. AMHS also supports the ability to automatically update various databases based upon formatted AUTODIN messages.

#### 6.1.5.2 Common Operational Picture (COP)

GCCS can display a wide variety of C4I data on the standardized mapping packages provided in the DII COE. The Unified Build (UB) component of the DII COE provides correlation and display of near real-time and data linked air, land, and sea tracks. These tracks overlay National Imagery and Mapping Agency (NIMA) raster and vector maps to display a COP.

##### 6.1.5.2.1 Common Operational Picture Time Sync (COP_TIME_SYNC)

The Common Operational Picture (COP_TIME_SYNC) is a segment originally developed for the Global Command and Control System (GCCS) Version 2.2, running Unified Build (UB) Version 3.0.1.6G. The COP_TIME_SYNC segment allows participating nodes to synchronize their system times.

##### 6.1.5.2.2 Global Positioning System (GPS) Time

GPS_TIME is a segment developed for the Global Command and Control System (GCCS) Version 2.2, running Unified Build (UB) Version 3.0.1.6G. The GPS_TIME segment provides the capability for a SPARC SunStation computer running Solaris Version 2.5.1 to keep its system time in sync with the time from a Global Positioning System (GPS) receiver.

##### 6.1.5.2.3 Tactical Information Broadcast Service (TIBS)

The Tactical Information Broadcast (TIBS) segment allows for the parsing of the Tactical Information Broadcast (TIBS) by COP machines. When coupled with its classified counterpart, it allows for the reception of amplifying track data that is transmitted on the TIBS.

##### 6.1.5.2.4 TACCIMS Interface

Interface to receive GOB data from USFK TACCIMS system and interject info into COP.

##### 6.1.5.2.5 CRESP Interface

CRESP interface is a means to receive ground order of battle from the NATO Crises Response Program. Data is transmitted from CRESP to GCCS and is then displayed in COP.

##### 6.1.5.2.6 TADIL B Interface

Provides receive-only tactical communications for TADIL data.

##### 6.1.5.2.7 PLRS/EPLRS Interface

Provides receive-only tactical communications capability for PLRS/EPLRS data.

**6.1.5.2.8 Enhanced Linked Virtual Information System (ELVIS)**
ELVIS uses Hyper-Text Transfer Protocol (HTTP) to service client requests for GCCS/COP Chart images, as well as links into Status of Forces data, where available. A CERN HTTPD process is installed to act as the server for this data; it can live on a workstation running other HTTP servers without conflict. ELVIS provides the capability to view COP displays from any computer SIPRNET device with a World Wide Web (WWW) browser. ELVIS incorporates corrected file ownership settings into the Postinstall script to ensure that owner COP is set on almost all files and subdirectories.

**6.1.5.3 Air Tasking Order (ATO) Review Capability**
The ATO Plus feature in GCCS' COP software and the GCCS ATO Read-Only Capability (GARC) both provide flexible capability to receive and view U.S. Message Text Format (USMTF) ATO Confirmation (ATOCONF) messages disseminated by the Contingency Theater Automated Planning System (CTAPS).

**6.1.5.4 Theater Battle Management Core Systems (TBMCS)**

**6.1.5.4.1 Rapid Application of Air Power (RAAP)**
Provides targeting capabilities for air battle planners (compares target nomination list to weapons options and facilitates target development). Used in a stand-alone mode today by individuals within JTFs/JFACCs.

**6.1.5.4.2 Joint Planning Tool (JPT)** Provides an independent capability for senior combat leaders to conduct initial planning essential to running the air campaign by automating the capability to plan an air campaign from strategy to task. JPT selects subsets of targets which must be hit based on a specific strategy.

**6.1.5.4.3 Air Tasking Order Read, Distribute, and Print (ARDP)**
Provides capability to Read, distribute, and print. Can access the ATO from GCCS.

**6.1.5.4.4 Computer Assisted Force Management Structure (CAFMS-X)**
Provides ATO dissemination, execution, and monitoring capability. Allows manipulation of the ATO (i.e., parse by unit, equipment type, etc.)

**6.1.5.4.5 TASKVIEW**
Translates standard ATO (AUTODIN message text format) into a more 'user friendly' ATO format that can be read like a word document.

## 6.1.6 System Administration Tools

### 6.1.6.1 GCCS System Tools

**6.1.6.1.1 Security Tools** Security Tools will be needed to maintain protection from hackers and malicious code. The use of browser, Internet Chat, and other Internet services will be increasingly important during deliberate and crisis action planning. Distributed communications/computing requires a robust array of security mechanisms to protect data throughout the exchange, and to prevent virus introduction into databases. GCCS 3.0 will include enhanced security tools to aid in data protection and to aid in maintaining overall security of the GCCS.

**6.1.6.1.1.1 Computer Misuse Detection System (CMDS)**
CMDS provides the capability to program patterns of behaviour and identify the patterns to possible suspicious activity on computer system platforms and across platforms on a network. User activities may be tracked pinpointing access times, objects accessed, and processes invoked. The CMDS and Stalker products provide similar functions though through different implementations. Both products are available for the choosing by the GCCS site.

**6.1.6.1.1.2 Stalker** Like CMDS, Stalker also provides a capability to program patterns of behaviour and identify the patterns to possible suspicious activity on computer system platforms and across platforms on a network. Also like CMDS, user activities may be tracked pinpointing access times, objects accessed, and processes invoked.

**6.1.6.1.1.3 Secret Agent** Provides a software implementation of public key based encryption protection for information stored in or transmitted between cooperating users.

**6.1.6.1.1.4 Security Monitoring and Reporting (SeMoRe) Tool**
The Global Command and Control System (GCCS) Security Monitoring and Reporting (SeMoRe) tool provides functions and procedures to monitor and report the security relevant configuration details on a UNIX platform file system. The SeMoRe tool examines and reports on the

configuration items identified in the DII COE Version 3.1 Security Checklists and as well as specific items identified in the GCCS Security Policy and Requirements.

**6.1.6.1.2 WIKI WIKI**

WIKI WIKI will provide the functoinality previously provided by the Run Remote RREM segment, which allow users to remotely execute selected applications. Run Remote used Executive Manager whic his not used in GCCS 3.0.

**6.1.6.1.3 Legato (LGTO) Networker**

The Legato Networker segment is a COTS product. It provides an open solution to software backups, including database backups. This software package is designed for installation on application/database servers and clients that require backup to the tape device controlled by the tape server. A separate segment, Legato Networker Server, is designed to run on tape servers only and provides the backup facility for this client segment.

**6.1.6.2 DII COE Tools**

**6.1.6.2.1 Database Tools**

**6.1.6.2.1.1 Database User (DBUSER)**

This Database User Management Segment was designed as a "one-stop shop" for system administrators to add and remove GCCS Oracle Database User Privileges. This "master" script also verifies in one place the existence of the user (or users) and that they have (or do not have) the appropriate DB privileges.

**6.1.6.2.1.2 Character Based DB Select**

This segment allows character based users to select an Oracle database.

**6.1.6.2.1.3 Oracle**

Provides Relational Database capabilities.

**6.1.6.2.1.4 ORACLE Memory Config (ORASYS**)

This segment ensures that the shared memory is adequate for ORACLE.

**6.1.6.2.1.5 SYBASE (SYBASE)**

This SYBASE segment represents a repackaging of the original SYBASE segment released with GCCS Version 2.1.

**6.1.6.2.1.6 SYBASE Run-Time Client (SYBCLT)**
Sybase Run-Time Client segment (SYBCLT) is a COTS segment that provides the run-time files necessary for Sybase clients. This segment does not provide developers files and executables. The following SYBASE files are included in this segment: bin/bcp, bin/isql, bin/probe, bin/syman, and bin/interfaces. Also included in this segment is the interfaces.master file, which is used when the workstation is booted to create the interfaces file. During installation, all Accout Groups are updated to source in the .cshrc.SYBCLT file. All segments who require the SYBCLT segment must use the $SYBCLT_HOME environment variable to locate the interfaces file.

**6.1.6.2.2 Security Tools**

**6.1.6.2.2.1 Audit (AUDIT)**
The AUDIT segment replaces the Basic Security Module (BSM) segment. The BSM segment installs audit configuration and management files that are used by the auditing features provided in the UNIX operating system. This auditing feature allows the superuser to maintain audit trail information of user activities.

**6.1.6.2.2.2 BSM (BSM)**
This BSM patch segment allows for the audit trails on /h/data/global/EMDATA/auditlogs/all_hosts/files to remain intact when BSM segments or BSM patches are deinstalled and replaced by the AUDIT segment

**6.1.6.2.2.3 Security Compliance Tool (SeComp)**
SeComp provides functions and procedures to determine if, where, when, and how COE kernel function and application segments might be disruptive to a system security configuration. This tool is provided by the DII COE.

**6.1.6.2.3 Web/Teleconferencing Tools**

**6.1.6.2.3.1 Netsite**
A commercial product which, like Netscape, replaces WIN Teleconferencing functionality. It is the server segment of a client/server product communicating using TCP/IP protocols. Netscape and Netsite were acquired, modified, and configured from public domain sources.

**6.1.6.2.3.2 Freeware Implementation of UNIX Talk**

UNIX Talk (CHATTER) allows a GCCS user to communicate with another GCCS user in real-time. It allows connection between two users at a time, but both users must be using the GCCS desktop.

**6.1.6.2.3.3 HyperText Transfer Protocol Daemon (HTTPD)**
The NCSA HTTPD improves performance and corrects several security problems and flaws in the cgi scripts. The following directives have been added to the configuration files: Startserver, Maxserver, ErrorDocument, Agentlog, RefererLog, and RefererIgnore.

**6.1.6.2.3.4 Teleconferencing (TLCF)**
TLCF is provided to GCCS users by two applications having teleconferencing functions. A third application provides a World Wide Web information search and retrieval capability.

**6.1.6.2.3.5 Internet Relay Chat (IRC)**
IRC is a chatter style application that allows multiple users to participate in conferences. Several types of channels, with varying degrees of privacy, can be established.

**6.1.6.2.3.6 Internet News**
Internet News provides access to a bulletin board style broadcast service. Articles posted to the bulletin board are arranged by news groups. Various functions are supported, including the ability to trace a subject through a series of articles within a news group and send correspondence to article authors.

**6.1.6.2.3.7 World Wide Web (WWW)**
WWW browser service is provided through Netscape. The GCCS user may retrieve information through queries or links to other documents or web sites.

**6.1.6.2.4 Network Administration Tools**

**6.1.6.2.4.1 NETM Memory Config (NETSYS)**
The HP NetMetrix product consists of two parts. One is the remote monitoring Power Agent which implements all nine groups of the RMON MIB (RFC 1271) plus extensions. The other is the application toolbox which implements the graphical toolset consisting of the network load monitor, the network file system (NFS) monitor, the protocol analyzer, the traffic generator, and the internetwork monitor. Together, this package assists in monitoring the performance of your network segments (ethernet, FDDI, token ring), and troubleshooting network problems.

**6.1.6.2.4.2 NetMetrix (NETM)**
The HP NetMetrix product consists of two parts:

1. The remote monitoring Power Agent that implements all nine groups of the RMON MIB (RFC 1271) plus extensions.

2. The application toolbox that implements the graphical toolset consisting of the network load monitor, the network file system (NFS) monitor, the protocol analyzer, the traffic generator, and the inter- network monitor.

Together, these packages assist in monitoring the performance of the network segments (ethernet, FDDI, token ring, etc), and troubleshooting network problems reported to the GMC.

**6.1.6.2.4.3 Empire (EMPIRE**) EMPIRE, along with the other network monitoring agents, is designed to collect statistical data on the health and performance of GCCS servers and applications. The Host Resource MIB data collected will be analyzed and reported back to the originating sites in addition to the GMC to assist in troubleshooting and optimizing their local GCCS assets. Centralized data collection will allow the users to spot trends and patterns that are common across all GCCS sites and will serve as a conduit for the distribution of feedback and lessons learned at each site.

**6.1.6.2.4.4 System/Network MIB Sets**
Empire UNIX Systems Management Agent implements MIB-II (RFC 1213), Empire's UNIX Management Information Base (MIB), and the Host Resources (RFC 1514) MIB. The UNIX MIB defines groups for kernel and systems parameters, boot configuration, network, streams and I/O buffer statistics, kernel performance statistics, and an object monitoring table. The host MIB includes information on storage areas such as file systems and disk partitions, running and installed software, and the host system's devices, including the mentioned stations: keyboard, disks, and network cards. The agent enables remote Network Management Stations (NMS) to access important information such as metrics. The agent includes self-monitoring capability for exception reporting management that eliminates the need for excessive polling. The UNIX Systems Agent interoperates with platforms such as SunNet Manager and others. A daemon started at boot-up handles the trap forwarding to the management station.

The HP NetMatrix product consists of two packages or partitions:

1. The remote monitoring Power Agent, that implements all nine groups of the MIB (RFC 1271) plus extensions.

2. The application partition, (which implements the graphical toolset) consisting of the network load monitor, the NFS monitor, the protocol analyzer, the traffic generator, and the internet work monitor.

Together, these packages assist in monitoring the performance of the site's network segments (Ethernet, FDDI, token ring, etc), and troubleshooting network problems. The host is the application server system attached to the FDDI segment at the GCCS site.

Legent System Manager is a manager/agent software application that is used to monitor the availability and performance of multi-vendor, UNIX system resources distributed on a network. System Manager presents a management view of UNIX system resources that conforms to the Simple Network Management Protocol (SNMP). It is designed to extend the functionality of leading network management platforms by providing a view of critical components of UNIX system resources. The function of System Manager is to automatically discover, monitor, analyze, and display critical network management parameters.

### 6.1.6.2.5 Office Automation Tools

**6.1.6.2.5.1 Applix** Office Automation is supported by a suite of Applixware COTS products, including Applix Words, Applix Spreadsheets, Applix Mail, Applix Power Brief and Applix Ovation. The latter is a presentation application that communicates with DOS based systems. GCCS 3.0 will upgrade all existing Applix licenses to support the full range of Applix Office Automation (OA) capabilities on Solaris, HP, and NT platforms. It will also allow users in low-bandwidth locations to run OA applications from the web-browser.

**6.1.6.2.5.2 WABI Desktop (WABI)** The Windows Application Binary Interface (WABI) segment is a UNIX application that enables you to run Microsoft applications on a SUN platform.

**6.1.6.2.5.3 Windows Distributed Desktop (WinDD)** The WinDD client is installed on Sun SPARCstations and HPs. The WinDD client enables X-

terminals and other X-devices to access Microsoft Windows NT applications on a WinDD NT application server.

**6.1.6.2.6 Unified Build (UB)** The UB core software provides basic C4I services to receive and process messages, updates a track database, performs correlation and data fusion services, and displays the tactical picture.

**6.1.6.2.7 Joint Mapping Toolkit (JMTK)**
This segment provides basic UB mapping services, including the Chart, the Chart Menu bar, digital maps, overlays, and tactical geographic plotting. This capability is provided by the DII COE.

**6.1.6.2.8 Character Based Interface (CHARIF)**
This segment provides the ASCII desktop foundation allowing text-based segments to be loaded. Those segments then enable a remote site to connect via a low speed circuit to the server and execute the character based segments.

**6.1.6.2.9 MAILX For CBIF (MAILX)**
This segment allows user to access UNIX mail via GCCS desktop.

**6.1.6.2.10 Mail Services (MSVCS).**
MSVCS provides pop3 access to users' e-mail accounts. This allows users on networked PCS and workstations that do not mount /var/mail to read their e-mail.

**6.1.6.2.11 PERL (PERL)**
This segment is a powerful scripting language intended for use by system administrators.

**6.1.6.2.12 Printer (PRINTER)**
This is the Printer software for the JMCIS COE. It provides text and graphic printing capabilities for a number of printer types.

**6.1.6.2.13 Point-To-Point Protocol (PPP**)
The HP REMOTE ACCESS segment and the required PPP for HP segment are intended to run on an HP 712 with HPUX V9.0.7 operating system and GCCS COE installed. The PPP for HP segment contains installation scripts and PPP (Morning Star Technologies) software.

**6.1.6.2.14 Remote Access (REMOTE ACCESS)**
This segment was designed to support 'EM Client' and 'standalone' configurations.

**6.1.6.2.15 Remote Install (REMOTE INST)**

The Remote Install program is used to install a segment from a support facility to the machine at a remote site. A segment install file is transferred over the network, and then the segment or segments contained in that file are configured for the Segment Installer's "Installation Server" mode.

**6.1.6.2.16 Remote Printing (REMOTE PRINTING)**

The Remote Printing allows a character-based user to create setup, and select a printer for session use.

**6.1.6.2.17 System Maintenance (SYSTEM_BACKUP)**

This release of System Maintenance represents a total redesign of the System Backup segment. The segment is now self configuring, e.g. if the NIS+ server, Sybase server, EM server, or DNS server are changed the segment will automatically detect this the next time it runs. The amount of archiving done has been reduced to three days if a platform has been designated to do tape backups. If no tape has been designated as a tape backup platform no archiving will be done, except for Sybase (3days) and NIS+ (1 day).

**6.1.6.2.18 Tools Command Language (TCL)**

TCL is a scripting language and Tk is an X-Windows interface builder. They are used extensively by the JSIT Commands Application, by JOPES Navigation Application, and possibly others.

**6.1.6.2.19 Volume Manager (VOLUME MANAGER)**

This segment loads the SUN SPARCstorage array Volume Manager, version 2.1.1 and associated Solaris patches. It upgrades the firmware on the SPARCstorage Arrays to 3.9 and the firmware on the F/C card to 1.33. When installing the segment the Segment Installer will load the following 9 Volume Manager software packages:

- SUNWassa Using the SPARCstorage Array AnswerBook
- SUNWdiagp SPARCstorage Array Online Diagnostics Tool
- SUNWssadv SPARCstorage Array Solaris 5.3 Drivers
- SUNWssahd SPARCstorage Array Solaris 5.3 Header Files
- SUNWssamn SPARCstorage Man Pages

- SUNWssaop SPARCstorage Array Utility
- SUNWvmman SPARCstorage Volume Manager (manual pages)
- SUNWvxva SPARCstorage Volume Manager Visual Administrator
- SUNWvxvm SPARCstorage Volume Manager

In addition the following Solaris patches will be loaded:

- SUN Diag Patch
- SPARCstorage Array 1.0, 2.0, 2.1, 2.1.1:
- Jumbo patch for Solaris 2.3
- Point patch for Solaris 2.3 sd driver
- Disks program supports only 16 drives per controller

**6.1.6.2.20 TELNET**

TELNET provides the GCCS user with the ability to log in and use the application resources of any server across the network. The principal function of TELNET is to initiate text based or X-Windows applications, which, because of application design or security, must be executed from a specific server instead of from the users local hardware.

**6.1.6.2.21 File Transfer Protocol (FTP)**

FTP is used to directly control the transfer of files to and from a distant server. FTP is especially useful in transferring large files and is recommended when e-mail attachments exceed 500K bytes.

## 6.2 Functional Areas Under the Hewlett Packard (HP) Operating System

### 6.2.1 Force Development and Deployment

#### 6.2.1.1 JOPES Planning and Execution Applications

The JOPES applications listed below run on the HP platform. HP clients can also remotely execute JOPES applications provided under the Sun Solaris operating system. JOPES contains a variety of applications used

for deliberate and crisis planning, as well as controlling execution of joint operations. GCCS 3.0 allows users to navigate among the various JOPES applications using the JOPES Navigation (JNAV) graphical system level navigation application. JNAV allows users to easily start GCCS applications and switch between them. The JOPES applications that run on the HP platform include (see paragraph 6.1.2 for descriptions of the individual applications):

**6.2.1.1.1 Ad Hoc Query (AHQ)**

AHQ is part of the Scheduling and Movement (S&M) application. AHQ allows Operations Plan (OPLAN) end users to query S&M on scheduling and movement requirements for a given OPLAN. A toolkit allows users to build queries and reports, thus minimizing the need for specialized knowledge of the database. For low-bandwidth AHQ users, GCCS 3.0 will support a new web-browser front end, greatly enhancing the simplicity and familiarity of database queries.

**6.2.1.1.2 Ad Hoc Query Character (AHQCHAR)**

AHQCHAR is the client/server replacement for JOPES Subsystem E. This character-based segment of S&M is called by a remote machine, such as a remote PC or SPARCstation 5, for execution over a small bandwidth serial or satellite line.

**6.2.1.1.3 JOPES Navigation (JNAV)**

JOPES consists of a number of applications that are traditionally divided into three categories: Requirements Planning and Execution, Deliberate Planning tools, and Functional Management. The application described manifests itself as an icon on the desktop. Opening the JOPES icon brings up a window pre-loaded with a form provid ing instructions to launch the application. The JNAV Client Segment consists solely of H yperText Markup Language (HTML) documents and UNIX scripts.

**6.2.1.1.4 Predefined Reports (PDR)**

PDR provides users with a report generation capability that supports planners in determining force and non-unit requirements during deliberate or crisis action planning. PDR allows users to analyze COAs in relation to asset allocations and TPFDD modifications.

**6.2.1.1.5 Requirements Development and Analysis (RDA)**

RDA allows editing of TPFDDS and graphical analysis of COAs with respect to TPFDD modifications. RDA also provides a capability for creating and modifying force and non-unit requirements associated with OPLANs.

**6.2.1.1.6 Scheduling and Movement (S&M)**
S&M handles C2 information on deployment activity and status. S&M tracks and reports on TPFDD requirements. S&M allows GCCS users to work with Transportation Component Command (TCC) carrier and organic movement data before and during deployment. S&M can provide carrier support for more than one OPLAN. S&M allows user Ad Hoc Queries (AHQs).

**6.2.1.1.7 External Transaction Processor (XTP)**
The XTP segment is designed to support transaction processing on a machine running System Services without the S&M program loaded. This requirement supports execution of other GCCS segments such as RDA.

**6.2.1.1.8 Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE) Client**
LOGSAFE uses logistics related attributes, such as unit consumption factors, to calculate time-phased requirements for non-unit related supplies. LOGSAFE can also receive data from the Joint Engineer Planning and Execution System (JEPES). Strategic movement requirements can be grouped to optimize transportation needs.

**6.2.1.2 Navy Reserve Unit Data Resource System (RUDRS)**
RUDRS provides an automated means through which the Commander, Naval Reserve Force (COMNAVRESFOR) can provide Naval Reserve Force (NRF) unit data to Fleet Commanders in Chief (FLTCINCs) for reserve commissioned and reserve augmentation units to use in both deliberate and crisis action planning. RUDRS accepts data maintained in the COMNAVRESFOR Reserve Training Support System (RTSS) and makes that NRF data available via a database structure. It provides an automated means of updating JOPES TPFDD files with Naval Reserve data to source OPLANS. The interface provides the capability for FLTCINCS to generate Reserve Geographic Location (GEOLOC) and type-unit characteristics (TUCHA) files for NRF data validation.

**6.2.2 Intelligence**
**6.2.3 Sustainment**
**6.2.4 Mobility & Survivability/Protection**
**6.2.5 Employ Forces/Firepower**

**6.2.5.1 Automated Message Handling System (AMHS)**
The GCCS AMHS provides GCCS users with the capability to receive (via profiles) and transmit with Automatic Digital Network (AUTODIN)

messages. AMHS also supports the ability to automatically update various databases based upon formatted AUTODIN messages.

#### 6.2.5.1.1 COTS Topic (TOPIC)

This segment contains the segmented version of COTS Topic. Consult the release notes that accompany the COTS product for release information. This segment supersedes the previously dated 12/02/94 version of this segment.

### 6.2.5.2 Common Operational Picture (COP)

GCCS can display a wide variety of C4I data on the standardized mapping packages provided in the DII COE. The Unified Build (UB) component of the DII COE provides correlation and display of near real-time and data linked air, land, and sea tracks. These tracks overlay National Imagery and Mapping Agency (NIMA) raster and vector maps to display a COP.

#### 6.2.5.2.1 Common Operational Picture Time Sync (COP_TIME_SYNC)

The Common Operational Picture (COP_TIME_SYNC) is a segment developed for the Global Command and Control System (GCCS) Version 2.2, running Unified Build (UB) Version 3.0.1.6G. The COP_TIME_SYNC segment allows participating nodes to synchronize their system times.

#### 6.2.5.2.2 Link 11 (LINK 11)

This version of Link 11/TadilA satisfies multiple platform requirements using an implementation-independent approach. Implementations currently supported include: FFG7 for Coast Guard, ATACC/TAOM for Marine Corps, Submarine for CCS Mk2, and TSC.

#### 6.2.5.2.3 Enhanced Linked Virtual Information System (ELVIS)

ELVIS uses Hyper-Text Transfer Protocol (HTTP) to service client requests for GCCS/COP Chart images, as well as links into Status of Forces data, where available. A CERN HTTPD process is installed to act as the server for this data; it can live on a workstation running other HTTP servers without conflict. ELVIS provides the capability to view JMCIS displays from any computer SIPRNET device with a World Wide Web (WWW) browser. ELVIS incorporates corrected file ownership settings into the Postinstall script to ensure that owner JMCIS is set on almost all files and subdirectories.

#### 6.2.5.2.4 Tactical Information Broadcast Service (TIBS)

The Tactical Information Broadcast (TIBS) segment allows for the parsing of the Tactical Information Broadcast (TIBS) by COP machines. When

coupled with its classified counterpart, it allows for the reception of amplifying track data that is transmitted on the TIBS.

**6.2.5.2.5 Global Positioning System (GPS) Time**

GPS_TIME is a segment developed for the Global Command and Control System (GCCS) Version 2.2, running Unified Build (UB) Version 3.0.1.6G. The GPS_TIME segment provides the capability for a SPARC SunStation computer running Solaris Version 2.5.1 to keep its system time in sync with the time from a Global Positioning System (GPS) receiver.

**6.2.6 System Administration Tools**

**6.2.6.1 GCCS Tools**

**6.2.6.1.1 GCCS Security Tools**

**6.2.6.1.1.1 Comuter Misuse Detection System (CMDS)**

CMDS discovers suspicious activity on computer networks as it takes place to pinpoint the source of potential misuse.

**6.2.6.1.1.2 Secret Agent**

Provides encryption protection for information stored in or transmitted between personal computers, workstations, and laptops.

**6.2.6.1.1.3 Stalker**

Security software designed to detect and respond to UNIX system misuse by comparing logs of system activities against its database of ways to break in to UNIX systems.

**6.2.6.2 DII COE Tools**

**6.2.6.2.1 Database Tools**

**6.2.6.2.1.1 Oracle Clients**

Provides Relational Database capabilities.

**6.2.6.2.2 Security Tools**

**6.2.6.2.2.1 Security Compliance Tool (SeComp)**

SeComp provides functions and procedures to determine if, where, when, and how COE kernel function and application segments might be

disruptive to a system security configuration. This tool is provided by the DII COE.

#### 6.2.6.2.3 Web/Teleconferencing Tools

##### 6.2.6.2.3.1 HyperText Transfer Protocol Daemon (HTTPD)

The NCSA HTTPD improves performance and corrects several security problems and flaws in the cgi scripts. The following directives have been added to the configuration files: Startserver, Maxserver, ErrorDocument, Agentlog, RefererLog, and RefererIgnore.

##### 6.2.6.2.3.2 Teleconferencing (TLCF)

TLCF is implemented under the HP UNIX operating system using Internet Relay Chat (IRC), which is a chatter style application that allows multiple users to participate in conferences. Several types of channels, with varying degrees of privacy, can be established.

##### 6.2.6.2.3.3 World Wide Web (WWW)

WWW access is provided by Netscape version 3.0. It is a browser that allows GCCS HP users to retrieve information through queries or links to other documents or web sites.

##### 6.2.6.2.3.4 News Groups (NEWSMKGRP)

NEWSMKGRP is designed as a network of servers to which clients attach to obtain the latest news-related information. The COTS software package provided in GCCS is called News Groups-XRN. News Groups provides text-based, non-persistent, non-real-time news access where multiple News Groups can exist simultaneously on the Internet. This product allows users to select a specific article, follow a given News Group thread, and upload and download files in text format.

##### 6.2.6.2.3.5 Netscape News Server

Netscape News Server provides a means of information sharing, workgroup discussions, and server-to-server replication of mission-critical information. It includes access control mechanisms, improved performance over earlier releases, scalability, and encrypted remote administration. Using this capability users can create electronic discussion groups, and post and retrieve messages of mutual interest.

##### 6.2.6.2.3.6 Netsite.

A commercial product which, like Netscape, replaces WIN Teleconferencing functionality. It is the server segment of a client/server

product communicating using TCP/IP protocols. Netscape and Netsite were acquired, modified, and configured from public domain sources.

#### 6.2.6.2.4 Network Administration Tools

##### 6.2.6.2.4.1 Config (NETSYS)

The HP NetMetrix product consists of two parts. One is the remote monitoring Power Agent which implements all nine groups of the RMON MIB (RFC 1271) plus extensions. The other is the application toolbox which implements the graphical toolset consisting of the network load monitor, the network file system (NFS) monitor, the protocol analyzer, the traffic generator, and the internetwork monitor. Together, this package assists in monitoring the performance of your network segments (ethernet, FDDI, tokenring), and troubleshooting network problems.

#### 6.2.6.2.5 Office Automation Tools

##### 6.1.6.2.5.1 Applix

Office Automation is supported by a suite of Applixware COTS products, including Applix Words, Applix Spreadsheets, Applix Mail, Applix Power Brief and Applix Ovation. The latter is a presentation application that communicates with DOS based systems. GCCS 3.0 will upgrade all existing Applix licenses to support the full range of Applix Office Automation (OA) capabilities on Solaris, HP, and NT platforms. It will also allow users in low-bandwidth locations to run OA applications from the web-browser.

#### 6.2.6.2.6 Unified Build (UB)

The UB core software for the JMCIS COE provides basic C4I services to receive and process messages, update a track database, perform correlation and data fusion service, and display the tactical picture. This segment is now part of the GCCS Account Group aggregate segment.

#### 6.2.6.2.7 File Transfer Protocol (FTP)

FTP is used to directly control the transfer of files to and from a distant server. FTP is especially useful in transferring large files and is recommended when e-mail attachments exceed 500K bytes.

#### 6.2.6.2.8 Motif 1.2.4

Motif is a library of routines useful in creating user interfaces in an X Windows environment. The Motif libraries contain software modules that expedite creation of graphical user interfaces (GUIs).

#### 6.2.6.2.9 DII COE Remote Installer

Remote Installer is a system management tool used by system administration personnel.

#### 6.2.6.2.10 Joint Mapping Tool Kit (JMTK)

JMTK is a spatial database and suite of tools that can be used in preparing visual graphics and in non-visual analysis. Visual capabilities include presentation graphics, overlays, symbology, and event management. Non-visual capabilities include terrain analysis, image analysis, threat envelopes, and analytical tools. The spatial database supports raster and vector maps, text, and imagery. The tool kit can also perform datum conversion, coordinate conversions, and data optimization.

#### 6.2.6.2.11 Mail Services

Mail Services provides Apop3" access to users' e-mail accounts. This allows users on networked personal computers and workstations that do not mount /var/mail to read their e-mail.

#### 6.2.6.2.12 X-Windows

X-Windows allows HP clients to access other HP and non-HP clients and servers. This is a very powerful capability, since it allows HP users to execute programs remotely, with only the output results sent to the HP client. The HP user thus has access to tremendous computing power and a wide variety of applications without having to have those resources available locally.

#### 6.2.6.2.13 Printer (PRINTER)

This is the Printer software for the JMCIS COE. It provides text and graphic printing capabilities for a number of printer types.

#### 6.2.6.2.14 Point-To-Point Protocol (PPP)

The HP REMOTE ACCESS segment and the required PPP for HP segment are intended to run on an HP 712 with HPUX V9.0.7 operating system and GCCS COE installed. The PPP for HP segment contains installation scripts and PPP (Morning Star Technologies) software.

#### 6.1.6.2.15 PERL (PERL)

This segment is a powerful scripting language intended for use by system administrators.

### 6.3 Functional Areas Under the NT Operating System

### 6.3.1 Force Development and Deployment

#### 6.3.1.1 JFRG II

JFRG II provides a Windows PC based remote TPFDD editing tool that will support all services TUCHA data and allow transaction updateing of OPLANS. JFRG II may be run in Windows NT environment on the GCCS network, or in a “stand-alone” environment on Windows 3.1 or 95, and fed to GCCS JOPES via other communications channels (low bandwidth).

#### 6.3.1.2 Smart Thin Clients

Smart Thin Clients are Personal Computers that download applications from a central server. They are architecturally simple, inexpensive to operate, and operate like a network terminal. All thin client application programs are stored remotely. A 'smart' thin client would have slightly more capability. Thin client technology permits a broader use of computer resources with central control of versions, upgrades, and access. Future growth of GCCS is intended to support thin client technology.

### 6.3.2 Intelligence

### 6.3.3 Sustainment

### 6.3.4 Mobility & Survivability/Protection

### 6.3.5 Employ Forces/Firepower

#### 6.3.5.1 Common Operational Picture (COP)

##### 6.3.5.1.1 C2PC

COP for Windows NT GCCS users is provided by C2PC version 4.1.0. It allows an NT-based personal computer (PC) to connect to a Track Database Master (TDBM) server via a Transmission Control Protocol/Internet Protocol (TCP/IP) connection. The functions provided by C2PC are a subset of those available to UNIX-based users, tailored to provide essential functionality using a low bandwidth connection to a TDBM.

### 6.3.6 NT System Tools

#### 6.3.6.1 GCCS Tools

#### 6.3.6.2 DII COE Tools

##### 6.3.6.2.1 Database Tools

##### 6.3.6.2.2 Security Tools

NT security tools will continue to be examined for suitability in the GCCS V3.0 environment. Phase 1 implementation will provide the NT security

configuration in the GCCS V3.0 Trusted Facility Manual (TFM) (Final document will be available 12/19/97, FINAL Draft version is available and dated 9/2/97).

#### 6.3.6.2.3 Web/Teleconferencing Tools

##### 6.3.6.2.3.1 Internet Relay Chatter Client (IRCC)

IRCC allows a Windows NT GCCS user to connect to an internet relay chatter (IRC) server. Once connected, the user indicates which channels are to be joined. The server then transmits all messages on those channels to the user. Further, when the user sends a message to the server, the server forwards this message to all other clients on the message's channel and to all other servers that have clients on the channel.

##### 6.3.6.2.3.2 World Wide Web (WWW)

WWW browser service is provided through Netscape version 3.0. The GCCS user may retrieve information through queries or links to other documents or web sites.

#### 6.2.6.2.4 Network Administration Tools

#### 6.2.6.2.5 Office Automation Tools

##### 6.3.6.2.5.1 Microsoft Office

Office automation support is intended to be provided by Microsoft Office 97 for Windows NT. This suite of applications includes Microsoft (MS) Button Bar 4.2 for user convenience in selecting office automation applications, MS Word for word processing, MS Power Point for presentation graphics, and MS Excel for spreadsheets. Purchase of Microsoft Office 97 licenses for NT-based platforms is a site responsibility. There are many versions of MS Office products available, the preferred package is for the highest version, MS Office 97.

##### 6.3.6.2.5.2 Windows Distributed Desktop (WINDD) Client

WINDD is an application that allows users to access, via local area network or via TCP/IP connection, a WINDD server which hosts and runs applications requiring hardware resources that exceed the capabilities of individual client users. UNIX-based GCCS users can also use this capability via X-Windows to access Windows NT-based applications that are not available on their UNIX platform.

#### 6.3.6.2.6 DII COE Kernel

DII COE Kernel provides the essential framework and services that provide a common operating environment for the GCCS or other DII system user.

## 7.0 OPERATIONAL EMPLOYMENT

### 7.1 Overview

GCCS supports deliberate and crisis action planning through integration of appropriate functional applications and shared databases. Broadly speaking, these functions include force requirements, readiness and training, transportation analysis, deployment, sustainment. and redeployment, In the course of ordinary events, GCCS permits deliberate planning; that is, it allows force models to be developed and updated based on today's actual force capabilities. GCCS supports crisis action planning by providing the supported commander access to these models and an electronic forum for tailoring existing OPLANS to meet specific requirements in near real time. Models can be changed dynamically and the ripple effects can then be assessed.

### 7.2 Deliberate Planning

Deliberate Planning provides the framework for building, updating, and maintaining threat assessments and corresponding force models. Particularly important functional applications that support deliberate planning include:

#### 7.2.1 JOPES Automated Data Processing (ADP)

JOPES supports deliberate planning through its applications. These are listed in paragraph 6.1.2 of this document.

#### 7.2.2 GSORTS

GSORTS is the central registry of all operational forces. It provides unit status information in four functional areas: Personnel, Training, Equipment-on-Hand, and Equipment Serviceability. Basic information about a unit (e.g. unit name, home or present location) is also provided.

#### 7.2.3 E-mail, FTP

E-mail, FTP or other means provide information exchange between supporting and supported commands. Teleconferencing and TARGET may also be used to provide information exchange links.

### 7.2.4 Resource and Unit Monitoring

Resource Unit Monitoring applications also support readiness assessments and operations. Collectively, these applications provide a common and accurate basis for assessing U.S. military capability. See the GCCS User CONOPS, paragraph 4.1.1, for a complete list of these functions.

## 7.3 Conventional Planning and Execution

Planning and execution applications provide a framework within which a force can be sized, deployed, sustained and returned. These applications support deliberate and crisis action planning. These applications provide the following functions:

- Generate and refine notional and actual force requirements and options.
- Generate and refine force movement requirements.
- Generate and refine non-unit cargo resupply and non-unit personnel movement requirement estimates.
- Merge, modify, tailor, source, and integrate force movement requirements in and among plans.
- Merge, modify, tailor, source, and integrate non-unit movement requirements in and among plans.
- Aggregate and summarize requirements and movement information.
- Tailor force lists to crisis operations.
- Develop, modify, and evaluate the feasibility of potential COAs.
- Determine option and OPLANs force and transportation availability and feasibility.
- Develop, refine, coordinate, and disseminate appropriate movement schedules and plans.
- Identify force, logistics, personnel, and transportation shortfalls and limitations.

- Reanalyze movement requirements rapidly and produce flow plans.

- Conduct force, logistic, personnel, and transportation sensitivity analyses.

- Merge force requirements and channel traffic requirements.

- Monitor deployment of forces and selected personnel.

- Identify location and status of airlift and sealift assets.

- Provide near real-time crisis management information, including force, logistic, and movement data.

- Provide information for the coordination of deployment routing, overflight routes, and landing rights.

- Provide information for the coordination of air refueling routes, requirements, timing, and schedules.

- Generate logistic requirements in selected functional areas, including:

- Civil engineering.

- Non-nuclear ammunition.

- Petroleum, Oils, and Lubricants (POL).

- Medical.

- Other supply classes as appropriate.

- Through interfaces with appropriate systems, provide for:

- Initial mobilization of reserve forces and the marshaling of logistic resources.

- Identification of the deployability status of deploying forces.

- Identification of critical logistic resources

- Incorporate host-nation support.

### 7.4 Crisis Action Planning (CAP)

CAP will follow a sequence of events starting with creation of a threat database. This database can be displayed through the COP. The sequence will depend upon whether U.S. involvement is necessary and the time availability. GCCS segments that are especially vital to CAP are discussed below.

#### 7.4.1 Teleconferencing

Teleconferencing will provide interactive information exchange among the CINCs, their components, and the services. IRC will also be used. Information transmitted will include crisis assessments, commander's estimate, COAs and, when appropriate, various orders.

#### 7.4.2 COA TPFDDs

TPFDD will be developed from existing TPFDDs. If time permits JOPES will be used to estimate sustainment lift requirements.

#### 7.4.3 COP

Use of GCCS COP functionality is governed by COP CONOPS (See para 3.0). Each CINC is responsible for developing a COP for his applicable Area of Responsibility (AOR). The COP combines data from subordinate commands and other sensors or information resources to create a picture of the entire AOR. The picture shows current, anticipated, projected, and planned disposition of hostile, neutral, and friendly forces. Additional overlays, models, labels can depict Commander's Intent, weather, battleplans, O/CONPLANS, JOPES, SORTS, other logistics data, Combat Ratios, Ingress Routes, Target Selections, etc. In the process of putting the COP together, Information Managers must resolve any conflicts in the COP through a correlation process at the appropriate responsible level . The CINC will maintain a Common Tac tical Dataset (CTD) which is the designated repository for current battlespace information for the AOR. A subset of the CTD and COP is the Common Tactical Picture (CTP), which is the current depiction of the battlespace for a single operation within a CINC's AOR. The CINC or subordinate JTF commander will be capable of using filters and permissions to tailor the dissemination of the COP or CTP for appropriate recipients.

## 8.0 SUMMARY

GCCS 3.0 will provide increased reliability, stability, and performance, and will extend support for NT platforms and web browser-based access. It also becomes the first major program to fully implement the concept of the DII COE. The DII COE will replace the GCCS COE used in GCCS 2.2 and earlier versions.

(INTENTIONALLY BLANK)

# ANNEX D TO ENCLOSURE 2

# SYSTEMS ARCHITECTURE

**Executive Summary** This Document describes the system architecture for GCCS 3.0. It describes the Hardware, Software, Network, and Personnel needed to support implementation of GCCS 3.0.

## 1. Background.

GCCS 3.0 is designed to be the first major operational system that is fully integrated with the DII COE. Previously GCCS had it's own Common Operating Environment.

## 2. New Features.

GCCS 3.0 will be based on the DII COE version 3.1. In addition to being based on the DII version 3.1, GCCS 3.0 will include: an OS Upgrade for both Solaris and HP, an upgrade to ORACLE 7.3.2.3, changes to the user interface, and new functionality provided to the user as listed in Appendix A.

## 3. Conclusion.

GCCS 3.0 will represent a significant change compared to previous GCCS versions. By implementing GCCS 3.0 using this system architecture, sites should have a more stable and manageable system with some new functionality as well.

## 4.0 Purpose

The purpose of this System Architecture is to provide a description of the proposed structure for the GCCS 3.0 system. GCCS 3.0 is the next iteration of the evolutionary development of GCCS and represents a significant design change from previous versions. GCCS 3.0 will be the first instance of GCCS fully integrated with the Defense Information Infrastructure (DII) Common Operating Environment COE and will also be the first major operational system in the DII. The GCCS 3.0 architecture described below will continue to satisfy the users functional needs specified in the Functional Description when implemented under

the System CONOPS. Users should see noticeable improvements in reliability and performance with GCCS 3.0.

## 5.0 System Requirements

a. The driving force behind GCCS 2.1 was the need to replace the Worldwide Military Command and Control System (WWMCCS) as the primary C4I system for planning and executing joint warfighting operations. GCCS provides functions for monitoring, threat assessment, deliberate planning, execution planning, risk analysis and a common tactical picture. Many of the mission applications to support these functions were derived from legacy WWMCCS functions but are implemented in a modern client server architecture. The first GCCS mission applications provided the same capability found in the legacy WWMCCS and Joint Operations Planning and Execution System (JOPES), but many other applications supporting a broad range of functional users were also added.

b. GCCS 2.2 was fielded to roll-up many of the patches fielded in GCCS 2.1 for a cleaner system and to exploit the newly developed GCCS 2.2 kernel capabilities. GCCS 2.2 was a relatively minor upgrade from version 2.1. GCCS 3.0 however, is a significant change from GCCS 2.2, involving :

1) Use of the DII COE instead of GCCS COE components.

2) An upgrade to Oracle 7.3.2.3 from Oracle 7.1.4.

3) Operating System Upgrades from Solaris 2.3 to Solaris 2.5.1 and from HP-UX 9.07 to HP-UX 10.20.

4) Level 5 compliance with the DII Integration and Runtime Specification (I&RTS).

5) Changes in the Desktop presented to the user.

c. The changes above are alterations to the basic software foundation upon which GCCS 3.0 will operate. The DII COE will essentially replace the GCCS COE with a more capable and more interoperable system. At the application level, changes will be mostly transparent to system users. At the system level, however, users should perceive increases in system reliability, user performance, system response time,

and ease of use. The Oracle upgrade will also eliminate some Oracle bugs and increase performance. The Solaris operating system upgrade is necessary to run Oracle 7.3.2.3. All software segments will be tested for compliance with the DII COE. The desktop provided by the Executive Manager in GCCS 2.2 will be replaced by the Common Desktop Environment (CDE) used in DII. The software changes described above are likely to complicate GCCS 3.0 backward compatibility with earlier GCCS versions and will require longer time to complete upgrades than the time required for GCCS 2.2 upgrades.

## 6.0 General System Architecture

a. GCCS 3.0 will use a three-tier client/server architecture which consists of a user interface (presentation layer), server layer and data layer. The description below concentrates on the physical implementation of the client/server architecture. The overall major components of the GCCS 3.0 system are described in terms of the principal system elements; JOPES Core Database Sites, Non-Core Database Sites, GCCS Remote Sites, and the interconnecting communications network, the SIPRNET.

1) A JOPES Core Database Site is connected to the SIPRNET and is responsible for operating and maintaining the JOPES Core Database accounts and application servers for not only its own users, but also distant SIPRNET users and remote users as well

2) A Non-Database site is also directly connected to the SIPRNET, but does not maintain the JOPES Core Database. It may or may not have an Oracle database server to support GCCS and other locally-run applications, and it will have application servers, but because it does not maintain a synchronized copy of the JOPES Core Database, its users are dependent upon distant JOPES Core Database Servers.

3). Each Non-Core Database site is homed to a primary JOPES Core Database site to access system-wide data. The GCCS 3.0 configuration of database sites and their associated Non Core Database sites is shown in Figure D-1.

4) A GCCS remote site is one that depends on serial (dial-in) connectivity to the SIPRNET. Users will not have a database server, but will have certain GCCS applications loaded on

application servers and clients that are geared specifically toward this type of low-bandwidth, slow speed connection.

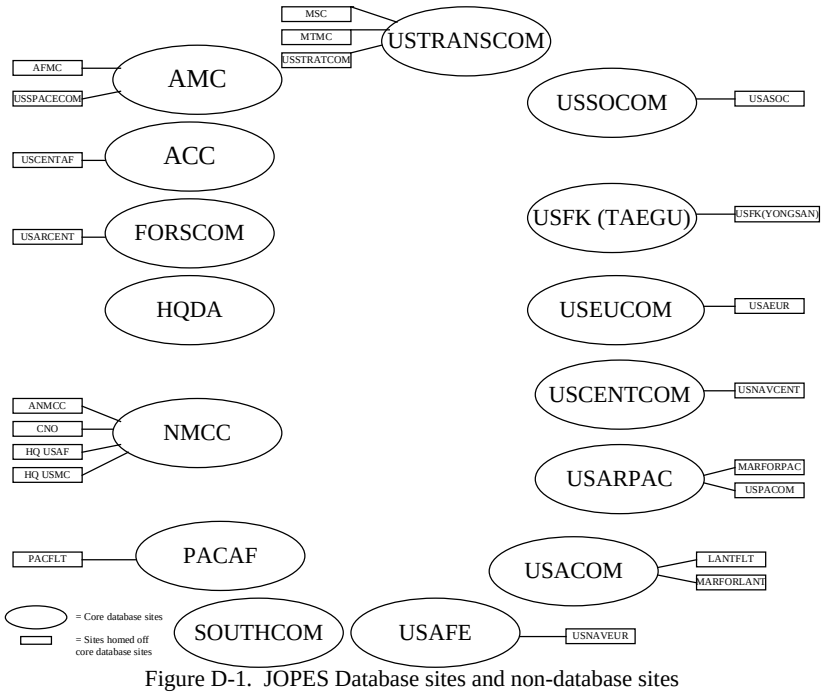



Figure D-1. JOPES Database sites and non-database sites

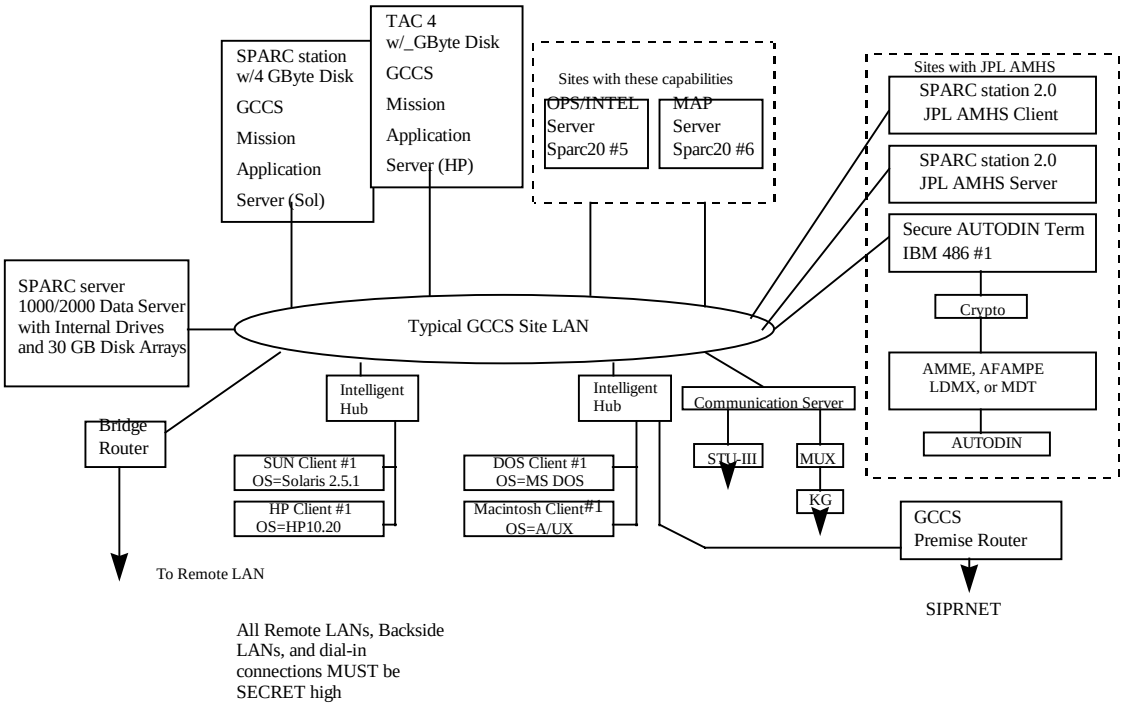



Figure D-2. JOPES 3.0 Core Database Site Configuration

5. The configuration for JOPES 3.0 Core Database Sites is shown in Figure D-2 and does not change from version 2.2. The principal components are the SPARCserver 1000/2000 database server, SPARCstation 20 and HP TAC-4 application servers, the site LAN, the local client machines, the AMHS suite for external communications, and the premise router connecting the site to the SIPRNET

6. The LAN provides local communications between clients and servers. The GCCS Premise router, located on the LAN, connects the GCCS LAN to the SIPRNET Router for backbone, long haul network communications with other GCCS sites. The AMHS suit allows connection to the AUTODIN network. Remote users can also access the site by dialing into the local Communication Server connected to the LAN.

b. <u>Hardware</u>

1) The GCCS 3.0 hardware will not differ from the GCCS 2.2 configuration. A SPARC 1000 should have at least 32 Gigabytes (GBs) of mirrored storage from a RAID Array and

have at least 512 MBs of RAM, with 1 GB being optimal. Variations will exist from site to site

2) Application servers will use SPARCstation 20s for Solaris platforms as in GCCS 2.2 and TAC-4s for HP platforms. SPARCstation 20s will usually have 4 GBs of hard disk storage and 224 MBs of RAM. The capacity requirements for TAC-4s as application servers is currently being determined.

3) Client workstations are usually defined as Sun Sparc 5s, HP Tac-3/Tac-4s, or Windows/Windows NT machines. GCCS clients should generally have at least 64 Mb of RAM and 2 Gb of hard drive storage. Windows clients running on Intel platforms are generally used only as Xterm devices, a role they serve well. GCCS does have applications that run in the DOS/Windows environment. In situations where PCs are actually running these applications, DISA recommends at least 32 Mb of RAM and 4 GB of storage. Where PCs are simply used as Xterms, DISA recommends no less than 16 Mb of RAM and 2 GB of storage. Requirements depend largely on how the system is used, and by how many people.

4) Although the GCCS 3.0 hardware does not differ from the GCCS 2.2 configuration, some sites may consider the acquisition of hardware to support additional user requirements. Sun Microsystems has moved to a new line of Ultra and Enterprise machines. The new generation hardware platforms have more capabilities than existing platforms used in GCCS. There are broader purchasing options available within the Ultra and Enterprise suites. Sites should assess user requirements and specific platform configurations before purchasing. Although there are more options, sites should purchase at least the equivalent of the client, workstation, or server platforms as they exist in the GCCS community today. There are no significant hardware changes in the HP TAC platform line.

c. <u>Software</u>

1) The GCCS 3.0 software functionality contains the same functionality to support the user as in version 2.2. The applications currently segmented to work on top of the GCCS COE are ported to the DII COE 3.1. In addition to the changes involving the DII COE 3.1 and the upgrade to Solaris 2.5.1 and HP 10.20 operating systems discussed earlier, other changes will be made to accommodate the HP application

servers and to ensure the software segments are compliant with DII COE. The JOPES 3.0 Core Database is the repository for all shared system-wide information. The database applications typically loaded on JOPES 3.0 Core Database Site servers are listed in Table 3-1 below (the DII COE will also be required). Some sites may not include all applications and others, such as the NMCC or USTRANSCOM may also load site-unique server segments.

**Table 3-1. JOPES 3.0 Core Database Software**

| | |
|---|---|
| Oracle Server Tools | PDR Server |
| Oracle RDBMS | JEPES Oracle Server |
| GSORTS Oracle Server | IMS_RFM |
| GSORTS Update Engine | NPG |
| S&M Database | Database User |
| LOGSAFE Database Server | Airfields DB Server |
| RDA Server | |

2) Application server and client software for GCCS 3.0 will be basically the same as for GCCS 2.2, with the exception of changes needed to accommodate the HP applications servers. A complete list of the segments in the GCCS 3.0 Build is dynamic. Current information on GCCS 3.0 segments can be found on the GCCS Home pages. GCCS 3.0 Stage 1 software is, for the most part, the same functionality as the current build. GCCS 3.0 Stage 2 software will include new functionality.

d. <u>JOPES 3.0 Non-Core Database Sites</u>

1) JOPES 3.0 Non-Core Database sites are generally configured to host GSORTS for the site, with remaining resources configured to support whatever special requirements a site may have. Load configurations vary greatly from site to site. Non-Core Database sites will be

provided specific segments corresponding to their type of system.

e. Network Communications

1) SIPRNET

a) The SIPRNET is a world-wide network of backbone routers interconnected by high-speed serial links (mostly 512 kbps interconnections). The SIPRNET supports the TCP/IP protocol service and is planned to eventually support the Government Open Systems Interconnection Profile (GOSIP) service. The SIPRNET serves all DOD Secret-level subscribers and is not dedicated to GCCS users. GCCS 3.0 users will comprise a small percentage of the subscribers to the SIPRNET. The primary GCCS sites access to the SIPRNET is via the sites Premise Router, connected to the site LAN. Regional topologies of the SIPRNET can be found in the GCCS System and Network Management CONOPS. The SIPRNET is supported by the SIPRNET Support Center (SSC). SIPRNET support provided for GCCS 2.2 will continue for GCCS 3.0. Sites using new functionality in GCCS 3.0 may need to increase their available bandwidth

2) Teleconferencing

a). GCCS 3.0 will continue to employ the three applications used in earlier GCCS versions to provide teleconferencing capability. These are Internet Relay Chatter (IRC), Usenet News (Newsgroups) and World Wide Web (WWW). These applications have been adapted from public and commercial sources to operate over the SIPRNET and within the DII COE environment. Users will be able to save GCCS 2.2 teleconferencing configurations (e.g. News groups) for reuse in GCCS 3.0 following transition. Users who use the public domain edition of NS News software must replace it with the licensed version of NS NewsServer (Netscape) for GCCS 3.0.

f. Data Flows

1). Data flow in GCCS 3.0 will also remain the same as for GCCS 2.2. Local users communicate with the JOPES Core Database either over the LAN, via the SIPRNET or by remote dial in capability. Character-based interfaces will be provided for text-based operations using low bandwidth circuits. Users will continue to utilize applications such as JNAV and Ad-Hoc Query to navigate and interface with JOPES applications in GCCS 3.0. GSORTS data will continue to be provided to GCCS 3.0 from the individual service and agency unit status reporting systems which feed information to the Joint Staff. Static reference information in reference files such as TUCHA data will continue to be provided to the JOPES database sites by the GCCS Management Center (GMC). The GMC will use GCCS application tools provided specifically for periodically updating these reference files at the JOPES Core Database sites via the SIPRNET. The GMC will also continue to ensure that GCCS 3.0 transaction processing is maintained so as to maintain synchronization between the Core Database Sites.

2). GCCS 3.0 accommodates the same tactical/operational data feeds found in earlier versions. DIIs Unified Build can accommodate almost any type of track data, while the Common Operational Picture (COP) synchronizes track data with other COP systems and display the tracks on a map background. The various feeds accepted by the COP listed in Appendix A. It is the responsibility of the service/agency owning the source system to coordinate any planned changes in these COP feeds with the Joint Staff.

**7. System Operations**

a. GCCS 3.0 System Control Elements

1). The GMC

a).GCCS 3.0 will be operated by the same organizations operating GCCS 2.2. The GMC will continue as the primary system operational control element. The GMC will monitor and control the health and status of the GCCS 3.0 system to include GCCS network operations and all Joint software applications. Services and agencies will be responsible for managing their own unique applications. The GMC will continue to coordinate closely with the DISN Global Control

Center (DISA) responsible for SIPRNET operations. The GMC will continue to operate the GCCS Help Desk and will continue to coordinate activities with the DISA GCCS System Assistance Center at the Operational Support Facility (OSF). The GMC will direct day-to-day system level changes to the GCCS 3.0 system needed to maintain continuous operations.

2. The GCCS Sites

a). GCCS sites will continue to be responsible for overall site operations with oversight from the GMC. Each site will require personnel with the same areas of expertise as required in GCCS 2.2. Site requirements will vary by site type, size, and platform mix but the positions which generally must be supported include:

- GSC - GCCS Site Coordinator
- GNA - GCCS Network Administrator
- GSA - GCCS System Administrator
- GDBA - GCCS Database Administrator
- DAA - GCCS Site Designated Approving Authority
- ISSO - GCCS Information Systems Security Officer

3. GCCS 3.0 Backup Procedures

a). Each JOPES Core Database site will have two designated backup sites. Sites served by a primary site which fails will be responsible for reestablishing contact with an alternate database site. Sites must maintain the proper permissions for Unix, Oracle, GSORTS, JOPES OPLANs, and applications access needed to quickly switch to and access the alternate database site. This procedure will be similar to procedures used in GCCS 2.2. However, there will be some changes in GCCS 3.0 since user account groups will be handled differently and DII-compliant GCCS applications can no longer create and use their own database accounts as they did in earlier GCCS versions.

**APPENDIX A**
**FEEDS TO GCCS COMMON OPERATIONAL PICTURE**

**Feeds Accommodated in GCCS 30**

JFRG II
GTN
COMPES
AGCCS
COMPASS
STACCS
OTCIXS/V6-TTY
OTCIXS 16 bit TDP8648
TDP8648 16 bit

**Links:**

ACDS
ACDS- Coast Guard
Link 14
Link 16
TADIL A: Link 11 - Indian Head, EDO
TADIL B

**Nav Interfaces:**

RAYCASV
CVNS
SDMS
SINS
SRN19
SRN25A
SRN25P
WSN5
WRN6
LORANC
NMEA-183 (GPS)
NMEA2 (GPS to adjust system time)
NSK-NMEA (GPS)
NAVSSI

**Other:**

SPA-25G MDT STU-III
TAMPS TIMS-OUT TRE/TRAP (GOLD or TABULAR)
API Network (TCP) Mdx
TRE/TRAP High-Precedence, Tabular
MdxNet/COP JTAV VT-100
Email NavOut/NavIn (NAVMACS V5)
CTAPS (ATO downloads via ATOX) Kermit and Kermit Binary
USMTF
V6TTY Message GFCP-LAN TLC-10
RF-NET (ANDVT or Harris modem + radio)
TCIM PLRS/EPLRS TIBS (TDIMF format)
AMP BSY-2 FCS
MX512P GBS Net Prec (TCP/Prioritized)

ANNEX E TO ENCLOSURE 2

SECURITY CONOPS

## 1. Introduction.

This section is excerpted from the GCCS Version 3.0 Automated Information System (AIS) Security Plan (intermediate unpublished Draft prior to 9/2/97 Final Draft product) and specifically addresses the Global Command and Control System (GCCS) Security Policy and Minimum Security Requirements The GCCS V3.0 is a major modification of and evolutionary upgrade to the GCCS V2.1/2.2. The GCCS V2.1 was granted a type certification and interim accreditation to operate (IATO) in May 1996. Details of the certification and accreditation (C&A) may be obtained through the GCCS Program Office by contacting the DISA GCCS Lead Security Officer (LSO), Headquarters, DISA, Arlington, Va. The Final Authority to Operate is scheduled to be issued in the mid-November 1997 time frame based on the GCCS V3.0 security implementation.

The GCCS V3.0 will utilize the Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.1 and provides both functional and security services and managers. This is a major modification to the GCCS 2.1/2 implementation and the DII COE security services and applicable managers will contribute new features to the implementation of the GCCS V3.0 security configuration. Despite theses new contributions, however, the GCCS V3.0 will continue to implement the basic security concepts adopted in V2.1/2.2 that provided the basis for the V2.1/2 type certification and have been shown to be sound under operational conditions when configured and maintained properly.

The security strategy presented in this Plan identifies the GCCS security policy and requirements and the AIS resources in GCCS V3.0 that will address and satisfy that policy and requirement set. The GCCS Security Policy and Minimum Security Requirements have been modified for V3.0 and this Plan will provide an overview mapping of the V3.0 requirements set to the security services adopted that meet the requirements.

This Plan will also address the GCCS V3.0 hardware considerations. However, this Plan specifies a type certification evaluation and therefore will not address the physical, environmental, procedural, and management issues that are associated with GCCS site specific accreditation issues. Each site is responsible for maintaining these

aspects in accordance with the various DoD Automated Information System (AIS) and Joint Staff directives and manuals that are beyond the scope of this Security Plan.

## 1.1 PURPOSE

This AIS Security Plan for the type certification of the GCCS V3.0 provides a description of the security strategy and protection features that will be implemented to meet the GCCS V3.0 Security Policy and Minimum Security Requirements (Joint Staff, GCCS Security Policy and Minimum Security Requirements, CJCSI 6731.01, DRAFT VERSION 22 May 1997). The security implementation described herein will demonstrate the strength of the security configuration and is designed to achieve a GCCS V3.0 type security certification and be granted the authority to be operationally implemented as the replacement for the GCCS V2.2 systems. The authority to operate is scheduled to be issued in the mid-November 1997 time frame. The certified type configuration will provide a security configuration and operational procedure template that will be used by the GCCS sites to baseline the site-specific security implementations. Further, this Plan can be used by the GCCS sites to substantiate portions of the site security implementation as part of the site certification and accreditation (C&A) package.

The intended audience of this Security Plan is:

- The GCCS V3.0 Security Engineering and Implementation staff
- The Joint Staff (J6) Designated Accreditation and Approval Authority
- The Security Test and evaluation test director and testing staff
- The GCCS site security implementation and maintenance staff

## 1.2 SCOPE

The GCCS V3.0 is a collection of operating system (OS), database management system (DBMS), DII COE, and GCCS application software operating on multiple vendors hardware platforms, operating systems (OS), and support medium. The combination of software and hardware elements are designed to provide a suite of capabilities that meet the core command and control ($C^2$) needs of the Department of Defense (DoD) organizations that function in the GCCS community. This AIS Security

Plan focuses on the composite software, hardware, and security needs of the GCCS community as a whole and that have been evaluated at the OSF in Sterling, VA. The fulfillment of additional/supplemental site or GCCS implementations other than the Secret GCCS (e.g., GCCS-T) security requirements are beyond the scope of this Plan.

## 1.3 SECURITY POLICY AND SECURITY ENVIRONMENT

This section addresses the security policy and security environment of the GCCS V3.0. It is from this framework that the security protection features presented in this plan can be implemented at GCCS sites.

### 1.3.1 Security Policy

The GCCS V3.0 Security Policy, CJCSI 6731.01 (FINAL date when released) addresses the system characteristics, role responsibilities, the minimum security policy for the system and supporting network, and the minimum security requirements for the GCCS V3.0. The policy addresses the system classification boundaries, specifically, that the security policy statements and references apply to both the GCCS Secret and GCCS Top Secret (T) applications and procedures (unless otherwise specified in the policy document).

### 1.3.2 Security Environment

The GCCS security environment is identified in the GCCS V3.0 Security Policy and its implementation is bounded by the Minimum Security Requirements. The satisfaction of these requirements require the implementation of the C2 class, Controlled Access Protection (CAP) or equivalent capabilities. The GCCS security environment is said to target the C2 class level of assurance, making use of the C2 capabilities when available and cost effective. Likewise, the GCCS security environment will take advantage of products already evaluated and contained in the Evaluated or Approved Product Lists maintained by the National Computer Security Center (NCSC) at the National Security Agency (NSA) when available, applicable, and cost effective. Supplemental products, such as for audit analysis, system configuration monitoring, etc., will be employed to aid the security staff in carrying out their duties and responsibilities.

It is wise to note what the GCCS V3.0 security environment is not. The GCCS V3.0 security configuration, although aided by automated system services and security products, is not automatic. The GCCS security environment requires the diligent and continuous employment of the safeguards and procedures identified in this plan by the GCCS security staff and users. To support this maintenance effort, the GCCS security environment requires clear and concise procedural guidelines and documents. There are two levels of documentation provided for this purpose:

| | |
|---|---|
| **JCS Instructions and Manuals** | These documents extend the Joint Staff policies and procedures to the GCCS site security personnel and include the CJCSI 6731.01 GCCS Security Policy, CJCSM 6731.01 GCCS Security Implementation Procedures. These documents provide GCCS sites with the guidance required to be applied to and correlated with the site specific security requirements, applications, and procedures (i.e., site-specific Standard Operating Procedures (SOP) and Site Security Implementation Procedures (SSIP)). |
| **DISA Engineering Documents and Guidance** | These documents describe the security implementation responsibilities and activities to the GCCS site security personnel regarding the functional application of the protection measures available. These documents include the Trusted Facility Manual (TFM)(FINAL 12 December 1997), Security Feature Users Guide (SFUG) (FINAL 12 December 1997, the various GCCS and DII COE manager and product System Administrator Manuals (SAM), and product user documentation. The TFM and SFUG are the key documents within this group and |

provide the security staff and user personnel with the information required to administer the system security and operate within the parameters of the security procedures.

Finally, it is important to note that the focus of this plan and, therefore, the protective measures that comprise the security environment, is to meet or exceed the security requirements identified in the GCCS V3.0 Security Policy and Minimum Security Requirements. It is expected that the test plan and procedures developed for the purpose of establishing the correctness of the implementation and strength of the protective measures be considerate of this focus.

## 2.0 GCCS SYSTEM OVERVIEW

This section provides an overview of the GCCS V3.0.

### 2.1 DII COE V3.1 AND GCCS V3.0

The GCCS is a major program component among the DISA pillar program systems integrating into and operating within the framework of the DII. Integrated for the platforms supported by the DII COE are the DII COE Kernel Services. The GCCS will implement the security and operational functions provided in the DII COE Kernel Services as they are appropriate to the GCCS V3.0 operational implementation and security configuration. Regarding the security functions, the GCCS will utilize the platform services provided by the DII COE and implement the security functions that are the subset of DII COE security features[2] targeting the C2 CAP features and capabilities as available and applicable.

It is important to note that the DII COE Security Requirements Specification (SRS) defines the requirements for the security services that are acceptable for inclusion into the DII COE. The SRS does not

[2] The DII COE Security Services Security Requirements Specification includes several requirements that will require B-class security functions to implement. GCCS V3.0 has no B-level requirements and will not attempt to implement features that meet these requirements.

mandate system requirements for systems integrating into the DII. Each system, such as the GCCS V3.0, that integrates into the DII is required to establish system security policy and requirements commiserate with the level of protection required for that system.

## 2.2 GCCS V3.0 DESCRIPTION

The GCCS V3.0 concept is as an architecture that is integrated within the framework provided by the DII COE V3.1, especially insofar as the integration pertains to:

- The DoD Technical Architecture for Information Management (TAFIM), Volume 3
- An approach for building interoperable systems; a collection of reusable software components
- A software infrastructure for supporting mission applications
- A set of guidelines and standards.

### 2.2.1 GCCS Type Configuration

The GCCS V3.0 type configuration will be integrated, tested, and maintained at the DISA Operational Support Facility (OSF) in Sterling, Virginia. The GCCS V3.0 type configuration represents the baseline (core set of) software and hardware components that could be implemented at any given GCCS site. The type security configuration is designed to provide a baseline GCCS V3.0 security implementation that is suitable for operational and security testing and evaluation and will provide the basis for the template security configuration to be replicated at each GCCS site. It is important to note that this configuration may not (in all probability, will not) represent the exact configuration of <u>any</u> particular GCCS site. The type configuration will represent the major GCCS V3.0 components and configuration and provides the core implementation for <u>all</u> GCCS sites.

The GCCS V3.0 Security Test and Evaluation (ST&E) process will be performed at the DISA OSF in Sterling, VA 1 October through 17 October 1997.

### 2.2.2 GCCS V3.0 Software

The GCCS V3.0 consists of software designed to support the GCCS community within the framework of the DII COE V3.1. DII COE architecture is based on a system kernel approach that utilizes and correlates platform-based OS mediation and resource management functions to support the core system functions provided by the DII COE kernel. The system kernel functions will also include core services required by all GCCS implementations such as print and security services.

The GCCS V3.0 software tested during the ST&E will represent the frozen CM release software components that will comprise the GCCS and be available to the GCCS sites for implementation.

### 2.2.3 GCCS Security Software Division

For the purpose of this Plan and to identify the origins on which the GCCS V3.0 bases its security implementation, it is convenient to divide the security software according to the origin of the provider.

As previously discussed, the DII COE provides security services and software that may be integrated into a systems security implementation. In addition to the security functions provided by the DII COE, systems integrating into the DII COE framework may implement additional/supplemental system services and software in support of the systems security policy and requirements. The GCCS V3.0 security implementation and configuration will utilize GCCS-provided security services and software as well as DII COE services and software.

#### 2.2.3.1 Security Services and Software Origins

The DII COE services and software are provided within the OSs supported by the DII and the DII system kernel[2] . Therefore, the two DII security software source categories are identified as:

- DII OS security services
- DII Kernel services

[2] Note that in strict DII COE terminology that the kernel includes the OS. This does not stand up well when attempting to identify the security service source so they are distinguished separately herein.

The GCCS security services and software are provided by either a commercial or government source. Therefore, the two GCCS security software source categories are identified as:

- GCCS commercial-off-the-shelf (COTS) tools
- GCCS government-off-the-shelf (GOTS) tools

### 2.2.3.2 DII COE Security Services

The DII COE security services are provided by the platform OS and the kernel security functions.

#### 2.3.3.2.1 DII OS Security Services

The platform OS will provide the base C2-CAP features providing the following DII OS security services:

- Identification and authentication (I&A) features and services.
- Auditing features and services.
- Discretionary access control features and services.
- TCB resource isolation features[3] .
- Object reuse features[4] .

#### 2.3.3.2.2 DII COE Kernel Services

The kernel services are provided in the form of management services. The DII COE also supplies a set of freeware security tools provided in the Freeware Tool Kit, however <u>these tools are not employed as part of the security configuration presented for certification[5] .</u> The management services provide GUI interfaces to the OS services allowing user and file system management chores to be completed. The applicable[6] DII kernel security services are primarily implemented with the following managers and services:

- Common Desktop Environment

---

[3] These are controlled totally within the operating system TCB and provide no application services.
[4] These are provided within the operating system at various levels of implementation.
[5] The Freeware tools provide some rudimentary security functions that in most cases are provided in the SeMore tool. The one tool that might be employed on site implementation basis to provide beneficial service is the TCP Wrappers tool. Referred to in some circles as the “poor man's firewall”, this tool requires an understanding of the site connectivity requirements and does require additional management effort to maintain.
[6] Although other tools may be available with the DII COE V3.1, this Plan focuses on the tools engineered for use to meet the GCCS V3.0 security requirements.

- Profile Selector

- Security Manager
  - Profile Management services
  - Session Management services

Reiterating, the GCCS V3.0 security implementation will not be dependent upon the use of the Freeware tools but are available to support the site security staff.

### 2.2.3 GCCS V3.0 Security Services

The GCCS V3.0 security services primarily provide support or supplemental tools and utilities to aid in the implementation and maintenance of the security configuration. Tool and utilities are provided in the form of a COTS or GOTS tools.

The COTS tools provided for the GCCS V3.0 are:

- Computer Misuse and Detection System (CMDS)
- Stalker
- Secret Agent

It is important to note that the GCCS V3.0 type certified security implementation will not be dependent upon the use of the GCCS COTS tools.

The GOTS tools provided for the GCCS V3.0 are:

- V3.0 Security Alignment (security segment)
- Audit Management (audit segment)
- Security Monitoring and Reporting (SeMoRe) tool

The use of the DII and GCCS security features and services are described in Section 5, Minimum Security Safeguards Strategy. The GCCS V3.0 type certified security implementation will be dependent upon the proper configuration and use of these GCCS V3.0 GOTS tools.

### 2.2.4 GCCS V3.0 Configuration Management

The DISA GCCS Configuration Management (CM) staff provides COE compliance checking and security compliance testing on all delivered segments. The CM process ensure that all software segments are properly formatted, documented, and operate within acceptable parameters. The CM process ensures that only acceptable and compliant software is made available to the GCCS sites and that all sites are operating with the same version of each software segment.

### 2.2.5 Software Application Security Compliance

The DISA OSF GCCS Integration and Quality Assurance departments, in conjunction with the current configuration management process, has instituted the Security Compliance (SeComp) tool and procedure to verify security compliance by the delivered GCCS V3.0 software segments. In conjunction with this process, the GCCS Developer Security Guidelines (DISA GCCS, January, 1997) describe the desired state of the delivered software regarding security-related files and directories. The GCCS V3.0 (as well as versions in the foreseeable future) will maintain a grand fathering approach[7] concerning the complete security compliance of the legacy GCCS applications. New software development must comply with the security guidelines.

The DISA OSF GCCS Integration security staff and the DISA GCCS IPO evaluate the security state of the delivered segments and report discrepancies to the segment provider and determine if out-of-compliance items are serious enough to warrant immediate fixing prior to acceptance as a GCCS V3.0 segment. The SeComp process is not a guarantee that the segments are 100% in compliance with the security guidelines, however, the process provides valuable insight into the security state of the delivered software and does help prevent major discrepancies from occurring.

### 2.2.6 GCCS V3.0 Hardware

As previously discussed, the GCCS V3.0 software is operable on multiple various platforms approved for use within the DII COE V3.1. The hardware platforms used in the GCCS V3.0 configurations are:

| Platform | OS | Version | Server (Y/N) |
|---|---|---|---|

[7] See Section 3.2, Statement of Security Concerns.

| | | | |
|---|---|---|---|
| Sun Microsystems | UNIX | 2.5.1 | Y |
| Hewlett Packard | UNIX | 10.20 | N |
| 486 Pentium Personal Workstation | NT | 4.0 | N - Xterm Client service only |

Each platform offers the C2-CAP features, however, each will implement these features in somewhat different ways. This makes it imperative that the security staff be capable of comprehending each platform's security feature implementation.

### 2.2.7 GCCS V3.0 Network Backbone Support

The GCCS V3.0 is designed to take advantage of the network architectures that are available to the GCCS V3.0 sites and will use the Defense Information System Network (DISN) as the primary information transport mechanism among the GCCS V3.0 sites. The DISN maintains the implementation of the US Only Secret Internet Protocol Router Network (SIPRNET) providing end-to-end information transfer and value added services for the transport of data up to the Secret level.

### 2.2.8 GCCS V3.0 Data Owners

Data ownership within the operational GCCS V3.0 is traced to the functional program that originates or develops it. The GCCS V3.0 type configuration will not process operational data.

### 2.2.9 Description of GCCS V3.0 Data

Data processed on the GCCS V3.0 AIS resources will include text, graphics, and images. The GCCS V3.0 type configuration will include processing of text and graphics.

### 2.2.10 GCCS V3.0 System Connectivity

The GCCS V3.0 will provide the required connectivity to the GCCS community as described in 2.2.8, GCCS V3.0 Network Backbone Support. Although other pillar program systems (e.g., Defense Message System [DMS], Global Combat Service Support System [GCSS], etc.) may connect to the GCCS V3.0 network, each will connect as a GCCS subscriber and will be required to meet the GCCS V3.0 Security Policy and requirements as well as the DISN SIPRNET connectivity requirements. All Secret GCCS V3.0 connections among the GCCS community of subscribers will occur at the Secret classification level[8] . Connectivity to systems not at the Secret classification level may only occur as the result of a separate certification and accreditation effort involving the GCCS system Designated Approval Authority (DAA) and the DISN connection approval authorities.

The GCCS V3.0 type configuration will be limited to the evaluation of the SIPRNET connectivity issues. Connectivity involving secure communication modems and COMSEC equipment will be evaluated for accreditation purposes at each applicable site.

## 3.0 Concept of Security Operations

The concept of security operation includes an assessment of the relationship between the sensitivity of the data processed and the security clearance of the user community. It also includes the determination of the minimum evaluation class for the protection of information and the level of trust that can be placed in that protection. The methodology for this process is contained in Enclosure 1, DoD 5200.28. This Plan addresses that relationship insofar as it pertains to the configuration of GCCS V3.0 Secret implementation. The following sections describe the steps in the process for making that determination as it pertains to the GCCS V3.0 type security configuration.

## 3.1 Sensitivity Determination

The determination of sensitivity for the GCCS V3.0 type security configuration is based on the relationship between the maximum sensitivity of the data processed and the minimum security clearance granted to the users. This relationship produces a Risk Index (RI). The RI can be calculated using the following formula, where $R_{max}$ is the

[8] GCCS-T does not maintain any connectivity to the Secret GCCS. GCCS-T operates at the Top Secret level and maintains the appropriate network connectivity at that level for its community of users.

maximum sensitivity (classification) of the data processed including categories, and the $R_{min}$ is the minimum security clearance of the least cleared user.

$$RI = R_{max} - R_{min}$$

Therefore, the sensitivity determination for the GCCS V3.0 at the OSF is calculated as follows. The maximum sensitivity of the data is Secret with no categories. Using Table 2, Enclosure 4 of DoD 5200.28, $R_{max}$ is found to be "3".

The minimum security clearance of the least cleared user of the OSF GCCS V3.0 is Secret. Using Table 1 of DoD 5200.28, $R_{min}$ is found to be "3".

The RI for the OSF GCCS V3.0 is RI = 3 - 3, or RI = 0. The minimum evaluation class for the protection of data with a RI = 0 is determined from Table 3, Enclosure 4 of DoD 5200.28. Using that Table, a RI of 0 requires a System High mode[9] of operations with a Minimum Security Class of C2 - Controlled Access Protection (CAP).

## 3.2 STATEMENT OF SECURITY CONCERNS

The following sections discuss areas of concern to the GCCS V3.0 security configuration.

### 3.2.1 SIPRNET Connectivity and System High Processing

As discussed previously in this Plan, the US Only SIPRNET provides network services up to the Secret classification in the system-high operational mode. The SIPRNET is the GCCS network backbone and is a commodity that is shared by multiple missions. Not all of these missions require access to the GCCS resources.

The SIPRNET does not provide automated discretionary access controls. This requires a basic element of the GCCS security philosophy that states that the SIPRNET provides a trusted path at the secret classification between all systems accessing it. Through its connection

[9] An AIS is said to be processing in the System High mode of operation when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has a valid security clearance for all information processed, a formal access approval for all information processed, and a valid need-to-know for some of the information processed on the AIS.

approval processes, the DISA SIPRNET authority procedurally maintains the mode of operation, classification, and releasability aspects. There is no implementation of a need-to-know mechanism structured into the SIPRNET access control procedures. The need-to-know or discretionary aspect is internally managed by each system accessing the SIPRNET, including GCCS, to prevent unauthorized or excessive access to the SIPRNET connected systems and system data. Hence, while the mode of operation, classification, and releasability aspects are reasonably and centrally controllable, the GCCS implementations must necessarily trust that the need-to-know aspect is well-behaved regarding other systems sharing the SIPRNET.

Regardless of the amount of trust that can be garnered from the SIPRNET controlling authority and processes, there remains an element of concern that authorized SIPRNET users without GCCS need-to-know privileges are provided some opportunity of GCCS access by virtue of sharing the SIPRNET bandwidth. This is a concern that is not easily mitigated via an automated prevention mechanism and requires the acceptance of the DISN authority as the controlling factor.

Maintaining and monitoring the security configuration and user activities is the primary protection implemented concerning unauthorized access to need-to-know privileged information by authorized SIPRNET users as well as tampering by an authorized GCCS user.

### 3.2.2 Legacy Applications and DAC Requirements

GCCS V3.0 will continue to utilize legacy applications that were designed to operate in standalone, non-networked, and isolated environments. In order to operate in a shared file system environment, these applications often employ permission sets on the application program elements that are considered promiscuous.

Although this is not the desired state of the software, it is considered an acceptable risk in light of the operational requirement, the costs of re-engineering, the system high secret environment of the SIPRNET and its connected systems. The GCCS V3.0 integration process employs the SeComp procedure and is gathering the information required to pinpoint the troublesome areas to the DISA GCCS Engineering Staff and to the software providers/developers. This is the first step in the long process to correct the software that is found out-of-compliance with the GCCS security policy.

### 3.2.3 Unowned Files on the GCCS File Systems

GCCS V3.0 will continue to utilize legacy applications that were designed to operate in standalone, non-networked, and isolated environments. When required to operate in a shared file system environment, these applications and database sometime present file ownerships or group accounts that are not prevalent on the importing system and are therefore “unknown” to the that system.

### 3.2.4 Oracle Internal and External Password Management

The Oracle database requires the use of a “programmed” password and the internal usage flag to be set in order to efficiently accomplish the administration tasks of adding or removing users or the grant privileges associated with the users. Not using the internal password mechanism requires the entering of the password an inefficient number of times during the administrative processes in order to coordinate all the table rights associated with a user.

The GCCS V3.0 standard policy is that during normal operation the external password flag is to be maintained on the Oracle database. The internal flag and use of a programmed password may only be used during administrative operations.

### 3.2.5 JAVA Implementation

This section will contain a discussion of JAVA implementation once the policy is established by the Joint Staff.

### 3.2.6 HPUX 10.2, C2 Features, and NIS

The NIS service on the HPUX 10.20 is required for operational account maintenance. HPUX 9.0.7 in GCCS V2.1/2 provided C2 feature capability for only local accounts and protected the root account which is the paramount concern of C2 system protection. In 10.20 this level of protection will be maintained.

The GCCS V3.0 is:

- the evolutionary replacement for V2.2.

- the initial integrating pillar system using the DII COE.
- the U.S. Command and Control system requiring control and confidentiality itself.

The GCCS V3.0 had been advertised to provide enhanced security to its subscribers. The security features available in HPUX 10.20 will be equal to its predecessor.

### 3.2.7 Lack of Input Password Age Checking Capability

The DII COE 3.1 X display manager (xdm) provided for the Solaris and HPUX OSs do supply password aging or minimum age checks. The XDM does supply user name, host domain name, length, and dictionary password checking; all features are configurable and extremely useful.

Additionally, the GCCS V3.0 does employ “after the fact” password checking using the Crack password vulnerability checker.

Aged passwords are the possible result of the XDM’s inability to check password age and minimum age. The TFM and SFUG do cover the password aging procedures, but an automated checking feature at the point of insertion and password life controls would be a boon to the security of the system.

### 3.2.8 Oracle OPS$ Usage

The Oracle database implementation used in conjunction with the JOPES database function will continue to use the OPS$ account mechanism. The OPS$ mechanisms are required in order to support a unitary login process when the data access process requires that another database server must be referenced. This issue is being examined in light of adding an authentication mechanism with the OPS$ but is not expected to be functional for the GCCS 3.0 implementation.

In the meantime, the GCCS site administrators are cautioned in the TFM to coordinate and take extra precautions to ensure that there are no duplicate user accounts (i.e., user name and user ID number) that exist for two different users on two servers.

## 3.3 Level of Trust

The C2-CAP level of trust for the security protection associated with the GCCS V3.0 is derived from the sensitivity determination calculation performed in Section 3.1. The following subsections concern the target level of trust and the strategy for achieving that level.

### 3.3.1 Target Level of Trust

The target level of trust for GCCS V3.0 is Class C2-Controlled Access Protection as defined in the DoD 5200.28-STD.

### 3.3.2 Establishing and Maintaining the Target Level of Trust

Within the GCCS V3.0, the target level of trust can be established and maintained using a combination of security services, software, and procedures from the DII COE OS services, DII COE Kernel services, GCCS V3.0 GOTS tools, and security documentation to address the four basic area associated with Class C2:

- Identification & Authentication that provides for Individual Accountability
- Discretionary Access Control
- Audit
- Object Reuse

#### 3.3.2.1 Evaluation Status of the OS Products

The GCCS V3.0 utilizes and requires the most recent of vendor releases concerning not only application but also OS software. This requires that the GCCS must utilize the most recent products available to provide the functional properties required to perform the $C^2$ tasks required. The operating systems and security software versions that are implemented for the DII COE V3.1 and therefore the GCCS V3.0 will likely *not* be listed on the evaluated product lists. With complete comprehension of the value of the statement, it is valid to state that each of the operating systems implemented *evolved from* an evaluated product that does not appear on the EPL. It should be noted, however, that in no case were the products evaluated in the networked environment presented with the DII COE or the GCCS.

Notwithstanding, the operating system products that are incorporated within the DII COE V3.1 kernel do provide the features required of a C2 class product. These products, despite the fact that they have not been approved of via a formal certification effort, still offer the C2 class

features of the evaluated ancestry. Additionally, the DISA OSF GCCS Security Engineering are recipients of all CERT and ALERT bulletins[10] . providing information and updates to the product baselines concerning the security features of the OS products. The applicable bulletins result in the appropriate actions or notice for actions being forwarded to the affected implementations of the product. Further, all OS products are continually maintained with the most recent system patches received from the product vendors.

#### 3.3.2.2 Using Non-Evaluated Products With C2 Features

When implementing the features of these products, special attention will be given to ensure that each product is properly configured[11] and that all of the required C2 features have been enabled. The details for the configuration will be contained in the TFM for GCCS V3.0. Procedural information describing the end-to-end details not covered by the automated processes will also be covered in the TFM and in the JCS 6731.01 Security Implementation Procedures, with supplemental information in site specific SOP and SSIP documentation.

## 4.0 Minimum Security Requirements

The GCCS V3.0 security policy in CJCSI 6731.01 is derived from national and DoD security policy and an analysis of the operational mission and requirements of the GCCS. The GCCS minimum security requirements are first and foremost based on the security policy stated for the GCCS. The minimum security requirements are then a fulfillment of those policy statements. Appendix E of the *GCCS Version 3.0 AIS Security Plan*, 2 September, 1997 (See appropriate GCCS/DII Home pages)maps the GCCS V3.0 minimum security requirements to:

- the origin of the requirement
- the components that are relied on to satisfy those requirements
- whether the requirement is part of the type configuration or implemented at a GCCS site specific level

[10] See Section 5.2.1.1, Security Bulletin Procedures.
[11] The DII COE Security Checklist is available as part of documentation supporting GCCS V3.0.

- whether the requirement is tested in the type certification process (not site-specific)

- whether the requirement is met via a procedure.

This section contains a discussion of the GCCS V3.0 area to be tested during the ST&E.

### 4.1.1 System Access Control

Access to the GCCS V3.0 is controlled using the I&A mechanisms provided by the OSs, X Display Manager, and DBMSs. Passwords are the primary and first level of protection into the system.

#### 4.1.1.2 Login/Password Mechanisms

The GCCS V3.0 employs the following login functions that are controlled via the UNIX or NT operating systems:

- RPC functions (e.g., remote login [rlogin], remote shell [rsh], etc.)
- telnet
- File transfer protocol (ftp)
- NT 4.0 login interface

The GCCS V3.0 also employs the following login functions that are controlled by the applicable database engines:

- Oracle login interface
- AMHS Sybase login interface

The GCCS V3.0 also supports network port/socket login functions:

- X Display Manager (xdm)
- Web application login interface

These mechanisms support a password challenge process using approved DES password encryption techniques.

#### 4.1.1.3 Network Daemon Control

Network daemon access control will occur through either disabling a service or providing DAC permission sets that allow access to specific groups of users. The network service configuration control files may be modified or the binaries of the network service commands may be modified.

#### 4.1.1.4 Host Access Control

The GCCS V3.0 Solaris hosts will be protected using the secure_rpc functions that supply key pairs to registered users and must be presented when network access is attempted via rpc and nfs operations.

#### 4.1.1.5 X Connection Control

The X Display Manager will be enabled with the .Xauthority protections. These protections provide a minimal amount of protection between an Xserver and Xclient.

### 4.1.2 User Account Management

The user account management mechanisms will be tested to ensure that the processing of user accounts is carried out in a logical and stepwise manner involving the elements *after* the physical user clearance management and access approval to a GCCS facility. The tested areas are:

- account addition.
- account modification.
- account disabling.

User access to the file system objects is controlled using the group assignments that are managed through the Profile Management services. The tested areas are:

- profile assignment (single and multiple).
- profile selection.
- validity of access controls instantiated through the profile features.
- validity of account groups access control.

### 4.1.3 File System

The GCCS V3.0 file system is required to be maintained in accordance with the least privilege concept. As discussed in section 3.2, Statement of Security Concerns, the propagation of the legacy applications into the GCCS V3.0 will represent an obvious contradiction to this policy. Notwithstanding, the SeComp process that is used in the DISA OSF GCCS Integration laboratory is providing a clearer view of the source of the file system objects that are maintained with promiscuous permission sets. The same statements apply to any files that may be generated during use that do not have a valid user or group ownership ID applied.

#### 4.1.3.1 Security-Related Object Control

The security-related file system locations such as /etc, /bin, /usr, /var, etc., should be maintained with a high adherence to the least privilege policy.

DAC testing for:

- The audit object controls.
- The I&A related database files and tables.

- The exported file system related objects and related support objects.
- The security tool related objects and reports.
- The network daemon control objects.
- The administrative related tools and program objects.
- The user home directory objects.
- The root environment control objects.
- NFS, NIS, rhost, hosts.equiv objects.
- Umask defaults.
- Set UID/GID program objects.

File System sanity validation testing.

- Development tool search.

### 4.1.4 Database

The Oracle and Sybase database implementations exist in the GCCS V3.0. AMHS is the sole user of the Sybase database. Oracle provides data services for all other database activities on the system, primarily, the JOPES database information.

Areas that must be tested and examined are:

- User access management; account sharing; UNIX account requirements.
- External and internal password requirements.
- OPS$ account requirements and risk-reduction management.
- Table access rights.
- Profiles and table access right relationships.
- Audit configuration.

### 4.1.5 World Wide Web (WWW) Services and Technology

The WWW servers must be tested to ensure that:

- Servers are operating only the approved software obtained via the GCCS CM Process.
- Browsers operating are the approved software obtained via the GCCS CM Process.
- TFM configuration requirements are met.
- All configurations reflect policy concerning automatic execution of downloaded software.

- Servers are maintained by GCCS security staff and in isolation from other command organization elements.

Additionally, the GCCS CM process is examined for its inclusion of the appropriate policies concerning the handling and processing of CGI scripts and automatically executing software (if applicable).

### 4.1.6 AMHS

The testing in the area of the AMHS will be limited to its configuration and execution as it relates and connects into the GCCS V3.0 system[12] . The GCCS V3.0 ST&E will focus on GCCS V3.0 issues; AMHS system operation is not a tested item.

### 4.1.7 System Configuration Maintenance

This will include the examination and testing of the system operational configuration maintenance and the correct application of the maintenance tools provided.

[12] AMHS, as a system, is certified and accredited as a separate action and not included with GCCS C&A.

### 4.1.8 System Backup and Restoration Procedures

This will include the examination and testing of the system backup and restoration procedures.

### 4.1.9 Audit Configuration and Archive Management

This will include the examination and testing of the system audit configuration and archive management procedures.

### 4.1.10 Software Configuration Management

This will include examination and walk-throughs of the GCCS CM process and procedures.

## 5.0 Minimum Security Safeguards Strategy

The strategy for providing security safeguards to the GCCS V3.0 includes the use of protection features inherent in the OSF evaluated software that willbe installed at each GCCS V3.0 site.

## 5.1 DII COE v3.1 Security Protection and Management

Security management provides the capability for managing the GCCS V3.0 account management security features. This includes the ability to control access to all GCCS V3.0 workstations, servers, applications and data protection. Implementation of security management capabilities will be provided as part of the DII COE V3.1 and kernel using the software described in the following sections.

### 5.1.1 Security Manager

The Security Manager is a DII V3.1 kernel capability that provides a set of services for administering users and groups. The Security Manager provides tools to

- manage user accounts.
- map users to profiles.
- manage profiles.
- map applications (or system functions) to profiles.

The Security Manager also provides a menu profiling function which updates profile menu data files per Integration & Runtime Specification (I&RTS). Additionally, the Security Manager will set up other user and profiled-based access permissions via "hooks" to kernel components.

A profile database will be implemented to store the data which provides the relationship between users, profiles and applications (or system functions). There exists a "local" profile database which can be accessed from a directory local to the workstation, as well as a "global" profile database which can be accessed via NFS mount. The profile database provides a number of APIs which will allow other components to access/update profile database information.

### 5.1.2 Profile Selector

The Profile Selector is a DII COE V3.1 kernel capability that provides a mechanism for users to select profiles at login or change profiles during a user's session. The Profile Selector, which is an optional capability that can be turned off by the site administrator, provides the following features:

- Allows a configurable number of selections, either 1 or n, where the user may be restricted to selecting one profile only or can select any number of profiles up to n where n is the total number of valid profiles for the user.

- Allows the administrator to restrict the occupancy of a profile to one user in an administrative domain, e.g., the capability to lock a profile on a profile by profile basis.

- Configurable audit capability, e.g., ability to audit user role(s).

A last role table will be implemented to store the user's most recently selected profiles. This file will be located in the user's home directory

There exists a concept of global and local profiles. Local profiles are only available to a user on the specific workstation where the local role has been defined in the local profile database. Global profiles are available to the user on all workstations where their login is supported.

### 5.1.3 Session Manager

The Session Manager is a DII COE V3.1 kernel capability that provides a mechanism to set up the user's work environment. The Session Manager will display icons in the CDE application manager representing the user's profiles system functions. Additionally, the Session Manager via "hooks" to COE components will set up other profile-based access permissions.

The Session Manager is a transient process which reads the LastProfile file at startup. The LastProfile file will contain either the profile selection(s) which the user selected at login or the user's last profile from their previous login session. The Session Manager then retrieves the list of application(s) for the selected profiles(s). The list of applications may be reduced if the applications in the profile(s) are not available at the login host. The Session Manager paints (or repaints in the case of profile switching) the icons in the CDE Application Manager and passes the user's profile(s) to the process executive via a socket. The Session Manager then exits until such time as it is reinvoked at login or during the user's session (for profile switching).

### 5.1.4 Profile Manager

Account groups and Profiles work together in a very tightly coupled manner. Sites are expected to maintain the Profiles required for the site, however, Account Groups are established by the DISA JIEO and provided to the GCCS sites in segment form.

The Profile Manager is a DII COE V3.1 kernel capability that provides the capability to support multiple user work environments for a single user which allows the user to select multiple profiles and change their profile configuration during a login session. The Profile Manager starts during the system boot to manage GCCS V3.0 processes including boot, background, session and session_exit processes. The Profile Manager manages the process environment, e.g. user and group ids and environmental variables and also supports multiple execution environments for multiple profiles (e.g., enables profile switching without logout).

A single user session may include multiple profiles where each profile defines the runtime environment for each process, e.g., group id(s) and environmental variables. The Profile Manager creates the runtime environment for each profile in the user's session. The runtime

environment is determined from the profile data and the base Account Group of the profile. When a user process is launched, it is launched within the runtime environment of its associated profile.

## 5.2 GCCS V3.0 Security Configuration

The GCCS V3.0 security configuration is established within the GCCS V3.0 installed software base, and is not intended to be modified in order to meet the GCCS V3.0 certification requirements. This is generically referred to as having GCCS V3.0 security established "out-of-the box".

### 5.2.1 Security Configuration Maintenance

Once the GCCS V3.0 base is installed and the system becomes operational, maintenance of the security configuration is required on a daily basis. The Security Maintenance and Reporting (SeMoRe) tool is provided to aid this effort.

The certified GCCS security configuration is based on the following tenets. The parenthetical references point the security staff to the applicable implementation sections in the *GCCS Version 3.0 Trusted Facilities Manual*:

- Protecting and controlling root or equivalent "super-user" type privilege is paramount. (Section 5, User Management).

- UNIX systems: The */etc* directory is the administrative and security directory. No files with world write permissions will exist within this directory, and group write is permitted only when required for normal operations. (Section 7, File Management).

- Controlling access to the interconnected system components begins with access point identity (i.e., network and communication connections and login methods) and applying the appropriate controls. Access control is maintained through pro-active and re-active configuration and audit trail monitoring. (Section 5, User Management; Section 10, NIS, NFS, and DNS Management).

- Personal workstation NT operating system platforms will be restricted to using the Xterm interface to establish a xterm client to server connection to the controlled Solaris server platforms.

- PCNFS programs will not be permitted to be installed on the NT personal workstation platforms used in the GCCS.

- Only the GCCS approved file system objects and executable processes (e.g., available through the GCCS CM process) that are required to complete the operational mission are maintained on a GCCS platform. No development tools are maintained or available in the operational system environment. (Section 6, Platform and System Management).

- UNIX systems: The system umask value will be maintained at 002 until such time that world-write is eliminated as a legacy application requirement. The root-user umask will be maintained at 077 to avoid incidental occurrences of excessive permissions on root created objects. (Section 5, User Management).

- Solaris UNIX systems: The Network Information Service Plus (NIS+) security level will be maintained at Level 2 (AUTHDES). Netgroups will be established and maintained for all connecting hosts, including non-NIS+ systems and used to control all host access through NFS controls and *r* command execution. The *nsswitch.conf* will be maintained with NIS+ tables as the primary user and host database files. (Section 10, NIS, NFS, and DNS Management).

- Hewlett-Packard/UNIX (HP/UX) systems:. At that time, the NIS tables will be used to control user access. Netgroups will be established and maintained for all connecting hosts. (Section 5, User Management; Section 10, NIS, NFS, and DNS Management).

- UNIX systems: The *.rhosts* files will be populated only with netgroup names unless a legacy mission application requires additional information. (Section 5, User Management).

- Auditing will be enabled for the approved list of audit flags. (Section 9, Audit Management).

- Auditing will always occur for all users to include audit of the root-user. (Section 5, User Management; Section 9, Audit Management).

- Home directory permissions will be maintained at 0775. (Section 5, User Management; Section 7, File Management).

- The root- or super-user will not be capable of direct login at the console or using network login mechanisms. (Section 5, User Management).

- The finger network application will be disabled. (Section 6, Platform and System Management).

- The network "snooping" commands will be disabled. (Section 6, Platform and System Management).

- UNIX systems: Binary executables are maintained at permissions of 111 (execute only). Shell executables, in particular SUID or SGID shell executables, will be maintained at permissions of 555 (read-execute). (Section 7, File Management).

- No login accounts will be maintained with a bogus default shell designation and locked password fields. (Section 5, User Management).

- All encrypted password fields will contain either a locked password and/or encrypted password. (Section 5, User Management).

- All password construction will include at least eight non-dictionary decipherable characters and two numbers or special characters. (Section 5, User Management).

- Unknown or unapproved file systems are never mounted in the operational GCCS environment. (Section 6, Platform and System Management).

- File system security and integrity is ultimately and more effectively gained through sensible DAC and user privilege control (through user account and profiling control mechanisms) management[13] (Section 6, Platform and System Management).

- Primary misuse prevention is accomplished through the diligent maintenance in support of the security tenets[14] (All sections apply).

- Primary misuse detection is accomplished through the diligent examination of audit and security configuration compliance tool reports. (Section 9, Audit Management; Section 6, Platform and System Management).

- Database passwords will be unique and applied to the internal and external authentication mechanisms where required. No external password will be operationally maintained for the purpose of over-riding internal DB authentication controls. (Section 8, Database Management).

- Establishment of a standard countermeasure plan or operating procedure to execute when misuse is detected. Once abnormal behavior is detected, the countermeasure procedure is followed that identifies the who, what, when, where, and why of the access, corrects the anomalies allowing the access, and then assesses the damages. (Section 3, Trusted Facility Management Concepts).

- Establishment of an SOP by each GCCS site to consistently dictate the site specific details of maintaining the GCCS security configuration. (Section 3, trusted Facility Management Concepts).

---

[13] Security implementation in the current GCCS implementation is not blind to the legacy application requirements and needs of the mission. Efforts are underway to bring the legacy applications into SeMoRe and ensure that new applications are developed in compliance with the security requirements.
[14] This is not meant to say that additional specialized detection mechanisms should not be implemented. Higher security environments may even require these mechanisms. For many environments, however, pro-active monitoring of the system configuration and audit logs will provide the information required to detect misuse attempts and assess damages by examining the historical system records. In fact, this method is sufficient for most system-high classified system implementations when rigorously applied and adapted to a systems security policy.

Sites that deploy a www server are required to use the current version of the server software available through the GCCS V3.0 CM library. Likewise, sites will use the current version of the browser software available through the GCCS V3.0 CM library. (Section 12, WEB SERVER AND BROWSER MANAGEMENT)

The www servers and browsers are required to be maintained in accordance with the requirements and guidelines as defined in this TFM and the policy and requirements documents the TFM supports. This means that the www servers will maintain the same controlled access and audit monitoring features as is typical of the GCCS V3.0 configuration and environment. (Section 12, WEB SERVER AND BROWSER MANAGEMENT)

Web servers maintained for the GCCS are to be maintained on an isolated, for GCCS only, GCCS controlled network server where possible, but required, in all cases, to be under the of the GCCS security staff and not shared with other command organizational elements. (Section 12, WEB SERVER AND BROWSER MANAGEMENT)

The www server is not permitted to export directories or file systems. (Section 12, WEB SERVER AND BROWSER MANAGEMENT)

The following services are required to be disabled for general use on the www server:

- ftp
- telnet
- rpc
- Xterm
- pcnfs
- nfs
- mail services

The I&A database, tables, and files are required to be maintained for only those personnel authorized to access the www server for administrative or maintenance purposes. (Section 12, WEB SERVER AND BROWSER MANAGEMENT)

Until notified otherwise, JAVA will be disabled on all web servers and teleconferencing browsing software. (Section 12, WEB SERVER AND BROWSER MANAGEMENT)

## 5.3 Security Bulletin Procedures

The GCCS is composed of multiple operating system and kernel software, software applications, database management systems, and database applications. The GCCS architecture is primarily client-server and the systems interoperate across a network backbone that provides connectivity to the GCCS sites around the world. Additionally, sites connect via remote telecommunications connection paths. Given this description, it can be stated that the GCCS software and system components interact in a tightly coupled fashion, with dependencies existing in the architectural framework that may affect the entire global network when a single component functionally misbehaves.

These facts give rise to a great deal of concern and effort to ensure that the system components remain at a high level of consistency across the network of GCCS sites. A rogue or mustang system component may cause a ripple in the operational system that may be felt in and possibly disrupt the operational integrity and reliability of the entire GCCS. It is therefore of extreme importance that all GCCS sites are operating only with approved versions of hardware and software. Furthermore, the GCCS Security Policy does not permit the introduction of unauthorized or unapproved software or hardware into the GCCS.

There are many reasons why system software or hardware can become out-of-sync with the global system version. This section will deal with one reason in particular, the installation and operation of field patches to the software or hardware that are broadcast via the CERT, ASSIST, or other security bulletin notification service. For the remainder of this section, the name CERT will be used and implies any security notification network or service that may be approved of for use by the GCCS Chief Engineer as an appropriate authority for recommended modifications to the GCCS software and hardware baseline.

This section will describe the process and procedure by which the CERT bulletins can be quickly but fastidiously processed and distributed to the GCCS sites. In general, the process will include:

- receiving and acknowledging (by the OSF to the GCCS sites as being processed)
- qualifying (whether or not a particular bulletin is relevant to the GCCS)
- integrating (segmented, if required)

- testing (the qualified bulletins and recommended patches/actions must be tested in the COE to ensure compatibility)

- distributing (made available to the GCCS sites for installation into the system.)

The remaining sections discuss these process steps.

### 5.3.1 CERT Bulletin Fielding Process

The CERT Bulletin Fielding Process (the Process) is designed to accomplish the receipt, qualification, testing, integration, and distribution of recommended changes or patches pertaining to the GCCS operational software components. The Process centralizes the approval and change distribution activities that may effect modifications to the approved GCCS and/or DII COE baseline. The intent is to ensure that recommended changes or patches are catalogued properly and do not have a negative affect on the GCCS and/or DII COE baseline. History has indicated that implementing unauthorized changes into the GCCS and/or DII COE baseline can have severe repercussions on the operational integrity and reliability of the GCCS.

Management of the Process must support the receipt, qualification, testing, and integration of recommended CERT or ASSIST bulletin recommendations. Supporting the Process involves staff participation from DISA OSF GCCS Integration, Quality Assurance (QA), and Configuration Management (CM) staff resources.

#### 5.3.1.1 Receiving and Acknowledging Receipt of CERT Information

The CERT information is distributed to recipients on a subscriber basis and is obtained via a subscription to the information. For the GCCS, the subscriber and recipient of this information is within the DISA OSF GCCS Integration department. Once a notice is received, it must be determined whether or not the information applies to the software that is used in the GCCS. If the information does not apply, then no integration activity is required. The GCCS sites need to be provided information concerning all CERTs, however, and a notice should be made to the sites

that this CERT is not applicable to the system and no further action is being taken.

If the CERT does apply to the GCCS, then the Process goes to work. The Process steps include:

1. The sites are notified that the CERT has been received and is in the CERT Bulletin Notification Process.

2. The Process staff resource determine the actions required by the CERT.

3. The Process staff resource integrate the CERT recommendations into the GCCS integration laboratory suite.

4. The Process staff resource test the recommended actions using the functional and security test procedures. If successful, determines the appropriate packaging (i.e., segmentation, checklist update, etc.) for distribution of the update product.

5. The Process staff resource forwards the update product to the configuration management process where the update product will be tested in the quality assurance laboratory suite.

6. Once successful testing is completed in the quality assurance test lab and the update product is ready for distribution to the sites, place the update product on the download server to be pulled by the sites.

7. Notify the sites via an GCCS administrative newsgroup that the update product is available for the CERT notice.

#### 5.3.1.2 GCCS CERT Database

The CERT notices that are pertinent to the GCCS will be compiled in an on-line database that will be available to the GCCS sites for reference purposes. The DISA GCCS integration staff subscribe to and receive the CERT information at the OSF.

#### 5.3.1.3 Acknowledging CERT Notices

All CERT notices require an acknowledgment of receipt to the GCCS ISSOs. This acknowledgment should cover whether or not the CERT

pertains to the GCCS, and if it does, the action expected to be taken by the DISA OSF GCCS Integration staff. This is necessary because many of the GCCS site administration and ISSO staffs are required to report the notice of a CERT (many sites subscribe to this information themselves) and a description of actions to be taken to the site ISSO.

#### 5.3.1.4 ISSO Newsgroup Usage

The special-access, ISSO newsgroup (if available) should be used to distribute the CERT activity information to the GCCS site ISSOs and staff security managers. This should not be a general access capability because of the potential volatility of the information shared within the ISSO community.

#### 5.3.1.5 Qualifying CERT Notices

Not all CERT notices that are published will result in actions via the Process. Not all CERTs apply to the software or hardware base that comprises the GCCS. Therefore, the GCCS integration staff must determine which CERT notices are valid for the GCCS and which are not. Again, all notices are acknowledged as being received and reviewed by the GCCS integration staff. Currently, the DISA OSF GCCS Integration staff make this determination.

#### 5.3.1.6 Testing and Integrating The Recommended Actions

The CERTs that are pertinent to the GCCS and the recommended actions must be integrated into a stable GCCS COE suite. In the case of an operating system patch, this will mean that a patch segment is developed. In the case of a file permission change, this will mean an update to the GCCS TFM Security Configuration guidelines, with possible follow on actions to the security configuration checking tool employed. This process may be identified as the update product.

Testing the recommended actions is vital to the maintenance of the stable GCCS baseline. Indeed, the primary purpose for the Process is to ensure change compatibility with the GCCS baseline and security requirements. The integration laboratory testing of the recommended actions may actually take place prior to the formal development of the update product for expediency and to determine if an update product is realistic when the test results are considered. For example, if the CERT recommended actions degrade the usefulness of an operational software or database application, then it may not be feasible to implement the recommended action until further analysis and development can occur.

In these case, the GCCS sites must be notified of the results and the anticipated direction concerning the implementation of the recommended action.

#### 5.3.1.7 Update Product Distribution

The final step in the Process is to make the update product available to the GCCS site. This part of the Process requires cooperation with the DISA OSF GCCS CM process and management to expedite the handling of CERT related products in order to make them available to the field as soon as possible.

ANNEX F TO ENCLOSURE 2
TEST AND EVALUATION MASTER PLAN (TEMP) CONOPS

1. **GCCS V3.0 Test & Evaluation Summary**. The overall test and evaluation strategy for GCCS V3.0 includes a modified developmental test approach that leverages the developer testing with user involvement, laboratory testing, user beta testing, and formal operational testing. The testing will verify the status of engineering development progress within each segment, verify that design risks have been minimized, substantiate achievement of technical performance requirements, measure the effectiveness of the functional requirements, and certify readiness for developmental testing and operational test (OT). Readiness reviews will be conducted before major milestone DT and OT events. This Annex does not seek to fulfill the functions of the TEMP but merely to highlight the overall test approach. For more specifics, refer to the TEMP, Modified Developmental Test (MDT) Plan and/or OT Plan (The TEMP is being coordinated separately from the EPIP).

a. Test and Evaluation Philosophy. The T&E philosophy incorporates the following concepts:

(1) Stronger user involvement. Early involvement from the user community is the key to a successful DT approach. Working closely with the user community in developing GCCS capabilities helps ensure user requirements are met and capabilities can be evaluated in a user-oriented environment.

(2) Extensive use of existing software. GCCS will integrate a wide assortment of software systems into the COE on a continuing basis. The applications to be integrated include existing command and control systems, and systems created by the Services. One of the goals of GCCS is to fully integrate selected Service applications into the DII COE to avoid large and lengthy development efforts.

(3) Use of event driven scenarios based on requirements as a means of evaluating the effectiveness of GCCS products and application software in a user-oriented environment.

(4) Use of exercise-like scenarios during end-to-end testing to evaluate the effectiveness of the multi-node environment and benchmark the thresholds of the system.

(5) Customizing the test and evaluation process according to segment type and the magnitude of the risk involved with inserting the segment into the operational GCCS system. Because the GCCS is made up of applications developed by each of the Service components as well as COTS software the testing completed by the development activity will be factored into the independent DT&E activities.

(6) Ensure that the OT&E interests are considered during DT&E events to include the participation of the OT&E community at DT planning events, DT events and DT analysis and reporting efforts.

(7) Use of development test data by the operational test community as preliminary operational data for input into their assessments supporting GCCS Version 3.0 determination of operational effectiveness and suitability and minimizing the need for collecting data multiple times.

b. DISA Developmental Test and Evaluation Methodology. The objectives of the developmental test and evaluation for GCCS are to reduce the risk of adverse impacts when inserting new segments and technology into the operational system, and determine the effectiveness and supportability of the component in a user-oriented environment. DISA will oversee and conduct DT for the GCCS Version 3.0 development and integration effort prior to Operational Test and Evaluation (OT&E) efforts. The DT&E methodology incorporating the DT&E philosophy into a three staged DT approach is depicted in Figure F-1 below and detailed in subsequent paragraphs within this section.

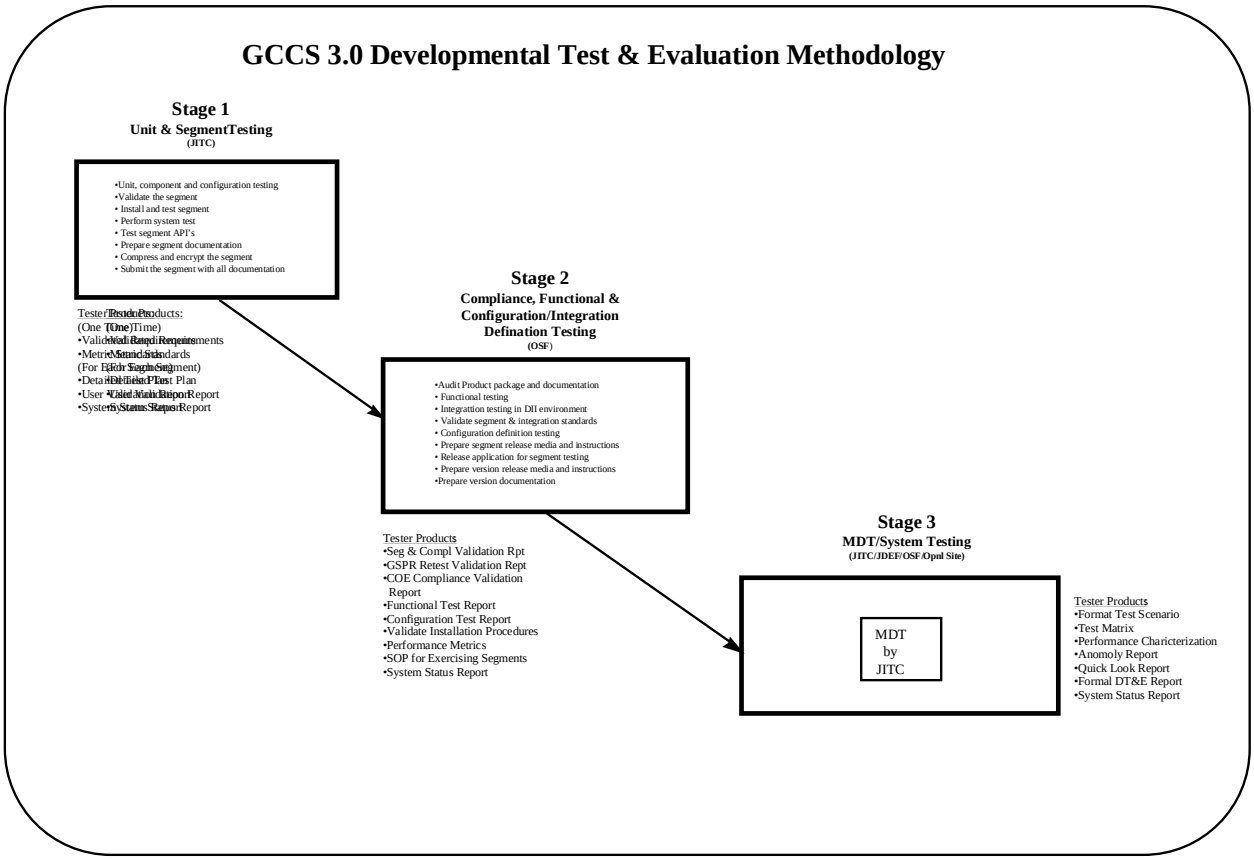



**Figure. F-1. GCCS 3.0 Developmental Test & Evaluation Methodology**

(1) **Unit and Segment Testing**. Stage 1 encompasses Unit and Segment Testing conducted at the developer's facilities. The segments or units will be developed and documented in accordance with MIL-STD-498. The segments shall then be validated by Subject Matter Experts (SMEs.) JITC will provide oversight and guidance to the developer to ensure exit criteria, shown in Table III-1 from Stage 1 has been met and SW Metrics are captured to effectively measure Stage 1 events.

a. The Designated Development Agency (DDA) for all segments and major configuration items will complete a Formal Qualification Testing (FQT) process in accordance with MIL-STD 498 during unit and segment testing. A Software Test Plan (STP) will document the developer's plans for conducting FQT. The developer will define a preliminary set of engineering requirements for each computer software configuration item (CSCI). As part of FQT, the developer will define a preliminary

set of qualification requirements for each CSCI. These requirements, to be documented in the preliminary Software Requirements Specification (SRS) for each CSCI, are to be consistent with the qualification requirements defined in the system specification. The developer will identify and describe the test cases for each FQT in the software test description (STD) for each CSCI.

b. FQT will consist of unit, component and configuration item testing. Unit testing ensures the component algorithms and logic employed by each unit are correct and that the unit satisfies its specified requirement. Component testing ensures that the component algorithms and logic are correct, that they satisfy the specified requirements and that the subordinate components and units are integrated properly. Configuration items testing ensures that the entire program operates according to design specifications.

c. Throughout the Stage 1 process the development proponent/users will be involved as both observers and commentators on the test results. The schedule and location for development proponent/user participation will be dependent on specific segment and application development.

d. The DDA will then deliver the software to the government upon satisfactory completion of FQT in accordance with MIL-STD 498, and per guidance contained in the Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 3.0, Specification/Draft, dated 1 January, 1997. Satisfactory completion of this testing is a prerequisite for the subsequent testing stages.

**(2) <u>Compliance, Functional, and Configuration Definition/Integration Testing</u>.** Stage 2 includes Compliance, Functional and Configuration Definition Integration Testing. All GSPRS that were identified to be fixed are re-tested and validated as corrected or returned. All segments are verified as complete and integrated into the GCCS version. Installation instructions and system documentation is developed and verified. Users will participate in or witness testing of selected GCCS V3.0 capabilities in this stage. JITC will provide oversight and guidance to JIEO to ensure that the exit criteria for Stage 2 has been met and software metrics are captured to effectively measure Stage 2 events.

a. Compliance Testing. Segments will be delivered to the GCCS program in accordance with the Configuration Management Software and Documentation Delivery Requirements, Version 2.0. All segments will have been functionally proven/accepted by development proponent prior to delivery to the GCCS program. All segments to include selected COTS and GOTS software components proposed for integration into the core system will be compliance tested in accordance with the DII I&RTS (low level integration with COE & associated segment) to ensure that they have been integrated with the COE and that they work with associated segments in the COE and do not damage the environment. A compliance checklist extracted from the I&RTS is utilized to validate each segment.

b. Individual Segment Functional Testing. Random sampling of the individual segment functionality using developer provided test plans (in the absence of test plans, individual segment test checklists and procedures will be developed) will be tested. The functional testing also includes validation of the system build/upgrade procedures (Solaris, HP, and NT), validation of segment installation instructions (Solaris, HP, and NT), validation of problem reports/fixes, and backward compatibility between versions.

c. Configuration Definition/Integration Testing. Configuration Definition testing involves integrating CSCIs with interfacing hardware configuration items (HWCI) and CSCIs, evaluating the resulting groupings to determine whether they work together as intended, and continuing this process until all CSCIs and HWCIs in the system are integrated and evaluated. It is designed to verify the proper integration of the configuration items with each other, and with the system environment. This process is designed to test the critical functionality of a critical mass of applications after integration with a GCCS version. This testing includes validating interfaces with Service and CINC applications migrating to or coexisting with GCCS. The testing will be performed in a lab environment at the OSF. Multiple GCCS nodes (a node includes a database server, application servers, and client workstations) will be utilized during this stage to validate database synchronization and system interfaces across a simulated wide area network.

(3) **Modified Developmental Testing (MDT).** Stage III consists of beta testing designed to verify integration, lead to a recommendation of acceptance, and prepare the system for an Operational Test Readiness Review (OTRR) with full user involvement. The user beta testing will evaluate if the functional and technical user requirements are met. All interfaces will be validated as well as corrections to priority 1 and 2 GSPRS that were identified for this stage. JITC, working with user subject matter experts, will ensure that the exit criteria for Stage III has been met and software metrics are captured to effectively measure stage III events for entrance criteria for the OTRR.

a. At this stage, JITC working with users, will verify the installation procedures, software load programs, and interfaces for each platform type. All platform types will be integrated, to include SUN, HP, and PC. The certified /accredited security features and procedures will be in place. Representative System Administrator, Network Manager, Security Manager, and Database Managers will validate their procedures. The IDTA will document any abnormalities. The PMO will either fix the problem or revise the installation procedures to document the error/workaround. The testing will validate that the mission specific software performs as designed under realistic operational constraints. The test will exercise the system in a multi-node environment. This will serve to validate the Wide Area Network (WAN) configuration. Using the provided user level documentation, the users will, with the aid of the JITC test team, evaluate the systems capabilities as defined in the requirements document at the test locations, exchanging representative data.

b. Service feeder systems will be incorporated into the multi-node environment to conduct an end-to-end evaluation. (End-to-end testing incorporates service and site unique feeder systems supporting GCCS functionality.) At least one feeder system (or service) shall work at version 2.2 to verify the degree of compatibility with release 3.0. With the feeder systems up, stress events will be executed to include but not be limited to application server loading, database queue stacking and Xterm sessions. OT&E team members will be involved at this point as independent observers for data collection purposes in preparation for subsequent OT activities.

c. Acceptance. Acceptance and verification that the DT&E of GCCS v3.0 is complete when DT&E analysis and results show that the user defined exit criteria have been satisfied. Formal reporting by the DT&E effort is provided to the developer, user, and operational tester as support documentation at the OTRR.

2. Project Lead Summary. Table F-1 below breaks out major sub-projects for the core DISA lead effort. Similar Service lead project efforts need to be initiated and identified to the Joint Staff and DISA D2 Program Office to ensure full coordination of efforts. GCCS Release 3.0 scope was limited to make sure a new release reached the field quickly and to replace equipment and database tools needed for functionality expected in future minor releases. It is critical to ensure with this release that the basic infrastructure and capabilities are available, so the user community is positioned for a new paradigm, when Service or sites select additional applications that enhance their productivity.

Service and Agency teams will need similar sub-projects to work with the Core team. Service and Agency teams need to keep the GCCS PMO apprised of their POCs to ensure smooth coordination of this major transition effort.

**TABLE F-1: GCCS Release 3.0 Core Sub-Projects**

| Sub-Project/Lead | Sub-Project Description |
|---|---|
| Segment Development : DISA/D68, EA, & dev | Executive Agents develop segments according to D68 GCCS System Engineering guidance (Prep: Nov 96 — Apr 97). Deliver segments and documentation to OSF (Execution: May — Jul 97). NOTE: Solaris first, then HP and finally NT. |
| MDT Stage I: DISA/JITC | Identify SMEs ( Prep: Apr — Jun 97). Capture user feedback on GCCS applications early by having users participate in a modified developmental test at the developer sites. Use feedback to enhance product before delivery or to generate list of new requirements to run through the prioritization process (Execution: Jul - Sep 97) |
| Pre-Production: DISA/OSF | Prepare plans and procedures (Prep: May — Jun 97). Do segment level and system level testing. Check for compliance with guideline — especially security Year, 2000, and DII COE guidance; verify segment documentation complete and correct and build system level documentation.; provide configuration management between delivery from vendors and release to the field. (Execution: Jul — Sep 97) |
| MDT Stage II: DISA/JITC w/OSF | Capture user feedback on GCCS applications early by having users participate in a modified developmental test at the OSF. Use feedback to enhance product before delivery or to generate list of new requirements to run through the prioritization process. (Prep: May — Jun 97) (Execution Jul — Sep |

| | |
|---|---|
| | 97) |
| Freeze Baseline Milestone<br>DISA/D68<br>DISA/D2 | GCCS System Engineers (D68) determines whether the target release deadline will be achievable with the target capabilities. If so, project is on track. If not, then segments that have not passed all the quality checks will be put off until the next release, unless the "operational utility" is such that a delay is warranted. The PMO, D2, with make the schedule slip decision, based on feed back from C2 Functional Proponent, J3. (Mid-Sep 97) |
| MDTRR Milestone: DISA/JITC | JITC will host a Modified Developmental Test Readiness Review, to ensure we are on track and ready to conduct MDT Stage III at the laboratory sites (late Sep 97). |
| MDT Stage III/DISA.JITC<br>w/OSF<br>w/labs & beta test sites | Capture user feedback on GCCS applications early by having users participate in a modified developmental test at the GCCS labs. Use feedback to enhance product before delivery or to generate list of new requirements to run through the prioritization process (Prep: May — Sep 97); (Execution: Oct — Nov) |
| ST&E: DISA/D25 | Check out the security features within GCCS as part of the DII COE and as part of the mission applications |
| New Equipment Training:<br>DISA/ISESF | Provide New Equipment Training to the 39 IOC sites and coordinate NET with other sites as requested -- new functionality for system or database administration due to new DII COE and tools. (Plans, materials, and coordination: May — Sep 97); (Support MDT III and OT&E: Oct — Nov 97); (Follow-on |

| | |
|---|---|
| | to support fielding: Dec 97 — Apr 98 |
| OTRR Milestone: JITC | Based on MDT III and ST&E, JITC conducts an Operational Test Readiness Review prior to engaging the operational sites (Dec 97 |
| OT&E:<br>DISA/JITC | Conduct the Operational Test and Evaluation for GCCS at operational sites in five regional area (selection of sites is critical factor for fielding, since these site will become major hubs as other sites transition). (Prep: Jun — Oct 97); (Execution: Jan — Feb 98) |
| SOR Decision Milestone:<br>JS | Based on the OT&E, a Flag Office Panel decides whether to fully field GCCS 3.0 or generates a list of required fixes needed prior to full fielding (Feb 98) |
| Fielding: | |
| DISA lead | Field to 39 IOC sites. Provide initial training and any required follow-on site support |
| Services lead | Field to Service/Agency server & remote sites |
| Site Accreditation: | To connect to the SIPRNET, each site must maintain accreditation. |
| Sites | Once GCCS 3.0 is installed, each site needs to do local accreditation and forward copy to the Joint Staff as a completion item. (Prep: Jul 97 — Apr 98); (Execution: May 98) |

(INTENTIONALLY BLANK)

ANNEX G TO ENCLOSURE 2

TRAINING CONOPS

## 1.1. Introduction

This Annex is a supplement to the basic Evolutionary Phased Implementation Plan (EPIP), Annex J-Economic Analysis (EA) & Annex H-Production Operations Transition Plan. The purpose of this document is to define the concept for the evolution of existing training programs to support version 3.0 transition and beyond. This updated training will meet the operational requirements of the GCCS community for version 3.0 Stage 1 and Stage 2 fielding scheduled to begin in 2d quarter, FY98.

## 1.1 Scope

This document is written for planning purposes and may be updated as necessary to reflect the dynamic nature of the evolutionary process. Every effort has been made to associate training responsibilities with the appropriate service or agency, based on known requirements.

## 1.2 Training Requirement

GCCS training for version 3.0 will be developed by two parallel efforts. The first effort, hereafter called Block 1 training, will present material designed to familiarize the technical operator with upgraded versions of the Solaris operating system and the ORACLE Database Management System provided by GCCS version 3.0. The target audience for Block 1 training will be current GCCS Systems Administrators, Database Administrators, and Security Administrators. The second effort, hereafter called Block 2 training, will present material designed to familiarize the operational user with new functionalities provided by GCCS version 3.0. The target audience will be the operational users responsible for developing and using C4I products, hereafter called the Warfighter. An additional Block 2 audience, hereafter called Future Users, is composed of all future GCCS users who require training.

## 2.0 Background

The GCCS Management Structure, CJCSI 6721.01 states that GCCS is a means to implement the Command, Control, Communications, Computers and Intelligence for the Warrior (C4IFTW) concept. The two

staged fielding plan will provide for enhanced technical capabilities under version 3.0 during Stage 1 fielding and enhanced functionalities under version 3.0 during Stage 2 fielding.

**2.1 Assumptions**

Previous success and failure have dictated the following assumptions:

1. Block 1 training development will be completed prior to Stage 1 fielding of version 3.0.

2. Block 2 training development will be completed prior to Stage 2 fielding of version 3.0.

3. Funding will be available to support Block 1 & Block 2 training development.

4. The training requirement will remain relatively stable.

5. Fielded sites shall send current administrators with adequate experience to Block 1 training.

6. All statutory requirements IAW Title 10, USC, remain in effect.

7. Block 1 training will be provided to each site within two weeks prior to fielding.

**2.2 Responsibilities**

Training is under development to support several critical events. Transition Training will be provided to participants of the modified development test (MDT) and the operation test (OT) at the OSF in Sterling, Virginia. This will precede the fielding effort and will require subject matter experts to develop and present the transition training. Institutional training for Block 1 fielding will be developed and ready for presentation in existing schools (AETC, JTO) by 1 January 1998. Every effort will be made to incorporate all lessons learned during the transition training into the institutionalized program of instruction..

Each segment, which requires Institutional training, has been assigned to a responsible agent. Although each agent will be responsible for the development and presentation of training, coordination will be accomplished through the DISA GCCS Training Manager (GCM).

**Table G-1. Training Matrix**

| SEGMENT | AETC | JTO | NAVY | UNKNOWN | BLK 1 | BLK 2 |
|---|---|---|---|---|---|---|
| Solaris OS 2.5.1 | X | | | | X | X |
| Oracle 7.3.2.3 | X | | | | X | X |
| Common Desktop Environment* | | | | Vendor | X | X |
| TP Edit | | X | | | X | X |
| TARGET | | X | | | X | X |
| System Security | X | | | | | X |
| COP | | | X | | | X |
| Intelligence Feed (COP) | | | X | | | X |
| Tactical Ballistic Missile Defense (TBMD) | X | | | | | X |
| Theater Battle ManagementControl System (TBMCS) | X | | | | | X |
| DARWIN | | X | | | | X |
| Airfields | | X | | | | X |
| METOC | | | X | | | X |
| JPET | | X | | | | X |
| JTAV | | X | | | | X |
| JPAV | | X | | | | X |
| MIDB | | | X | | | X |
| SYBASE (MIDB) | X | | | | | X |

*Note - The Common Desktop Environment has training on demand through the TriTeal Corporation. DISA POC is Ms. Nancy Blevins, (703) 681-2316.

## 3.0 Training Concept

The concept is to present training, during each of the two stages, to a specific audience. The target audiences are Current System/Database/Security Administrators, Operational Users (Warfighters), and Future Users. Every effort will be made to leverage existing technology in order to reduce training costs and improve the transfer of knowledge. Training media to be considered are Video Tele-Training, Video Tele-conferencing, Embedded Training, CD ROM, Formal

Instruction, Web Based Training, On-Line Help, and Self-Paced Tutorials (Users Help Book).

### 3.1 Transition Team Training (MDT/OT)

Transition training will focus on the MDT & OT participants prior to the beginning of the development test. Additional participants include JITC and members of the Help Desk. This training will replicate the actions that administrators must take to transition form version 2.2 to 3.0. The instruction will involve physically transitioning a GCCS 2.2 database server to a version 3.0 database server. Subject matter experts will provide information seminars and will be available for questions. Both Sun and HP platforms will be addressed. This training will be provided at the OSF with limited seating due to the number of available terminals. POC for transition training is Mr. Ken Love, 735-8675.

### 3.2 Block 1 Training (Stage 1)

Block 1 training development will be completed in parallel with version 3.0 developmental/operational testing. This is necessary to allow for the development and validation of installation procedures and for the training of transition team members prior to fielding. The presentation of Block 1 training to the target audience will be centrally located and will use a hands on approach. The actual location for Block 1 training will be determined by the fielding schedule and site constraints. It is anticipated that training will be conducted either at the OSF in Sterling Virginia or at regional training sites to be identified at a later date.

Due to the extremely technical nature of Block 1 materials, formal classroom instruction is preferred. Version 2.2 NET training success will be used to model this effort. It is essential that the target audience be made up from current System Administrators and Database Administrators. Previous attempts to insert untrained, inexperienced personnel into this effort have slowed down the training and reduced its effectiveness. For this reason, participants will be closely monitored. For best results, this training will be presented no earlier than two weeks before fielding. This will allow the participants to return to duty and begin work on version 3.0. The most important aspect of Block 1 training will be a complete documentation package that will be available to administrators on-line.

### 3.3 Block 2 Training (Stage 2)

Block 2 training must meet the immediate requirements for version 3.0 Stage 2 fielding as well as sustainment requirements created as we transition form GCCS version 2.2 to 3.0 and beyond. Therefore, Block 2 training must be further defined in order to meet the needs of two distinct target audiences. Block 2 New Equipment Training (NET) will address the training requirement for the Warfighter and Block 2 Sustainment will update the existing training program for the Future Users. Block 2 NET must expose the Warfighter to the enhanced functionality of GCCS provided by Stage 1. This training should be representative of any additional functionality not provided by version 2.2. Once again, it is essential that the target audience be made up from current GCCS operational users. The training will focus on the differences between version 2.2 and version 3.0. Participation by untrained, inexperienced personnel is not recommended. For best results, this training will be presented no earlier than two weeks before fielding version 3.0 Stage 2. This will allow the participants to return to duty and begin work with the new functionality as soon as possible.

Block 2 Sustainment training will be developed and integrated into existing course material by the responsible agent in parallel with Block 2 NET. Beginning with version 3.0 fielding (Stage 1), all training materials will be revised to reflect enhanced technical capabilities of GCCS version 3.0. As version 3.0 Stage 2 is fielded, additional revision of sustainment training will be required prior to fielding. This will ensure that Future Users receive the latest training prior to assumption of GCCS duties.

### 3.4 Risk

Training risks are categorized as technical, cost and schedule. Due to previous training experience, and the use of existing technology, technical risk is judged to be low. Historically, the cost of training development is indirectly proportional to schedule. If the schedule does not provide adequate time for training then more man years are required which drives costs up. Every effort will be made to develop training that can evolve to meet follow-on training requirements. For example, transition training will be used to develop Block 1 training. This approach will provide timely, valuable information to update existing training programs for Future Users. This effort is currently identified and funded by the FY98 spend plan.

## 4.0 Training Media

Several training media should be explored and used to the maximum extent possible, By leveraging existing technology, significant cost

savings as well as intangible benefits can be realized. One such media is Video Tele-Training television network. Exploitation of VTT will provide a real time training experience to the operational user at each home station. This can reduce or eliminate the need to travel and reduce the amount of lost duty time. Due to time zone differences among the CINCs, careful coordination and scheduling is required. A second media is CD ROM based training. This represents an exportable training media that can be used at remote locations or at sea. Operational Users have requested that CD ROM packages be scenario based to provide more realism to training. Web based training should also be considered as an attractive alternative. Historical success, such as the JTO homepage, may be used as a guide. Additionally, CINCs could tailor scenarios for their operational area and include them on their own homepages. Video Tele-conferencing has received favorable comments from the user community. This requires a Subject Matter Expert (SME) to participate in an interactive chat room at specific times. Users can submit questions and receive immediate feedback from the SME. The video tape recording of the transition training will be provided to training developers. All CINCs are encouraged to video tape on site training. These become a valuable resource for remote sites.

## 5.0 Training Schedule

Due to the dynamic nature of GCCS, Block 1 and Block 2 NET will be event driven. The goal is to present this training within two weeks of the actual site fielding date. This will ensure that the material presented will not be forgotten prior to fielding. The classroom training will be supplemented by a complete set of version 3.0 documentation that can be accessed and used by experienced operators.

The development of version 3.0 training is underway with the transition training scheduled to be completed by early October 1998. Development of Block 1 training can begin immediately following the transition training. Previous planning factors have used a 5 to 1 ratio of development to execution time. This ratio provides five hours development time for every hour of training, five days for every day, etc. Historically, this figure has proven inadequate when new material is being considered. Recommend an 8 to 1 ratio be used for scheduling purposes. A one week training session would require approximately eight weeks of development time. Given the technical nature of the training, this factor does not seem unreasonable.

Version 3.0 Block 2 training development can begin as individual segments are tested/integrated and when funding is made available. All

cost estimates within Annex J (EA) are based on current training requirements in paragraph 1.0 above. Any adjustments to these training requirements, once the process begins, will have significant impact to cost and schedule.

ANNEX H TO ENCLOSURE 2

PRODUCTION OPERATIONS TRANSITION CONOPS
(IMPLEMENTATION PLAN)

**1. Executive Summary.**

a. Major Criteria. The major criteria used to develop this implementation approach are:

1) Minimum impact on operations.

2) Minimize the risk.

3) Leverage testing with implementation.

4) Allow for the GCCS baseline to stabilize.

5) Available qualified DISA personnel to support the plan.

6) Available hardware resources.

b. Two Stage Approach. GCCS implementation will occur in two stages, fielding of the baseline and fielding of the functional applications. Implementation will be on a regional basis. Each region will take approximately 2 months, *however this plan is designed to minimize impact to operations*. Regional users will be pointed to a backup database site during the upgrade then pointed back to the 3.0 database server at the completion of the server upgrade. Implementation will be in two stages, the DII COE baseline change followed by the application loading. The stages include the following:

1) Stage 1, migrate baseline functions in GCCS 2.2 to COE. In this stage the GCCS baseline migrates to DII COE 3.1. The DART application will not work in this environment, therefore a TPEDIT capability will be added in this stage. Emphasis will be on installation of the baseline, compatibility with service programs, and stabilization of the baseline.

2) Stage 2 , implement functional enhancements, include new capabilities, and fix top priority GSPRs.

c. Major Assumptions.

1) ASSUMPTION: This plan resides on the assumption that there is backward compatibility sufficient enough across three levels: data base level, application server level, and client level. Figure 1 illustrates the relationships:

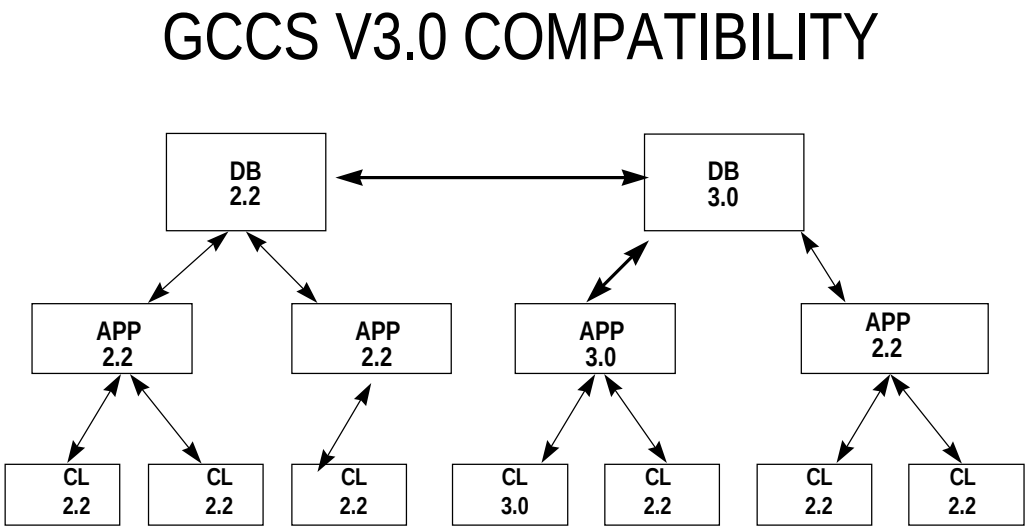



**FIGURE H-1. COMPATIBILITY ASSUMPTIONS**

**IMPORTANT**: Servers/databases must be upgraded to GCCS Version 3.0 before their remote systems are upgraded. In order for sites to transition to GCCS Version 3.0, the user accounts for the sites must be maintained until all of the site's client machines (both local and remote) are installed with the new release. The transition plan includes the installation of a GCCS Version 3.0 account server to maintain user access and file systems. The Executive Manager Server must remain on a GCCS Version 2.2 baseline until all remote clients have been migrated to GCCS Version 3.0.

2) ASSUMPTION**:** The GCCS Version 2.2 database servers must be capable of maintaining accurate transaction flow until the GCCS Version 3.0 database servers become activated. The GCCS Version 3.0 Implementation Procedures will be published later detailing specific site actions and contain transition procedures.

## 2. Implementation Support

a. Site Installation Support.

1) Support for Stage 1 install will be by 7 teams. The installation will be a joint operation of qualified DISA, service and site members. Therefore, the sites must be prepared to support the teams with qualified technical personnel. Services must begin identification of qualified personnel immediately and forward the names to DISA for planning purposes. The necessary skills are; data base administration, systems, security, and network administration. Teams will be physically located at the sites listed in Table H-1 during the installation of GCCS V3.0. Teams will be resident at the site during the install. Their functions are to ensure that site personnel are well trained in the differences between GCCS V2.2 and V3.0 and that the system is fully functional prior to departure.

2) Installation of the GCCS V3.0 is estimated to take approximately 14 days at JOPES Core database sites and approximately 10 days at non-JOPES database sites. As part of the exit criteria, the team members will ensure that the hardware listed below is upgraded to V3.0 in that order and is fully functional:

- Database server
- 1 Account server
- 1 Application server
- 2 - 3 client machines

3) Installation teams and sites will keep DISA and the GCCS Management Center (GMC) informed of implementation status. DISA will keep J3 informed. Any difficulties encountered, and not resolved by on-site installation teams, will be addressed through normal GCCS problem reporting channels.

4) DISA team members traveling to the sites will provide guidance to on-site personnel, *who are expected to load system software*. Problems arising with the installation or use of GCCS V3.0 should be addressed to DISA personnel in theater or the GMC help desk. If not resolved at that level, the problem will be expeditiously referred to the appropriate personnel for resolution.

5) The service agencies will be responsible for the remainder of the client machines and their remote sites. Site and service personnel will be adequately trained at DISA prior to the on-site upgrade. All software segments associated with the GCCS V3.0 upgrade will be loaded by on-site personnel. The JOPES database imports will be accomplished by site personnel. Important: *Sites are required to provide root and oracle database administrator privileges to the database experts at the OSF for the installation period.* If requested, these database experts can remotely log in to the 15 JOPES database sites and monitor the JOPES database import.

6) To accomplish success in the installation of the 15 JOPES database sites the teams will deploy to the sites in groups. Four JOPES core database site installations will be on-going at the same time. Teams will begin installation at four databases in four separate geographical locations. After validation of successful transaction flow, teams will begin installation at four additional JOPES database sites. This process will ensure that the JOPES transactions have successfully been processed by the GCCS Version 3.0 databases prior to the start of an additional group of sites. This installation process will continue until all JOPES data base sites are installed with V3.0. Table H-1 depicts this approach.

7) Regional data base installs will be done in parallel with the operating system. Once a data base server is ready for use the site will be pointed over to the appropriate IP address, minimizing impact on operations. Sites within the region will not see significant performance changes operating between different database versions. The chart below illustrates the process:

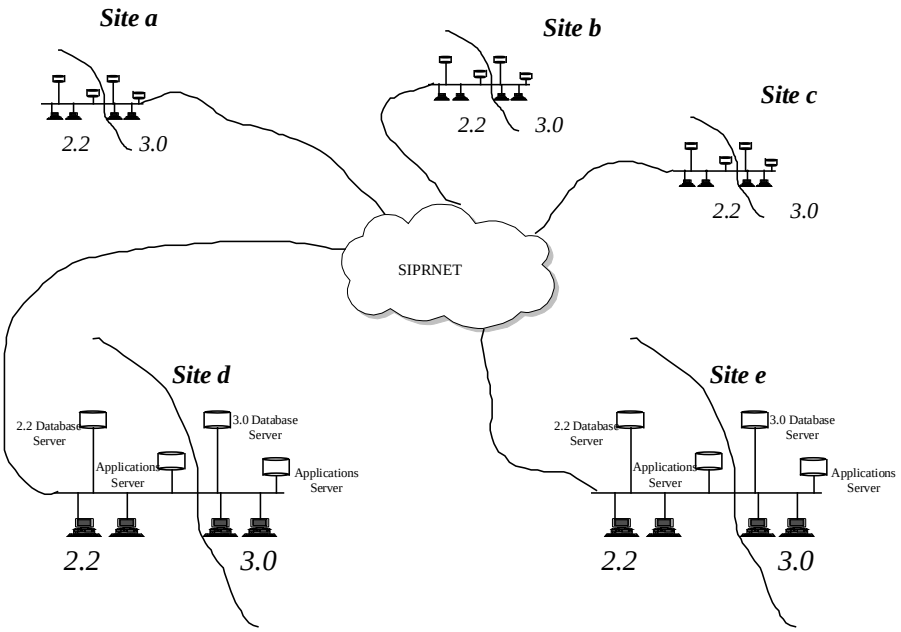



**Figure H-2. Regional Database Installs**

8) Upon completion of a database site's upgrade to V3.0, the sites remote facilities will then commence upgrading to V3.0 utilizing the same set of procedures implemented at the primary database site for the application servers and clients. Assistance in this effort should be provided by the primary site which has already had the installation completed with the assistance of the DISA installation team. The installation sequence is shown in Table H-1.

9) This plan fields GCCS V 3.0 to first the 15 JOPES database sites (the OSF is an additional site) and to the 37 IOC sites. The NMCC will be done first due to special files that are contained in the database. The 15 JOPES database sites have been grouped in to 5 regions as follows:

| | |
|---|---|
| Europe: | EUCOM and USAFE |
| Pacific: | PACAF, ARPAC and Korea |
| Southeast: | CENTCOM, SOCOM and SOUTHCOM |
| Midwest: | TRANSCOM, AMC and FORSCOM |
| 11)Mid-Atlantic: | HQDA, ACC, ACOM and NMCC |

Note that all five regions will be involved in the OT&E as described in the TEMP and the OT&E Plan.

10) General Implementation. The steps shown in Figure H-3 are required to perform the V3.0 implementation.

**Table H-1. Sites**[1]

| |
|---|
| **OSF (RADAR)**<br>**HQDA**<br>**USFK (T)**<br>USFK (Y)<br>USFJ<br>CNO |
| **NMCC**<br>**CENTCOM**<br>**SOUTHCOM**<br>MARFORLANT<br>USASOC<br>NAVSPACE<br>MSC |
| **ACOM**<br>**ACC**<br>LANTFLT<br>MTMC<br>HQMC<br>CENTAF<br>HQAF |
| **ARPAC**<br>**PACAF**<br>PACOM<br>PACFLT<br>MARFORPAC |
| EUCOM<br>**USAFE**<br>AREUR<br>NAVEUR |
| **SOCOM**<br>**FORSCOM**<br>ARCENT<br>NAVCENT<br>USSPACECOM |
| **TRANSCOM** |

[1] **Bold** indicates JOPES Database Site

| |
|---|
| **ANMCC** |
| **AMC** |
| JTO |
| AFMC |
| STRATCOM |
| ARSPACE |
| AFSPACE |
| AETC |
| ALCOM |
| AFCENT |
| VINCENZA |
| TAZAR |
| KTOWN |
| JTASC |
| ARMY WAR COLLEGE |
| NAVY POST GRADUATE SCHOOL |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GCCS V3.0 Transition/Installation | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| Server | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| DB Server | X | X | X | X | X | X | X | X | X | X | X | X | X | X | |
| /h/USER/global | X | X | | | X | | | | | | | | | X | |
| /h/data/global | X | X | | | X | | | | | | | | | X | |
| NIS+ Server | X | X | | | | X | X | | | | | | | X | |
| App server | X | X | | X | | X | | | | | X | X | X | X | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| Activity | Prep | V2.2 Patch Install | JOPES Oracle Backup | Export JOPES Database, Prep App servers | Continue DB Export, Build file servers | Build JOPES Database Server, DII COE to NIS+ and App Servers | Continue Build of JOPES Database server Continue NIS+ server | Import JOPES Oracle Database | Continue Import of JOPES Oracle Database | Continue Import of JOPES Oracle Database | Complete restoring JOPES Database, Load App server Segments | Perform Database Quality Checks, Load App Server Segs | Backup New Oracle Database, Complete App Server Loads | Start User Activity | |
| | | | | | | | | | | | | | | | |
| Day | -1 | -1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |

**Figure H-3. Implementation Steps**

11) For each site there is approximately 170 hours of work to be done. This does not imply that sites will work on a 24hr basis to accomplish this until done, it is more prudent to take breaks at logical steps to review and validate progress. With this in mind there is probably more than 170 hours of work ahead for each data base server. The table below summarizes the steps and effort in hours:

**Table H-2. Database Server Effort**

| *Major Steps* | *Time req (hrs)* |
|---|---|
| *Shutdown TDS and TP* | *1* |
| *Export/save core database and user accounts* | *23* |
| *Rebuild server with O/S, Oracle RDBMS, DII COE, and GCCS segments* | *21* |
| *Restore and import database* | *98* |
| *Restore user accounts and profiles* | *8* |
| *Backup new database* | *8* |
| *Startup TDS and TP, flush TDS/TP queues* | *10* |
| *Allow GCCS clients, apps server to connect to 3.0 database* | *1* |
| *Total* | *170* |

12) Exit Criteria:

a) Ensure:

1. Sites can login to the workstation with user account provided by the Security Administrator.
2. Users can access user data files.

b) For all applications ensure:

1. Required/appropriate icons are present.
2. The application launches without errors.
3. The application screens can be read.
4. The application's menus and buttons operate as expected.
5. The appropriate data base can be accessed.

c) In general ensure:

1. Newsgroup functions work.

2. Users can print to multiple printers.
3. Zircon/chat can be executed and user can start a conference.
4. COP communications reflect actual track data.
   - appropriate maps can be accessed
5. NETSCAPE is present and the network is accessible.
   - Mail and Newsgroups operate properly.
6. Site Administrator can install a 3.0 client/server.
7. Security Administrator can add users.

b. Stage 2, Addition of new functionality and GSPR fixes.

1. Individual applications will be made available upon final testing and Joint Staff approval. Notification of applications ready for download will be done in an expeditious manner. Before installing any new application, all sites will coordinate the activity through the GMC. Distribution of new applications will be done over the network where ever possible.

2. These applications are being built so they may be added to a site's current GCCS configuration in a modular fashion and will not require a complete reload or reconfiguration of the system as for GCCS 3.0 Stage 1. Additionally, not all applications will be needed or required at all sites. Applications will be loaded based on the site's needs and Joint Staff requirements.

a. 3. The procedures by which applications will be loaded will depend upon the unique configuration of that application. Sites will either receive training on how to load these new applications or be provided automated loading scripts. DISA will maintain a team to assist the sites with any problems that arise.

(INTENTIONALLY BLANK)

ANNEX I TO ENCLOSURE 2

INTEGRATED LOGISTICS SUPPORT PLAN

## 1. Overview

This document is to provide ILS and logistical guidance for defining and implementing support concepts, techniques, policies and responsibilities for the Services, Agencies (S/As), and those sites scheduled to receive the Global Command and Control System, Version 3.0. Maintenance support is a significant part of this document and is essential in the sustainment of GCCS. The maintenance concept recommended and employed by DISA for GCCS is contractor support. The initial maintenance coverage of GCCS equipment was funded by DISA with subsequent maintenance support funded by the Services. Each Service is responsible for their individual maintenance approach which may be service organic maintenance and/or contractor support. This document provides a summary of the contract award, contract team, points of contact, instructions for obtaining contract support and the key maintenance options. The GMC Help Desk provides a great assistance to GCCS users and sites in the day to day operation of GCCS. A list of the services/support provided by the Help Desk and phone numbers/electronic addresses is contained in this document. Also included are instructions for submission of new GCCS requirements, Global System Problem Reports (GSPRs)and waivers for temporary local changes to the GCCS Baseline, a key feature in improving both short and long term operation and management of GCCS.

## 2. ILS Concept

This section addresses the various ILS elements and concerns in the fielding and logistical support of GCCS V3.0.

### 2.1 Maintenance

DISA awarded an omnibus maintenance and technical support contract, DCA100-96-D-0060, 30 August 1996, for GCCS equipment. The prime contractor is E-Systems and the contract team is comprised of the following vendors: High Performance Technologies, Inc., Information Systems Consultants, Inc., Oakcreek Funding Corp., Strategic Resources, Inc., Sun Service, and Unisys. The following are a few of the options available under this contract: maintenance support, technical

services, Solaris operating system software support, reconditioning and relocation of equipment.

This contract is a source available to the S/As "for one stop shopping" for obtaining GCCS maintenance and technical contract support. The S/As electing to use this contract are responsible for developing a tailored support plan for their respective sites.

This contract is available on the DISA external home page HTTP://WWW.DISA.MIL/LINE/GCCS.HTML . Sites wishing to use this contract should refer to Section G, Contract Administration Data, Paragraph 5, Other Administrative Matters, in particular subparagraph c, Delivery Order Guidelines, and subparagraph d, Distribution of Delivery Orders. Sites must first complete a delivery order package (DD Form 1155 or your agency's equivalent). Second, the sites must obtain a control number from the DISA Contracting Officer Representative (COR) or the Alternate COR prior to submitting the package. Upon receipt of control number, sites should submit their delivery order package to the E-Systems contract specialist and a copy to the DISA COR. The addresses are as follows:

Raytheon, E-Systems, Inc.
ATTN: Mr. Terry Mason
Garland Division (ISSO)
11320 Random Hills Road, STE 500
Fairfax, VA 2203-6001

DISA
ATTN: Valerie Saucerman
5111 Leesburg Pike, STE 9141
Falls Church, VA 22041-3205

Sites requiring additional information should contact: D20C, Valerie Saucerman, COR, saucermv@ncr.disa.mil,(703)681-0287, (DSN 761) or Judith Sweatmon, ACOR, sweatmoj@ncr.disa.mil, (703)681-0278 .

As stated above, this contract provides maintenance and technical support for GCCS workstations, servers, routers and the GCCS Solaris operating system software. The basic contract includes a 7 day x 24 hour telephone technical assistance at no cost, to supplement the information provided in the manuals and publications. A brief description of the services and options available are provided below:

1. Monthly Coverage: The contractor shall respond to an unlimited number of calls for corrective and preventive maintenance during 0800 to 1700 hours (nine hour), Monday through Friday, except government holidays. This period of coverage is referred to as the

Principal Period of Maintenance (PPM). In addition to the basic monthly coverage, the contract provides for extensions to the PPM of 11, 13, 18 or 24 hours x 5, 6, or 7 days (except government holidays) a week with response times of 2,4, 8 or 24 hours.

2. Per Call: The contract allows for the site to order on call maintenance in lieu of ordering the basic monthly coverage. Per call maintenance may include worldwide global deployment.

3. On-Site: The contract allows for the site to have on-site contractor support. The contractor is assigned to a site and is physically present during the ordered on-site maintenance period (e.g. 5x9, 6x13, 7x24).

4. Special Maintenance Services: The contract offers coverage during times of an exercise, crisis, and/or deployment. Each of these options are a separate CLIN under the contract. Listed below is a summary of the coverage provided under these services. Requester should reference Section C, Statement of Work, for specifics.

   (a) Exercise- The contractor shall provide the necessary on-site maintenance personnel 24 hours per day, 5, 6 or 7 days a week including government holidays. The contractor has 72 hours to report upon being notified by the contracting officer or designated site representative. The contractor shall accomplish all repairs within 4 hours after Government notification, or within 4 hours after a bona-fide attempt is made to notify the contractor.

   (b) Crisis and Deployed- The contractor shall provide the necessary on-site maintenance personnel 24 hours per day, 5, 6, or 7 days a week including government holidays. The contractor has 24 hours to report upon being notified by the contracting officer or designated site representative. The contractor shall accomplish all repairs within 2 hours after Government notification, or within 2 hours after a bona-fide attempt is made to notify the contractor.

In addition, technical support is an option available under this contract. The contractor personnel shall perform assignments in support of Command, Control, Communications, Computers and Intelligence (C4&I) systems in one or more of the following disciplines: communications engineering, electronic engineering, network analysis, communications security, monitoring of systems resources, maintenance of configuration files, data base management support, and resolution of minor

software/hardware problems. The contractor shall also provide advice, assistance, installation, and guidance in the use of C4&I systems, systems design, and operating system interface with telecommunications software. The support shall also include the integration of maintenance corrections and the physical configuration audit and inspection of newly developed software additions, and enhancements and the implementation of other approved software modifications and hardware configurations. In addition, the contractor shall conduct studies and analyze user requirements, identify alternative system approaches, develop recommendations, and prepare reports.

## 2.2 Software Support

The policy for SW license management and funding for maintenance support of the COT SW licenses issued to the initial 37 IOC sites is to transfer this responsibility to the Services on 1 October 1997. The GCCS COTS SW life cycle management will transition from a centralized DISA control, where DISA executes all aspects of COTS SW life cycle management, to a decentralized Service responsibility. The Services under this approach, would assume responsibility of the software life cycle management for supported CINCs and GCCS users, while DISA would continue to provide centralized configuration management and help desk responsibility for GCCS. The following SW vendor licenses issued at IOC are being transferred:

| Application Name | Version | Vendor |
|---|---|---|
| XPORT Topic | | Ascent Technologies |
| Netscape | | BTG, Inc |
| Commerce Server | 1.0 | |
| News Server | | |
| Proxy Server | | |
| Navigator | 2.0 | |
| Browser | 3.0 | |
| Verity Topic | 3.1.5 | Verity, Inc. |
| Oracle RMDS | 7.1.4 | Oracle Corporation |
| Sybase | 10.0.02 | Sysbase, Inc. |
| Objectivity | | Objectivity Inc. |
| AT&T Secret Agent | | Xen Corporation |
| ADA SQL Connect, Inc | | Objective Interface Systems, Inc. |
| MOTIF | 1.2.4 | Integrated Computer Systems, Inc. |
| Gain Momentum | 1.0.01 | Triton Services, Inc. |

DISA will continue to fund the maintenance coverage of the Applix software now upgraded to Version 4.3.5 under GCCS 3.0, through 16 May 1998 and WinDD through, 30 September 1998.

The DISA Configuration Management Office has been working with the Services License Representatives on the transfer of the SW license management. CM has posted on the DISA GCCS Home Page a GCCS COTS Application List which includes: ICASE License File, COTS License Costs, and GCCS Application Vendors List. The CM office also has an itemized breakdown of the vendor licenses for each Service. This information is available from the CM Office, Licensing Support Contract Staff. (703) 735-8746 or 8803.

The following SW applications will be procured and issued by DISA under COE:

Netscape Browser
Common Desk Environment (Tri-Teal)
Distributed Computer Environment (TransArc)

The new DII COE 3.1 applications and functionalities (TIBS, TADIL-B, PLRS/EPLRS, and TRE interface to support TBMD) are GOTS software products and already have in place Service support agreements.

## 2.3 Training

Training is critical to the support of GCCS and must keep pace with the evolution of COE and migration of new functions. Training will continue to have an impact on the sites in terms of time and funding. Services are responsible for the TDY costs of students attending formal training. A considerable part of the training will be DII COE related. While mainly transparent to the user, this new version will require additional new skills on the part of the system administrators. As required, AETC and JTO will support the V3.0 training efforts. In addition, the Joint GCCS Training Community will explore various alternatives (documentation, user guides, scenario based training, videos, etc.) in instructing and training GCCS users. The training plan, Annex G, a joint effort between the trainers, engineers, and users outlines the overall GCCS Training requirements particular to GCCS V3.

## 2.4 GCCS Management Center

DISA WESTHEM, through the Joint Staff Support Center (JSSC), operates and maintains the GCCS Management Center (GMC) and the GCCS sites at the National Military Command Center (NMCC) and the Alternate National Military Command Center (ANMCC). The GMC supports the activities of all the GCCS sites and the functions of the JCS/J6 GCCS Director. The GMC Help Desk (HD) is the user's primary entry point of contact for all problems associated with the joint mission pertaining to hardware, software network, or communications. Any user may report a problem; however the action should be coordinated with the GCCS Coordinator to verify a problem exists.

Most of the CINCs and the S/As have or are setting up their own help desk structure and procedures to review/verify problems before contacting the GMC HD.

The GMC HD has implemented the Remedy Corporation Action Request System (ARS), an automated system used to submit, process and track GCCS trouble tickets. This program is a benefit both to the GMC HD and GCCS users. GCCS sites and end users have the ability to generate trouble tickets from their GCCS workstation by accessing the ARS through the GCCS Netscape web browser at www.gmc.nmcc.smil.mil. Local site administrators can query the trouble ticketing database for status and to obtain background information on same or similar problems submitted by other GCCS sites and end users. GMC technicians use the ARS to generate trouble tickets, query the data base, transmit responses, and close out trouble tickets.

The GMC HD will perform the following major tasks in operating and managing the trouble ticketing system: assign the proper, "priority" field, ensure the trouble tickets are forwarded to the proper organization for corrective action, ensure the "classification" field is properly assigned and monitor/provide the "status" of each trouble ticket. The GMC HD interfaces directly with the GCCS Program Office, contract representatives, engineers, and other functional elements in resolving user problems. The GMC HD is also responsible for receiving, processing, and coordinating the day-to-day routine and non-routine operational issues from GCCS users.

Specific tasks performed by the GMC technicians to support the GMC Help Desk will include, but are not limited to the following:

- Maintaining component inventory management to track problems against hardware or software.
- Maintaining parent-child relationships or dependencies between components or segments.
- Maintaining trouble ticketing system to provide problem history
- Maintaining vendor/maintenance responsiveness history.
- Problem status escalation to higher levels (interfacing with DII/DISN RCCs and S/A and CINC WAN management centers).
- Monitoring machine generated trouble tickets (trouble tickets are automatically generated when system events occur due to network management integration).
- Providing centralized problem management and information services (for troubleshooting network operating software, system operating software, GCCS application software, all GCCS hardware, and GCCS security problems).
- Archiving of problems/trouble tickets for future reference.
- Interfacing to GCCS.GMC.HELP NewsGroup to distribute system. advisory notices to users.
- Interfacing to user's e-mail to create trouble tickets.
- Interfacing to web server to create trouble tickets.
- Interfacing with users to query status of trouble tickets via secure e-mail.
- Interfacing to user's telephonically.

The GMC HD operates 24 hours a day, seven days a week and can be contacted as follows:

Telephone:
Commercial (703) 695-0671
DSN 225-0671

Fax Unclassified:
Commercial (703) 614-9082
DSN 224-9082

Fax Secret:
Commercial (703) 695-0025
DSN 225-0025

E-Mail: (Unclassified) GCCSHELP@NCR.DISA.MIL
(Secret) DJ9HELPL@NMCC20A.NMCC.SMIL.MIL

AUTODIN: DISA WASH DC //WEY31//

## 2.5 Manpower and Personnel

Each Service is responsible for manpower assessment. Manpower and personnel requirements will vary from site to site according to the type of site, the level of support provided by host activities and the configuration, number and physical arrangement of subsystems and equipment. The following describes briefly the various positions and duties which may be required to support a GCCS site.

***GCCS Site Coordinator (GSC)***.

The GSC is responsible for coordinating all system and network support activities within the GCCS site. The individual filling this role will be the primary focal point for coordinating with the GMC and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site. For large organizations, the site commander or DAA may want to appoint additional personnel in this function. They will be referred to as an Assistant GCCS Site Coordinator (AGSC).

***GCCS Network Administrator (GNA)***.

The GNA is responsible for the day-to-day operation of the GCCS LAN, the data and applications servers, the communications devices (premise router, communications server, and intelligent hubs) and related GCCS equipment. A few of the duties are:

- Maintain the Local Area Network (LAN)
- Maintain the AUTODIN/DMS (future) interface
- Identify and be capable of installing each LAN component
- Maintain the LAN system interface
- Operate the LAN
- Troubleshoot network and communications problems
- Provide expertise in TCP/IP services

***GCCS System Administrator (GSA)***.

The GSA is responsible for a variety of duties with the major focus being on maintaining the GCCS applications, providing local user support, and troubleshooting site problems associated with the GCCS applications. This includes the responsibility of determining if the GCCS applications

are properly storing correctly formatted data to the GCCS database servers. A few of the duties are:

- Direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site.
- Maintain access permission lists.
- Add and remove hardware and software at the local site.
- Perform system startups and backups.
- Generate periodic summaries of system performance and utilization.
- Routinely backup data and audit files.
- Setup GCCS User IDS and initial passwords.
- Coordinate database modifications with other site personnel and the GMC-Pentagon.
- Diagnose system problems and report them to the GSC and GMC personnel.
- Monitor total system performance to ensure optimal performance.
- Reconfigure GCCS to regain processing capabilities for non-routine equipment malfunctions.

A thorough understanding of the DII COE and software philosophies will be instrumental in accomplishing the duties of this position.

***GCCS Database Administrator (GDBA)***.

The GDBA is responsible for the day-to-day operations of the databases located at the GCCS site. This may include the primary database server running the Oracle RDBMS or the AMHS server application using the Verity Topic RDBMS. If the GCCS site does not have any of these databases this position may be vacant. A few of the duties are:

- Coordinate incremental/partial backups of the databases with the GSC and the GMC-Pentagon.
- Generate periodic summaries of database performance and utilization.
- Coordinate and maintain database modifications.
- Monitor all database applications for proper performance.
- Manage disk/tape storage.

This position most closely matches the shared responsibilities of the TDBM and the site's system DB personnel.

***Site GCCS Designated Approving Authority (Site GCCS DAA)***.

The Site GCCS DAA is responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations is maintained. This person receives direction and guidance from the Joint Staff GCCS DAA. The Site GCCS DAA is responsible for accrediting GCCS at the site.

***Site GCCS Information System Security Officer (Site GCCS ISSO)***.

The Site GCCS ISSO is responsible for ensuring the integrity and security of the local GCCS system and network. The Site GCCS ISSO is responsible for providing security information to the Site GCCS DAAs. The duties of the Site GCCS ISSO are identified in CJCSI 6731.01. The GMC will be supported by the Site GCCS ISSO appointed at these locations.

## 2.6 Support Documentation

The following documents are to assist the GCCS site personnel in the management and operation of GCCS V3.0:

- System Administration Manual - Provides the GCCS Site Coordinator and System Administrator overall system Technical Management
- Implementation Procedures - How to Plan and Load Installations
- Release Bulletins- Description of Segments
- Software Users Manual
- Software Version Description Document

## 2.7 Configuration Management (CM)

CM is a necessary and fundamental part in the life cycle management of GCCS. CM is a management discipline that applies technical and administrative direction to the development, production, and support life cycle of a configuration item (CI). The discipline is applicable to hardware, software, processed materials, services, and related technical documentation. CJCSI 6722.01, Global Command and Control System (GCCS) Configuration Management Policy, 1 July 1997, should be

referred to regarding CM roles, structure, and responsibility.

CM will actively monitor principal GCCS servers to ensure that baseline configurations are maintained and pertinent functional, performance, and physical interfaces between GCCS system components and software segments are adequately documented. Services are responsible for clients and Service/site unique systems. Services, must however provide data on clients to DISA GMC as required. CM ensures that the DISA maintained specifications, documentation, data, and related baseline information are adequate. CM also ensures that adequate user, system, and other documentation are created, tested, and maintained for DISA controlled CIs. CM will oversee all segment releases to the GCCS baseline and control all automatic upgrades to segments in the baseline (to include CM Executive Agent(EA)supplied segments that contain automatic update capability).

## 2.8 New Requirements, Global System Problem Reports (GSPRs) and Waivers for Temporary Local Changes

The purpose of this section is to briefly describe to GCCS users how the CM process addresses the orderly submission of new GCCS requirements or proposals for migration system candidates, GSPRs, and waivers for temporary local changes in the GCCS Baseline:

### 2.8.1 New Requirements and Proposals for Migration

The Joint Staff J-3 is the office of primary responsibility (OPR) for GCC. The Joint Staff J-33/CSOD is the OPR for the submission of new joint functional requirements and proposals for migration of systems to GCCS. The Joint Staff J-33/CSOD is also responsible for ensuring that a process exists for identifying, validating, integrating, and prioritizing functional requirements. The proposed changes that will require a new evolutionary build or a new baseline will be reviewed and approved/disapproved by the J-3 at the GCC General/Flag Officer Advisory Boards. The GCCS Configuration Control Board (CCB), the C4 Systems Integration Working Group (SIWG), and Functional Area Working Groups will propose to the GCC Review Board a prioritized order of implementation of changes; an implementation plan for an evolutionary build; and an implementation plan of new requirements that are not part of an evolutionary build. All CINCs and S/As through their appropriate OPR and GCCS working groups may input requirements for GCCS. It is recommended that the OPR in each S/A serve as a clearing house for joint GCCS requirements submission. The description of the requirement including candidate applications is then

submitted through the Global Command and Control Requirements Database for processing. Upon approval, the status will be posted on the SIPERNET. CJCSM 6721.01, Global Command and Control System (GCCS) Functional Requirements Evaluation Procedures, 15 March 1997, should be referred to for more specific guidance and instruction regarding this process.

### 2.8.2 Global System Problem Reports (GSPRs)

As mentioned in paragraph 2.4, GCCS Management Center, the GMC HD is the primary entry point for reporting all GCCS hardware, software, network and communication problems. Prior to submittal, all problems are to be reviewed and verified by the respective site CM Executive Agent (EA). Any problems not resolved by the GMC HD result in GSPRs which are entered in a master data base for tracking as part of the formal CM process. The GSPRs are reviewed by the Problem Change Review Board for approval or disapproval. At this point, the approved GPRS are identified as Change Requests or Problem Reports, subsets of GSPRs. The change requests are recommendations that would result in any changes to existing hardware, software segments, documentation to enhanced/improve/expand the operation of GCCS.
The problem reports are notification/identification that a segment, application, interface, etc. is not performing to its functional specification(s). The status of the GSPRs are available in the configuration master data base and accessible via the SIPERNET to authorized CM personnel. CM EAs will submit to the GMC HD pertinent information such as the level of security clearance, address, phone number and site certifier's name. This must be kept current by site Systems Administrator.

### 2.8.3 Temporary Local Changes in the GCCS Baseline

The site System Administrator may request a waiver through his CM EA and GCCS Program Management Officer (PMO) to allow for a temporary local fix or work around into the baseline when, as a result of prioritization of changes, a significant and critical requirement is not met and results in critical capability shortfall for a given CINC, Service, and/or Agency. The originator of the temporary change is to submit the affected modified system components to the DISA GCCS PMO through his GCCS PMO. Once verified by the GCCS CCB and approved by the Joint Staff, the CINC, Service, or Agency PMO may direct incorporation of the modified system components into their baseline. It is the responsibility of that particular requesting site to fund the fix or work

around. DISA will record and place the status of the request for waiver on the SIPRNET within five days of the decision by the GCCS CCB and Joint Staff.

## 2.9 Support Equipment

No unique support equipment has been identified. For all equipment maintained under the DISA GCCS omnibus maintenance contract, the contractor will be responsible for providing any support and test equipment necessary to maintain the equipment at the level specified by the contract.

## 2.10 Technical Data

Technical data are recorded information of a scientific nature and includes the manuals, drawings, parts lists, change notices , system software documentation, and other technical publications related to the operation and support of a system. Documentation of computer programs and related software are technical data; the actual computer programs and related software are not. Technical data also includes specifications, standards, engineering drawings, task analysis instructions, data item descriptions, reports and equipment publications. The attachment contains a listing of GCCS Documentation provided to the sites with Release v2.2. The listing for GCCS 3.0 has not been finalized; however, few changes are anticipated.

## 3.0 Fielding/Transition

DISA will notify S/As and sites via a message once a final fielding schedule has been determined. Prior to fielding, training instruction for system administrators, “how to install 3.0” will be held at the DISA Operational Support Facility, Sterling, VA. The attendees should have experience in GCCS V2.2. The upgrade of GCCS V2.2 to GCCS V3.0 should be transparent to the user and any downtime should be minimal. The objective is to minimize the transition in regards to training, personnel and operation time. The GCCS Transition Plan, currently in staffing, documents a strategy for transitioning GCCS from the GCCS COE to the DII COE.

## 4. ILS Manager/POC

The GCCS ILS Manager is Berk Jeffries, D42, 735-8629 and is matrix to D2. He provides ILS and logistic support to the D2 GCCS Program

Manager and staff.

**Attachment - GCCS Version 2.2 Documentation**

| DOCUMENT # | DOCUMENT TITLE |
|---|---|
| CM-128-08-03 | EVAC User Manual |
| CM-128-10-02 | EVAC (GCCS) EVAC v 2.0 Sun Solaris2.3 Version Description Document |
| CM-128-11-02 | EVAC (GCCS) EVACDB v 2.0 Sun Solaris 2.3 Version Description Document |
| CM-201-73-07 | AHQ Users Manual & AHQ Version 2.2 Release Notes *( S&M (GCCS) AHQ, AHQCHAR v 5.6 Release Notes)* |
| CM-201-73-08 | System Services v 2.2 Release Notes *(SM, SMCHAR v 5.6 Release Notes)* |
| CM-210-19-03 | JDISS System Administration Manual for JDISS Server Segment v 2.0.3 and Client v2.0.4, GCCS 2.1/2.2 with Change 1 |
| CM-21—21-02 | JDISS Image Product Archive (IPA) Client v1.2.1 Installation & System Administration Manual for GCCS v2.1/2.2 with Change 1 |
| CM-210-30-02 | JDISS Installation Manual for Server Segment v 2.0.3 and Client Segment v 2.0.4, GCCS 2.1/2.2 with Change 1 |
| CM-300-02-03 | TBMD 3.0.5.2 (GCCS) Version Description Document for Solaris 2.3 |
| CM-300-03-03 | TBMD 3.0.5.2 (GCCS) Users Guide for Solaris 2.3 |
| CM-316-01-XX | Unified Build Users Guide GCCS 2.2, (Document Series) |
| CM-316-17-XX | Unified Build Version Description Document, GCCS 2.2, (Document Series) |
| CM-316-27-XX | Unified Build Systems Administrators Guide, GCCS 2.2, (Document Series) |
| CM-316-44-03 | Unified Build (GCCS) HP Operating System and UB 3.0.1.6G Application Installation Guide |
| CM 316-47-01 | Unified Build (GCCS) HP Operating Systems 2.3.0.3 for GCCS 2.2 Release Notes |

| | |
|---|---|
| CM 316-48-01 | Unified Build (GCCS) UBPATCH 3.0.1 6GP2 Release Notes |
| CM-500-29-17 | GCCS 2.2 System Administration Manual |
| CM-500-102-08 | GCCS Version Description Document Version 2.2 |
| CM-500-103-XX | GCCS Implementation Procedures Version 2.2 |
| CM-500-168-05 | GCCS Software Users Manual: JOPES Users Guide Update |
| CM-500-298-01 | GCCS v2.2 HP Segment Implementation Procedures |
| CM-500-298-02 | GCCS v2.2 HP Segment Implementation Procedures, ADDENDUM: Scheduling & Movement (SM) Segment |
| CM-500-299-01 | GCCS v2.2 HP Operating System and Unified Build 3.0.1.6G Application IP |
| CM-500-300-01 | GCCS v2.2 HP Operating System Upgrade Implementation Procedures |
| CM-500-302-01 | GCCS/DII COE System Administration Manual Netscape Web Browser v3.0.0.0 (HP-UX 9.07/SOL 2.4 & 2.5.1) |
| CM-500-303-01 | GCCS/DII COE Users Manual Netscape Web Browser v3.0.0.0 (HP-UX 9.07/SOL 2.4 & 2.5.1) |
| CM-500-304-01 | GCCS/DII COE Installation Procedures Netscape Web Browser v3.0.0.0 (HP-UX 9.07/SOL 2.4 & 2.5.1) |
| CM-509-03-04 | RDA Software Users Manual Update |
| CM-514-02-09b | EMPIRE UNIX Systems Management Agent VDD, SRS, OM, STP, STD, KPL, II for Solaris |
| CM-515-02-08 | HP NetMtrix Power Agent VDD, SRS, OM, STP, STD, KPL, IP |
| CM-515-06-01 | HP NetMtrix (GCCS) Segment Abstract |
| CM-516-03-13a | RUDRS v2.0.9 (GCCS) Version Description Document for HP |
| CM-516-03-13b | RUDRS v2.0.9 (GCCS) Version Description Document for Solaris |
| CM-516-05-02 | RUDRS Software Requirements Specification |
| CM-516-06-03 | RUDRS Operator's Manual for CSCI (FRONT END) |
| CM-516-06-04 | RUDRS Operator's Manual for CSCI (BACK END) |
| CM-516-07-02 | RUDRS v2.0.9 Abstract |
| CM-517-04-07 | PREDEFINED Reports (PDR) Users Manual (Update v1.6.2) |
| CM-518-03-08 | GRIS (GCCS Reconnaissance Information System) Version Description Document |
| CM-518-11-02 | GRIS (GCCS Reconnaissance Information System) System Administrators Manual |
| CM-518-13-01 | GRIS (GCCS Reconnaissance Information System) |

| | Segment Abstract |
|---|---|
| CM-521-04-05 | Airfields (GCCS) V.2.1.1 Software Version Description |
| CM-521-04-06 | Airfields (GCCS) V.2.1.2 Software Version Description |
| CM-522-02-04 | FRAS (Fuel Resource Analysis System) Installation Instructions |
| CM-522-02-06 | FRAS (Fuel Resource Analysis System) Software User's Manual |
| CM-532-02-02 | ELVIS (GCCS) 1.3.2.0 Version Description Document for Solaris 2.3 format |
| CM-532-03-02 | ELVIS (GCCS) 1.3.2.0 Installation Procedures |
| CM-532-04-02 | ELVIS (GCCS) 1.3.2.0 System Administrators Guide |
| CM-532-05-02 | ELVIS (GCCS) 1.3.2.0 Users Manual |
| CM-532-11-01 | ELVIS (GCCS) 1.3.2.0 Comprehensive Test Plan |
| CM-532-10-01 | ELVIS (GCCS) 1.3.2.0 SW Test Report for GCCS 2.2 Sparc 5, 10, 20 Solaris 2.3 |
| CM-532-09-01 | ELVIS (GCCS) 1.3.2.0 SW Requirements Specification for GCCS 2.2 Sparc 5,10,20 Solaris 2.3 |
| CM-539-06-01 | TIBS Secret Data Segment Software Version Description |
| CM-539-07-01 | TIBS v 2.1.4 Segment Users Guide for GCCS 2.2 |
| CM-541-02-01 | GCCS COLISEUM Client Version 2.2.0.0 AIS Security Certification Test Report (Test Date 1/24/95) |
| CM-541-03-01 | GCCS COLISEUM DIA Department of Defense Intelligence Management System Security Plan |
| CM-541-04-01 | GCCS COLISEUM DIA Department of Defense Intelligence Management System Security Requirements |
| CM-541-05-01 | GCCS COLISEUM DIA Department of Defense Intelligence Management System Security Concept of Operations |
| CM-541-06-01 | GCCS COLISEUM DIA Department of Defense Intelligence Management System Security Analysis |
| CM-541-07-01 | GCCS COLISEUM DIA Department of Defense Intelligence Management System Accreditation Test Plan |
| CM-541-08-01 | GCCS COLISEUM DIA Department of Defense Intelligence Management System Accreditation Test Procedures |
| CM-541-09-02 | GCCS COLISEUM DIA v2.2 Users Manual Draft |
| CM-541-10-01 | GCCS COLISEUM Requirements Definition Document |
| CM-541-11-01 | GCCS COLISEUM Concept of Operations (CONOPS) for Secret Collateral Version |

| | |
|---|---|
| CM-544-03-01 | JTAV (Joint Total Asset Visibility) GCCS Interface Users Guide |
| CM-544-04-01 | JTAV (Joint Total Asset Visibility) GCCS Interface Client 1.0.0.1 Version Description |
| CM-546-46-01 | NIPS (GCCS) Software Requirements Specification (SR) v3.0.1 |
| CM-547-02-01 | GCCS Tactical C4I Applications Imagery Segments v2.2.8 Installation Procedures |
| CM-548-03-01 | GCCS COP TIME SYNC 1.0.0.0 Version Description Document |
| CM-548-04-01 | GCCS COP TIME SYNC 1.0.0.0 Software Users Manual |
| CM-549-03-01 | GCCS COP v1.0.1.0 Application Software Version Description Document |
| CM-549-04-01 | GCCS COP v1.0.1.0 Application Software Users Guide |
| CM-550-02-01 | GCCS GPS TIME v1.0.1.0 Application Software Version Description |
| CM-549-03-01 | GCCS GPS TIME v1.0.1.0 Application Software Users Guide |

(INTENTIONALLY BLANK)

ANNEX J TO ENCLOSURE 2

ECONOMIC ANALYSIS

# Annex J:
# Table of Contents

1. INTRODUCTION ..... 1
1.1 Scope ..... 3
2. COSTS AND BENEFITS ..... 4
3. COST SUMMARY ..... 12
4. ASSUMPTIONS ..... **Error! Bookmark not defined.**
4.1 Joint Assumptions ..... **Error! Bookmark not defined.**
4.1.1 Scope - Joint ..... **Error! Bookmark not defined.**
4.1.2 Limitations - Joint ..... **Error! Bookmark not defined.**
4.1.3 Hardware Assumptions - Joint ..... **Error! Bookmark not defined.**
4.1.4 Software Assumptions - Joint ..... **Error! Bookmark not defined.**
4.1.5 Training Assumptions - Joint ..... **Error! Bookmark not defined.**
4.2 Assumptions for DISA-Sponsored Sites ..... **Error! Bookmark not defined.**
4.2.1 Scope - DISA ..... **Error! Bookmark not defined.**
4.2.2 Hardware Upgrades and Maintenance - DISA ..... **Error! Bookmark not defined.**
4.2.3 Software Assumptions - DISA ..... **Error! Bookmark not defined.**
4.2.4 Communications - DISA ..... **Error! Bookmark not defined.**
4.2.5 System, Network, and Security Administration - DISA **Error! Bookmark not defined.**
4.2.6 Training - DISA ..... **Error! Bookmark not defined.**
4.3 Assumptions for Navy-Sponsored Sites ..... **Error! Bookmark not defined.**
4.3.1 Scope - Navy ..... **Error! Bookmark not defined.**
4.3.2 Hardware Upgrades and Maintenance - Navy ..... **Error! Bookmark not defined.**
4.3.3 Software Assumptions - Navy ..... **Error! Bookmark not defined.**
4.3.4 Communications - Navy ..... **Error! Bookmark not defined.**
4.3.5 System, Network, and Security Administration - Navy . **Error! Bookmark not defined.**
4.3.6 Training - Navy ..... **Error! Bookmark not defined.**
4.4 Assumptions for USMC-Sponsored Sites ..... **Error! Bookmark not defined.**
4.4.1 Scope - USMC ..... **Error! Bookmark not defined.**
4.4.2 Hardware Assumptions - USMC ..... **Error! Bookmark not defined.**
4.4.3 Software Assumptions - USMC ..... **Error! Bookmark not defined.**
4.4.4 Training Assumptions - USMC ..... **Error! Bookmark not defined.**
4.5 Assumptions for Army-Sponsored Sites ..... **Error! Bookmark not defined.**
4.5.1 Scope - Army ..... **Error! Bookmark not defined.**
4.5.2 Hardware Upgrades and Maintenance - Army ..... **Error! Bookmark not defined.**
4.5.3 Software Upgrades and Maintenance - Army ..... **Error! Bookmark not defined.**
4.5.4 Communications - Army ..... **Error! Bookmark not defined.**
4.5.5 Network and System Administration - Army ..... **Error! Bookmark not defined.**
4.5.6 Training - Army ..... **Error! Bookmark not defined.**
4.5.7 Funding Perspective - Army ..... **Error! Bookmark not defined.**

4.6 Assumptions for Air Force-Sponsored Sites.....**Error! Bookmark not defined.**
4.6.1 Scope - Air Force.....**Error! Bookmark not defined.**
4.6.2 Limitations - Air Force.....**Error! Bookmark not defined.**
4.6.3 Hardware Assumptions - Air Force.....**Error! Bookmark not defined.**
4.6.4 Software Assumptions - Air Force.....**Error! Bookmark not defined.**
4.6.5 Training Assumptions - Air Force.....**Error! Bookmark not defined.**

# ECONOMIC ANALYSIS

## 1. Introduction

This Annex describes the incremental cost of moving to GCCS version 3.0 Stages 1 and 2 and is organized as follows:

- Section 2 COSTS AND BENEFITS: This section identifies the costs and benefits of the incremental changes associated with GCCS versions 3.0.
- Section 3 COST SUMMARY: This section summarizes the total cost of GCCS versions 3.0 by resource sponsor.
- Section 4 ASSUMPTIONS: This section documents all assumptions used in deriving the costs contained in this EA.

### 1.1 Scope

Only the incremental costs associated with changes in GCCS functionality are addressed in this cost analysis. The costs associated with the existing GCCS baseline (e.g., operation and maintenance of existing hardware and software) are not included herein even if updates to components of the baseline are covered under this EPIP. The rationale for this is that the cost analysis of the existing baseline accounts for “refreshes” to existing hardware and software. Figure J-1 depicts the scope of the analysis.

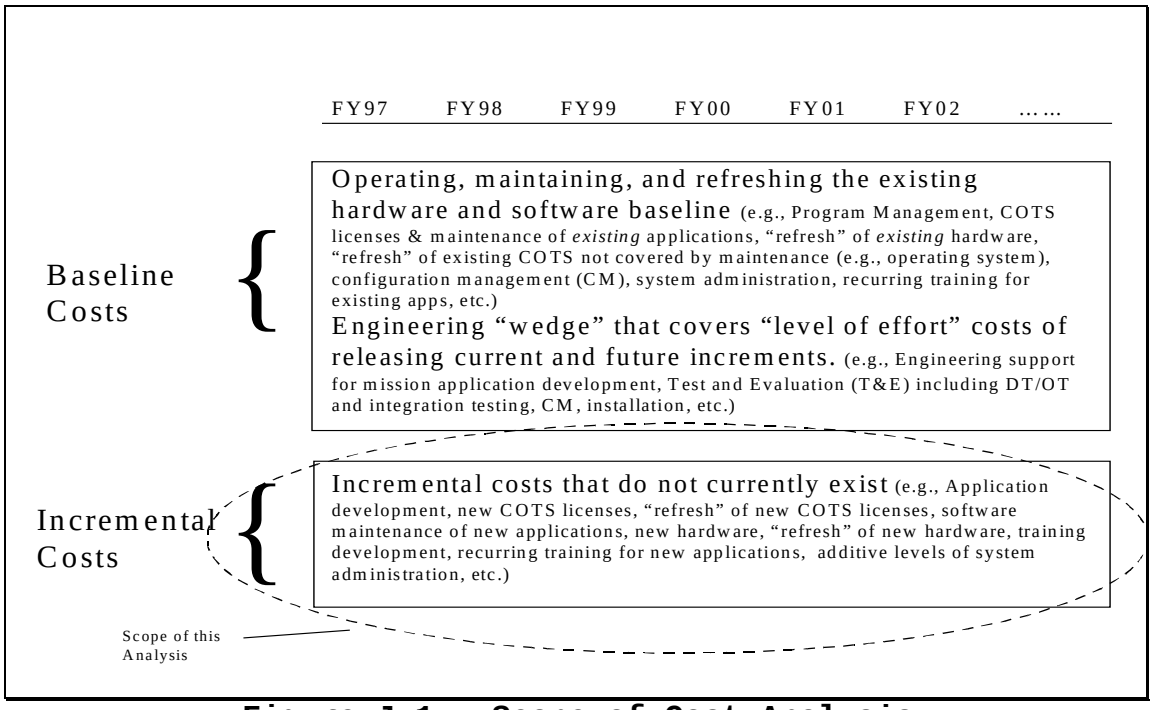



**Figure J-1: Scope of Cost Analysis**

Given this costing strategy, the cost of enhancements to existing mission applications (e.g., GCCS System Problem Report fixes for JOPES applications) are not included because they are considered maintenance of the existing baseline. This same rationale applies to updates of existing operating systems (e.g., Solaris 2.5.1) and database management systems (e.g., Oracle 7.3.2).

Note from Figure J-1 that the cost analysis of the existing baseline also includes a funding "wedge" that covers the recurring costs of releasing current and future incremental changes.

Although, under this costing strategy, development costs for new GCCS mission applications should be addressed in this EPIP, due to the timing of this document, most of these costs are now sunk and are no longer germane to the decision-making process. Thus, with the exception of JPET and JFRG (which have not yet been segmented for GCCS), development costs are not included herein.

## 2. Costs and Benefits

This section summarizes the costs and benefits associated with GCCS versions 3.0. The costs of the following

incremental changes to the existing GCCS version 2.2 baseline are provided:

- Move from GCCS COE version 2.2 to DII COE version 3.1.
- Integrated Intelligence Capabilities
- Joint Planning and Execution Toolkit (JPET)
- Joint Total Asset Visibility (JTAV)
- Joint Personnel Asset Visibility (JPAV)
- Meteorology and Oceanography (METOC)
- Web-Based Access to Mission Applications
- Theater Battle Management Core System (TBMCS)
- Joint Force Requirements Generator (JFRG)
- Miscellaneous Costs Not Attributable to Specific Increments

Tables J-1 through J-10 summarize the benefits of each increment and present the costs by Service.

| | |
|---|---|
| **Incremental Change** | Move to DII COE version 3.1 |
| **Description of Benefits** | • The Services have indicated their intent to migrate their Service-unique C2 applications to DII COE version 3.1; thus, moving GCCS to this same operating environment improves inter- and intra-Service interoperability and offers the first real possibility of consolidating Joint and Service-unique applications on a single hardware platform.<br>• Additional capabilities provided by DII COE version 3.1:<br>  • Parallel processing capabilities of Solaris 2.5 and Oracle 7.3 will dramatically improve the performance and reliability of existing JOPES applications.<br>  • Elimination of the previous GOTS desktop (i.e., Executive Manager) and replaces it with an industry standard thus improving opportunities for interoperability.<br>  • Improved system security and security administration. Aids in data protection, virus prevention, and protection from hackers and malicious code.<br>  • Improved system and database administration<br>  • System performance data collection via Empire 2.0.0 network monitoring agent.<br>  • Additional receive-only tactical communications interfaces including TRE/TRAP, TIBS, TADIL B, PLRS/EPLRS.<br>  • Enhanced track correlation. Enhanced automated capability to distinguish and correlate COP tracks thus reducing potential ambiguity.<br>  • Ability to access PC-based office automation applications (running in their native environment on WinDD servers) from Sun clients.<br>  • COTS web browser (Netscape for Unix, HP, and NT platforms. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | • Provides a Windows NT-based COE client which improves opportunities for future development of PC-based C2 applications. GCCS 3.0 will include the "C2 PC" application which provides PC users running Windows NT with a dynamic COP display superior to that currently provided by the Enhanced Linked Visual Information (ELVIS) application. Thus, it provides low-bandwidth users with a viable capability for viewing the COP. | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA | 183 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| Navy[3] | 392 | 361 | 328 | 119 | 121 | 110 | 110 | 110 | 110 | 110 |
| USMC[4] | 353 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 | 23 |
| Army[5] | 2750 | 1500 | 1500 | 1500 | 1700 | 1700 | 1700 | 1700 | 1700 | 1700 |
| Air Force[6] | 1500 | 2574 | 529 | 718 | 907 | 1097 | 1286 | 1286 | 1286 | 1286 |
| **TOTAL:** | 5178 | 4481 | 2403 | 2383 | 2774 | 2953 | 3142 | 3142 | 3142 | 3142 |

**Table J-1: Cost and Benefit Summary for Moving to DII COE version 3.1**

| | |
|---|---|
| **Incremental Change** | Integrated Intelligence Capabilities |
| **Description of Benefits** | Intelligence Database and Imagery Access<br>• Offers a quantum leap in providing a fused, near real-time picture of the battlespace. Serves as a host for receiving finished intelligence products into a GCCS tactical display and the injection of threat data into the COP.<br>• Provides access to the Defense Intelligence Agency's Modernized Integrated Database (MIDB) and the National Imagery and Mapping Agency's Imagery Product Library (IPL) from within a GCCS Common Operational Picture.<br>• Puts MIDB objects, underlying data, and intelligence imagery at the |

[3] FY-97 does not include initial training for system/database administrators.
[4] FY-97 does not include initial training for system/database administrators.
[5] FY-97 does not include initial training for system/database administrators.
[6] FY-97 includes initial training for system/database administrators.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | secret/collateral level alongside near real time land, sea and air tracks injected from tactical data feeds or national broadcasts.<br>• Pointing/clicking on an icon opens a window with intelligence analysts' comments and information.<br>Intelligence Collaboration<br>• Provides collaboration tools with the capability to provide connectivity and with component, theater, and national intelligence analysts.<br>Request for Intelligence Information<br>• Supports the registration of crisis and non-crisis intelligence requirements with the national intelligence community as well as the validation, tracking and management of requests for intelligence information.<br>Theater Ballistic Missile Defense (TBMD) Early Warning<br>• Provides indications and warnings of incoming ballistic missiles in near real-time. Specifically, this application provides:<br>  • TBM launch/impact points<br>  • Track viewing capability with time-to-impact information<br>  • TBM tactical information for defensive or mission-critical uses.<br>Summary of Synergistic Effects<br>• Provides commanders with reliable near-real-time red force info. during all phases of the force projection cycle including battle damage assessment.<br>• Provides planner access to any finished intelligence products including: (1) logisticians who require information on transportation infrastructure to move or plan to move supplies and materials, (2) medical personnel requiring knowledge of diseases endemic to a region, and (3) local commanders who require information on personalities with whom they will routinely interact. | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA | 555 | 22 | 22 | 490 | 22 | 22 | 490 | 22 | 22 | 490 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Navy[7] | 117 | 793 | 634 | 542 | 784 | 634 | 542 | 784 | 634 | 634 |
| USMC | 222 | 11 | 11 | 222 | 11 | 11 | 222 | 11 | 11 | 222 |
| Army | 750 | 400 | 400 | 400 | 400 | 250 | 250 | 250 | 250 | 250 |
| Air Force | 0 | 919 | 126 | 126 | 126 | 126 | 126 | 126 | 126 | 126 |
| JDISS PMO[8] | 0 | 430 | 430 | 430 | 430 | 430 | 430 | 430 | 430 | 430 |
| NIMA[9] | 0 | 535 | 535 | 535 | 535 | 535 | 535 | 535 | 535 | 535 |
| DIA[10] | 0 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 |
| **TOTAL:** | 1644 | 5103 | 4151 | 4738 | 4301 | 4001 | 4588 | 4151 | 4001 | 4680 |

**Table J-2: Cost and Benefit Summary for Integrated Intelligence Capabilities**

| | |
|---|---|
| **Incremental Change** | Joint Planning and Execution Toolkit (JPET) |
| **Description of Benefits** | Provides for a combination of Advanced Concept Technology Demonstration (ACTD) applications that dramatically improve crisis management planning capabilities.<br>• Enhanced TARGET - Newer version provides user identified enhancements plus software capability to conduct voice with limited video conferencing between two or more workstations. Site hardware, and possibly, communications upgrades are likely required to take advantage of voice/video conferencing. Improvement to current version of TARGET include:<br>  • Multiuser safe<br>  • Can “point” to other TARGET databases<br>  • Expanded (Operations Planning Tool) OPT entries for CINC<br>  • Added Joint Staff functions to OPT<br>  • Course of Action Selection Tool allows for assignment of UICs to units in COAs.<br>  • Can time phase units in a COA.<br>  • Collaborative map, multicast video teleconference, whiteboard<br>  • Uses upgraded map similar to JTF-ATD map.<br>  • Can collaborate with JTF-ATD map. |

[7] FYs 98-06 include software maintenance of TBMD segment ($500K /year).
[8] Software maintenance of Intelligence Collaboration segment ($430K/year).
[9] Software maintenance of IPL access segments ($535K/year).
[10] Software maintenance of MIDB segments ($1625K/year) and Coliseum client ($368K/year).

| | |
|---|---|
| | • Planners workbench<br>• Can share data with JTF-ATD Plan Server<br>• Direction connection to GSORTS unit data using SQL.<br>• Modules interface with FMEDIT.<br>• FMEDIT (Force Module Edit)<br>• Provides capability not previously available on GCCS.<br>• Provides the user with ability to manipulate TPFDD force modules. Greater flexibility in building new and modifying existing TPFDDs.<br>• Generates force "capability sets" for initial deployment analysis<br>• Passes gross force deployment requirements to TPEDIT for detailed refinement/sources<br>• Force Module management capability.<br>• TPEDIT (TPFDD Edit)<br>• Provides TPFDD development and analysis capability. Version 6/96 replaces DART version currently on GCCS.<br>• New version includes user identified enhancements such as refined, tailored, sourced force deployment requirements |

| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
|---|---|---|---|---|---|---|---|---|---|---|
| DISA[11] | 586 | 473 | 473 | 473 | 473 | 473 | 473 | 473 | 473 | 473 |
| Navy[12] | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| USMC | 104 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| Army | 0 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| Air Force | 0 | 13 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| **TOTAL:** | 690 | 546 | 534 | 534 | 534 | 534 | 534 | 534 | 534 | 534 |

**Table J-3: Cost and Benefit Summary for Joint Planning and Execution Toolkit (JPET)**

[11] FY-97 includes $395K for segmentation/Level 5 compliance and $191K for COTS licenses. FYs 98-06 contain $21K for COTS maintenance and $452K for software maintenance.
[12] Navy did not estimate costs for JPET.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Incremental Change** | Joint Total Asset Visibility (JTAV) | | | | | | | | | |
| **Description of Benefits** | The client portion of this GCSS application will be included in GCCS 3.0.<br>Provides logistics planners and others ready access to joint force logistics information from a variety of logistics sources. Specifically, JTAV provides visibility into the status of:<br>• general supply assets data<br>• petroleum, oils, and lubricants (POL)<br>• supplies<br>• transportation<br>• requisition status<br>• war reserves<br>• unit equipment<br>• bulk fuel<br>• munitions | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Navy | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| USMC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Army | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Air Force | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **TOTAL:** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table J-4: Cost and Benefit Summary for Access to Joint Total Asset Visibility (JTAV)** [13]

| | |
|---|---|
| **Incremental Change** | Joint Personnel Asset Visibility (JPAV) |
| **Description of Benefits** | The client portion of this GCSS application will be included in GCCS 3.0.<br>• Integrates and analyzes Joint and service-specific processes and data requirements relating to force conversion, mobilization, deployment, and sustainment operations in support of Joint Task Forces (JTF).<br>• Functionality includes tracking of military |

[13] Training development, server costs, or software maintenance costs are attributable to GCSS. Further, Services will not incur costs for unique COTS software licenses to be incurred by the GCCS user community.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | personnel movements into, within, and out of the area of operations. | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Navy | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| USMC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Army | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Air Force | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **TOTAL:** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table J-5: Cost and Benefit Summary for Access to Joint Personnel Asset Visibility (JPAV)** [14]

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Incremental Change** | Meteorology and Oceanography (METOC) | | | | | | | | | |
| **Description of Benefits** | Provides the capability to overlay finished meteorology and oceanography products on the COP, including:<br>• Weather imagery (i.e., cloud cover)<br>• Severe METOC conditions (icing, turbulence, high winds, etc.)<br>• Current and forecast positions of hurricanes/typhoons<br>Integrates additional tactical decision aids into the COP to support improved planning and decision making involving the deployment and employment of Joint forces. | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Navy[15] | 0 | 758 | 758 | 758 | 758 | 758 | 758 | 758 | 758 | 758 |
| USMC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Army | 0 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| Air Force | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **TOTAL:** | 0 | 808 | 808 | 808 | 808 | 808 | 808 | 808 | 808 | 808 |

**Table J-6: Cost and Benefit Summary for METOC**

| | |
|---|---|
| **Incremental Change** | Web-Based Access to Mission Applications |
| **Description** | This increment provides for World-Wide Web- |

[14] Training development, server costs, or software maintenance costs are attributable to GCSS. Further, Services will not incur costs for unique COTS software licenses to be incurred by the GCCS user community.

[15] Includes corrective and perfective maintenance for JMS software of approximately $758K/year.

| | |
|---|---|
| **of Benefits** | based access to the following mission applications:<br>• Ad Hoc Query (a.k.a. DARWIN): A new web-browser (e.g., Netscape) front end to this application will greatly enhance the simplicity and familiarity of Scheduling and Movement (S&M) database queries - especially for low-bandwidth AHQ users.<br>• AIRFIELDS: Provides access to a comprehensive source of information on over 40,000 free world airfields from any GCCS compliant workstation using a web browser tool. This is one of the first web browser-based applications in GCCS that provides a more familiar user interface, better support for low-bandwidth GCCS users, and support for any workstation capable of hosting a web browser. |

| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
|---|---|---|---|---|---|---|---|---|---|---|
| DISA | 7 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| Navy | 180 | 5 | 5 | 168 | 5 | 5 | 168 | 5 | 5 | 168 |
| USMC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Army | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Air Force | 0 | 120 | 31 | 34 | 36 | 39 | 42 | 42 | 42 | 42 |
| **TOTAL:** | 187 | 128 | 39 | 205 | 44 | 47 | 213 | 50 | 50 | 213 |

**Table J-7: Cost and Benefit Summary for Web-Based Mission Applications**

| | |
|---|---|
| **Incremental Change** | TBMCS |
| **Description of Benefits** | The Joint TBMCS Segments planned for GCCS include the following:<br><br>Rapid Application of Air Power (RAAP): Provides targeting capabilities for air battle planners (compares target nomination list to weapons options and facilitates target development). Used in a stand-alone mode today by individuals within JTFs/JFACCs.<br>• Segmentation provides a GCCS-capable version so the stand-alone version used today is no longer needed.<br><br>Joint Planning Tool (JPT): Provides an independent capability for senior combat leaders to conduct initial planning essential to running the air campaign by automating the capability to plan an air campaign working from strategy to task. JPT selects subsets of targets which must be hit based on a specific strategy. Fielded in a prototype mode today on a unique set of hardware.<br>• Segmentation will eliminate requirement for unique hardware and provide the capability on the GCCS suite.<br><br>Air Tasking Order Read, Distribute and Print (ARDP): Provides capability to Read, distribute and print. Can access the ATO from GCCS.<br><br>Computer Assisted Force Management Structure (CAFMS X): Provides ATO dissemination, execution and monitoring capability. Allows manipulation of the ATO (i.e., parse by unit, equipment type, etc.)<br><br>TASKVIEW: Standard ATO is AUTODIN message text format. TASKVIEW translates this into a more ‘user friendly” ATO format that can be read like a word document.<br><br>Initial fielding plans are for the battle labs only and will not go out for worldwide distribution on the GCCS V3.0 tapes. If |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | commands want to load any of these capabilities on their system, they will have to contact the Theater Battle Management Core Systems Program Management Office for distribution. | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Navy | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| USMC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Army | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Air Force[16] | 0 | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 |
| **TOTAL:** | 0 | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 | 200 |

**Table J-8: Cost and Benefit Summary for Theater Battle Management Core Systems (TBMCS)** (See Note)

Note: The COTS licenses and maintenance costs associated with these segments were not estimated by the Navy, USMC, or Army. Air Force position is that there are no additive costs for licenses because the Air Force already uses the applications and doesn't anticipate additional licenses will be required.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Incremental Change** | Joint Force Requirements Generator (JFRG) | | | | | | | | | |
| **Description of Benefits** | Provides a Windows-based, Joint TPFDD feeder system consistent with the recommendations of the JOPES User Review Panel (URP).<br>• Provides for "remote" computation of unit and non-unit sustainment requirements for all Services.<br>• Incorporates TUCHA data and transaction processing algorithms (adds, modifies, deletes) consistent with Service logistics doctrines.<br>• Provides a remote interface to the JOPES database. | | | | | | | | | |
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA[17] | 335 | 300 | 300 | 300 | 300 | 300 | 300 | 300 | 300 | 300 |
| Navy | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| USMC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

[16] FY 98-06 costs are for software maintenance.

[17] FY97 includes $335K for JFRG development. Outyear costs are for software maintenance.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Army | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Air Force | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **TOTAL:** | 335 | 300 | 300 | 300 | 300 | 300 | 300 | 300 | 300 | 300 |

**Table J-9: JFRG Costs**

| **Incremental Change** | Miscellaneous Costs Not Attributable to Any Specific Increment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Cost Summary ($K)** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
| DISA<br>- Transition Training<br>- Block 1 / Block 2 Training Development<br>- Block 1/ Block 2 Initial Training | 40<br>764<br><br>371 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Navy[18] | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| USMC[19] | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Army<br>- Initial User Training | 350 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Air Force[20] | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **TOTAL:** | 1525 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table J-10: Miscellaneous Costs**

### 3. Cost Summary

Table J-11 summarizes the incremental costs associated with this EPIP.

| **Organization** | **FY97** | **FY98** | **FY99** | **FY00** | **FY01** | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** |
|---|---|---|---|---|---|---|---|---|---|---|
| DISA | 2841 | 821 | 821 | 1289 | 821 | 821 | 1289 | 821 | 821 | 1289 |

[18] Initial user training costs not available.
[19] Initial user training costs not available.
[20] Initial user training costs not available.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Navy | 689 | 1917 | 1725 | 1587 | 1668 | 1507 | 1578 | 1657 | 1507 | 1670 |
| USMC | 679 | 44 | 44 | 255 | 44 | 44 | 255 | 44 | 44 | 255 |
| Army | 3850 | 2000 | 2000 | 2000 | 2200 | 2050 | 2050 | 2050 | 2050 | 2050 |
| Air Force | 1500 | 3826 | 887 | 1079 | 1270 | 1463 | 1655 | 1655 | 1655 | 1655 |
| JDISS PMO | 0 | 430 | 430 | 430 | 430 | 430 | 430 | 430 | 430 | 430 |
| NIMA | 0 | 535 | 535 | 535 | 535 | 535 | 535 | 535 | 535 | 535 |
| DIA | 0 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 | 1993 |
| **TOTAL:** | 9559 | 11566 | 8435 | 9168 | 8961 | 8843 | 9785 | 9185 | 9035 | 9877 |

**Table J-11: Cost Summary**

4. ASSUMPTIONS

The costs in this economic analysis were built from individual estimates made by DISA and the four Services. The assumptions provided by DISA and the Services for this analysis are described in the following sub-sections:

- Section 4.1: Joint assumptions used by DISA and all Services
- Section 4.2: Assumptions for DISA-sponsored sites
- Section 4.3: Assumptions for Navy-sponsored sites
- Section 4.4: Assumptions for USMC-sponsored sites
- Section 4.5: Assumptions for Army-sponsored sites
- Section 4.6: Assumptions for Air Force-sponsored sites

### 4.1 Joint Assumptions

#### 4.1.1 Scope - Joint

- The costs included in this economic analysis are only the incremental costs to field, operate, and maintain the new capabilities described in this EPIP. Sunk costs (e.g., certain non-recurring software development costs) are not included.
- Operations and maintenance costs of existing GCCS applications (including JOPES enhancements) are not included.
- A 10 year life cycle projection is required beginning in FY97.
- All costs are in FY97 constant dollars.

### 4.1.2 Limitations - Joint

- The costs in this EPIP are based upon bottom-up estimates of the number of servers, workstations, and applications running at various sites throughout DOD. The number of workstations and applications running at any given site were best estimates and cannot be assumed to be exact representations of reality.
- The cost of network communications devices (routers, LANs, WANs, cables, and associated equipment) are not included.
- SIPRNET charges are not included.
- Resources used to support the GCCS Management structure established by CJCSI 6721.01, *GCCS Management Structure*, are not included.
- Program Management Office (PMO) costs are not included.

### 4.1.3 Hardware Assumptions - Joint

The following hardware refresh cycles are assumed for any incremental hardware associated with this EPIP:

- Workstations and associated cables and non-printing peripherals are replaced on a three year cycle. One third of the inventory of these devices is replaced each year after initial procurement of all devices in year 1 (FY 1997).
- Servers, printers, and non-network communications devices are replaced on a three year cycle. The full inventory is replaced every three years after initial procurement in year 1 (FYs 2000, 2003, and 2006).

#### 4.1.3.1 GCCS COE Version 2.2 to DII COE Version 3.1 - Joint Hardware

- The need for an Executive Manager (EM) server is eliminated with the introduction of the Common Desktop Environment (CDE) in GCCS 3.0, thus freeing up that asset for other use.
- No new servers are required to implement DCE.
- All sites desiring to implement WinDD are assumed to possess sufficient numbers of PCs to satisfy the server requirement for WinDD without additional cost.

#### 4.1.3.2 Integrated Intelligence Capabilities - Joint Hardware

- DIA and NIMA will install MIDB and IPL servers respectively at the required number of sites necessary to make the GCCS MIG segments operationally effective. At the present time, these sites are still TBD.

- No new hardware is required to handle incoming data feeds for the GCCS TBMD segment. Sites that currently serve as "master" track management sites have hardware already in place to handle the real-time data feeds and will feed track data via SIPRNET to all other GCCS TBMD "slave" sites as required.
- A dedicated Imagery Transformation Service (ITS) (i.e., a specially configured Sparc20) is required at each site installing the GCCS Intelligence Imagery segment and desiring to perform local manipulation of imagery products.

**4.1.3.3 Joint Planning and Execution Toolkit (JPET) - Joint Hardware**

- Existing Sun and HP workstations require 8 bit video cards to support JPET, but 24 bit video cards will be purchased to support the introduction of JTF Planner which is scheduled for the next release of GCCS 3.X. The hardware "bundle" available through the JDISS PMO to support MCM is suitable for supporting the multimedia requirements of JPET and JTF Planner.

**4.1.3.4 Joint Total Asset Visibility (JTAV) - Joint Hardware**

- JTAV servers will be provided by the Global Combat Support System (GCSS).

**4.1.3.5 Joint Personnel Asset Visibility (JPAV) - Joint Hardware**

- JPAV servers will be provided by the Global Combat Support System (GCSS).

**4.1.3.6 Meteorology and Oceanography (METOC) - Joint Hardware**

- Although the data storage requirements for METOC call for at least 2GB of disk space, it is assumed that sufficient storage capacity exists to handle this with existing assets.

**4.1.3.7 Web-Based Access to Mission Applications - Joint Hardware**

- No additional hardware is required to support DARWIN or Enhanced AIRFIELDS.

**4.1.3.8 Theater Battle Management Core System (TBMCS) - Joint Hardware**

- No additional hardware is required to support TBMCS.

#### 4.1.3.9 Joint Force Requirements Generator (JFRG) - Joint Hardware

- No additional hardware is required to support JFRG

### 4.1.4 Software Assumptions - Joint

The primary assumption used by the Services in developing cost estimates for this EPIP is that the Services are responsible for all software license and maintenance costs. However, it is recognized that DISA procured a large number of CDE licenses from TriTeal, Inc., and this procurement is assumed to be sufficient to satisfy the initial CDE license requirements of the GCCS user community. Nevertheless, initial license and maintenance costs for TriTeal CDE are included in this cost analysis and are based on the estimated CDE inventory objectives in each of the Services.

#### 4.1.4.1 GCCS COE Version 2.2 to DII COE Version 3.1 - Joint Software

- DII COE 3.0 COTS software that was included in earlier versions of the COE (e.g., Solaris, HP/UX, Netscape, etc.) are not included in this cost analysis. These COTS products are considered maintenance of the GCCS 2.2 baseline; therefore, the costs are not included herein. Only the costs of new COTS products (i.e., those not included in earlier versions of the COE) are addressed.
- Assume all sites (except PC only sites) will need 1 WinDD server (10 user pack) and additional WinDD server 10 user packs based on the number of SUNs. For example, a site with 40 SUNs needs 1 Win DD server + 3 WinDD additional 10 user packs.
- Microsoft Office is required for all SUN and HP workstations, excluding AMHS server.
- Although the access to Microsoft Office applications is being provided by GCCS 3.0 (via a WinDD implementation), the need for Applix office automation software is not eliminated. Many GCCS applications have dependencies on Applix for the display of data.

#### 4.1.4.2 Integrated Intelligence Capabilities - Joint Software

- Sybase licenses are required to support the MIDB segment.
- An MCM COTS license is required to support the Intelligence Collaboration segment.

**4.1.4.3 Joint Planning and Execution Toolkit (JPET) - Joint Software**

- Objectivity and Orbix COTS licenses are required to support JPET.

**4.1.4.4 Joint Total Asset Visibility (JTAV) - Joint Software**

- No special COTS licenses are required to support JTAV.

**4.1.4.5 Joint Personnel Asset Visibility (JPAV) - Joint Software**

- No special COTS licenses are required to support JPAV.

**4.1.4.6 Meteorology and Oceanography (METOC) - Joint Software**

- No special COTS licenses are required to support METOC.

**4.1.4.7 Web-Based Access to Mission Applications - Joint Software**

- AIRFIELDS will be accessed via the GCCS 3.0 Java version thereby eliminating the need for the ADA-SQL Connect COTS product. Any web-server software package is capable of hosting this application including the existing Netscape Web Server. Thus, no additional COTS is required for this application.
- An Oracle Web Server license is required to support the web-based AHQ application (a.k.a. DARWIN). The Oracle Web Server license covers the same number of concurrent users as the RDBMS server license.

**4.1.4.8 Theater Battle Management Core System (TBMCS) - Joint Software**

- No special COTS licenses are required to support TBMCS.

**4.1.6.9 Joint Force Requirements Generator (JFRG) - Joint Software**

- No special COTS licenses are required to support JFRG.

4.1.5 Training Assumptions - Joint

The GCCS program funds the development of new courses, and AETC develops course curricula with inputs from the DISA PMO. AETC POMs for training courses to support the estimated training requirement. The JTO also operates with its own budget line. The cost incurred by the Services for training is generally for TDY.

## 4.2 Assumptions for DISA-Sponsored Sites

### 4.2.1 Scope - DISA

DISA is responsible for the operation and maintenance of GCCS at the following sites:

- NMCC
- ANMCC
- OSF

### 4.2.2 Hardware Upgrades and Maintenance - DISA

The following quantities of hardware are assumed at each DISA site:

| Site | Number of Clients | Number of Servers |
|---|---|---|
| NMCC | 59 Sun Sparc 5<br>21 Windows NT | 2 Sun 1000 Database<br>4Sun Sparc 20 Application<br>1 Sun Sparc 20 Print Server<br>1 Sun Sparc 20 AMHS<br>1 PC AMHS SAT |
| ANMCC | 11 Sun Sparc 5 | 2 Sun 1000/2000 Database<br>2 Sun Application<br>1 PC AMHS SAT |
| OSF | 33 Sun Sparc 5<br>3 HP 712<br>10 Windows NT | 14 Sun 1000/2000 Database<br>36 Sun Sparc 20 Application<br>14 HP 712 Application<br>3 Sun Sparc 20 AMHS<br>3 PC AMHS SAT |

- NMCC quantities are based on a January 1997 inventory conducted by the GCCS Management Center (GMC)
- ANMCC quantities are based on a February 1997 inventory conducted by the GMC.
- OSF quantifies are based on a February 1997 inventory conducted by the OSF.

The hardware assumptions used to estimate the cost of each new increment of functionality at DISA sites are provided in the following sections.

**4.2.2.1 GCCS COE Version 2.2 to DII COE Version 3.1 - DISA Hardware**

- No new servers are assumed necessary to support Transarc DCE (i.e., SUN servers) or WinDD (i.e., PC servers) at the NMCC, ANMCC, or OSF.

**4.2.2.2 Integrated Intelligence Capabilities - DISA Hardware**

- The costs for MIDB and IPA servers at the NMCC and ANMCC have not been included. These are assumed to be provided by DIA and NIMA.
- The costs for an additional Sparc 20 server is assumed in FY97 at both the NMCC and ANMCC for local imagery manipulation - this server is referred to as an Imagery Transformation Service (ITS). One high resolution printer is also assumed to be required at each site. Additional workstation and printer requirements for MIG are not assumed to be necessary for the OSF.
- Multimedia hardware to support MCM is assumed to not exist at the NMCC and ANMCC and is assumed to be procured in FY97.

**4.2.2.3 Joint Planning and Execution Toolkit (JPET) - DISA Hardware**

- Multimedia hardware to support JPET is assumed to not exist at the NMCC and ANMCC and is assumed to be procured in FY97. However, since the same multimedia hardware costs are addressed as part of the intelligence increment, they are not included in the JPET costs.

**4.2.2.4 Joint Total Asset Visibility (JTAV) - DISA Hardware**

- No additional JTAV-specific hardware is assumed necessary for the NMCC, ANMCC, or OSF.

**4.2.2.5 Joint Personnel Asset Visibility (JPAV) - DISA Hardware**

- No additional JPAV-specific hardware is assumed necessary for the NMCC, ANMCC, or OSF.

**4.2.2.6 Meteorology and Oceanography (METOC) - DISA Hardware**

- No additional METOC-specific hardware is assumed necessary for the NMCC, ANMCC, or OSF.

**4.2.2.7 Web-Based Access to Mission Applications - DISA Hardware**

- No additional DARWIN/AIRFIELDS-specific hardware is assumed necessary for the NMCC, ANMCC, or OSF.

**4.2.2.8 Theater Battle Management Core System (TBMCS) - DISA Hardware**

- No TBMCS-specific hardware is assumed necessary for the NMCC, ANMCC, or OSF.

### 4.2.3 Software Assumptions - DISA

The software assumptions used to estimate the cost of each new increment of functionality at DISA sites are provided in the following sections.

**4.2.3.1 GCCS COE Version 2.2 to DII COE Version 3.1 - DISA Software**

- New license/maintenance costs for the following COTS products are assumed for every SUN and HP client machine at the NMCC, ANMCC and OSF sites (upgrade costs for other SUN and HP COTS products required for DII COE v. 3.1 are assumed to be covered under existing maintenance agreements).
  - Triteal CDE
  - Transarc DCE client
  - WinDD client
- No new COTS license/maintenance costs are assumed for PC clients at the NMCC, ANMCC, and OSF sites.
- New license/maintenance costs for the following COTS product are assumed for SUN and HP application servers at the NMCC, ANMCC, and OSF sites.
  - Transarc DCE Cell Directory Service
  - Transarc DCE Security Service

**4.2.3.2 Integrated Intelligence Capabilities - DISA Software**

- MCM will be supported on 59 machines in the NMCC, 11 machines in the ANMCC, and 2 machines at the OSF.
- MIDB access is assumed for 59 users at the NMCC, 11 users at the ANMCC, and 2 users at the OSF. Thus, the cost for 72 Sybase SQL server licenses is

assumed. Sybase licenses are assumed to currently exist at the NMCC, ANMCC and OSF so Sybase costs are considered part of the existing baseline and are therefore not included in this analysis.

- IPA/IPL access and TBMD are assumed for 59 users in the NMCC, 11 users in the ANMCC, and 2 users at the OSF.

**4.2.3.3 Joint Planning and Execution Toolkit (JPET) - DISA Software**

- JPET is assumed for 59 users at the NMCC, 11 users at the ANMCC, and 2 users at the OSF. Thus, the cost of 72 Objectivity and 72 Orbix licenses is assumed.
- Approximately $395K is required to complete segmentation of JPET software for DII COE version 3.1.
- Approximately $452K is required for annual corrective and perfective software maintenance for JPET. Current assumption is that DISA will fund this cost element.

**4.2.3.4 Joint Total Asset Visibility (JTAV) - DISA Software**

- No GCCS-specific software costs are assumed for JTAV at DISA sites.

**4.2.3.5 Joint Personnel Asset Visibility (JPAV) - DISA Software**

- No GCCS-specific software costs are assumed for JPAV at DISA sites.

**4.2.3.6 Meteorology and Oceanography (METOC) - DISA Software**

- No GCCS-specific software costs are assumed for METOC at DISA sites.

**4.2.3.7 Web-Based Access to Mission Applications - DISA Software**

- New license/maintenance costs for the following COTS product are assumed for a single SUN database server at the NMCC, ANMCC, and OSF sites to support the DARWIN application.
    - Oracle Web Server

  Upgrade costs for other SUN database server COTS products are assumed to be covered under existing maintenance agreements.

- The Java version of AIRFIELDS obviates the need for ADA SQL Connect COTS licenses.

**4.2.3.8 Theater Battle Management Core System (TBMCS) - DISA Software**

- No GCCS-specific software costs are assumed for TBMCS at DISA sites.

**4.2.3.9 Joint Force Requirements Generator (JFRG) - DISA Software**

- Approximately $335K is required to port JFRG to a Windows NT environment and to modify JFRG to satisfy Joint requirements. Approximately $300K per year (FY-98 through FY-06) is required for corrective and perfective software maintenance for JFRG. Current assumption is that DISA will fund these efforts.

4.2.4 Communications - DISA

No changes to existing communications costs at DISA sites are assumed as a result of the new increments of functionality.

4.2.5 System, Network, and Security Administration - DISA

No changes to existing levels of system administration at DISA sites are assumed as a result of the new increments of functionality.

4.2.6 Training - DISA

This section addresses both the costs of DISA-funded training development at AETC and the JTO and the costs of initial user and system administration training at DISA-supported operational sites. As discussed in Annex G (Training Annex), the GCCS 3.0 training concept is comprised of three distinct efforts:

- Transition Team Training - Focused on the actions that administrators must take to transition from version 2.2 to version 3.0.
- Block 1 Training - Focused on the new technology associated with GCCS 3.0 Phase 1. The primary audience is system and database administrators.
- Block 2 Training - Focused on the new functionality associated with GCCS 3.0 Phase 2. The primary audience is operational users.

**4.2.6.1 Training Development**

**4.2.6.1.1 Transition Team Training Development**
This training is associated with physically converting a GCCS 2.2 database server to a version 3.0 database server. Subject matter experts will provide information seminars and will be available for questions. Both Sun and HP platforms will be addressed. AETC and JTO are not supporting the Transition Team Training. DISA is using vendors and in-house resources for this effort.

Transition Team Training cost is approximately $40,000.00. (includes both development and delivery of the course).

**4.2.6.1.2 Block 1 Training Development**
Block 1 training will be developed by AETC and the JTO. This effort includes the costs associated with developing system/database administrator training to support the move to the DII COE 3.1 and includes development efforts for the following:

- Solaris 2.5.1
- Oracle 7.3.2.3
- Common Desktop Environment (CDE) 3.1
- TP Edit
- TARGET

In the past AETC and JTO personnel have had to travel to DISA's OSF to develop training using DISA computer resources. However, to support GCCS 3.0 (and training development for future increments) DISA has purchased Sun Ultra SPARC 4000's for the AETC and JTO locations. The cost for this was $514,000.00 (FY97 dollars). Thus, AETC and JTO now have their own version 3.0 testbed and will not have to travel to the OSF to develop training courses.

Personnel required to develop training courses at AETC are provided under Air Force funding lines; therefore, DISA does not incur the cost of personnel required to develop training at AETC. However, DISA has provided $250,000.00 to JTO for training development efforts at that location.

$514,000.00 + $250,000.00 = $764,000.00 total for Block 1 Training development.

**4.2.6.1.3 Block 2 Training Development**
Training courses for the new mission applications also need to be integrated into the existing course structure of both AETC and the JTO. This will be accomplished via Block 2 Training development which is required for the following applications:

- Solaris 2.5.1
- Oracle 7.3.2.3
- Common Desktop Environment (CDE) 3.1
- TP Edit
- TARGET
- System Security
- Common Operational Picture (COP)
- Intelligence Feed (COP)
- Tactical Ballistic Missile Defense (TBMD)
- Theater Battle Management Control System (TBMCS)
- DARWIN
- Airfields
- Joint METOC Segment (JMS)
- JPET
- JTAV
- JPAV
- MIDB
- Sybase (MIDB)

AETC and JTO will also be able to work from their home stations on Block 2 Training development; therefore, no TDY costs will be incurred.

As is the case with Block 1 training, personnel required developing training courses at AETC are provided under Air Force funding lines; therefore, DISA does not incur the cost of personnel required to develop training at AETC. A portion of the $250,000.00 DISA has provided to the JTO for Block 1 training is being used for Block 2 training development efforts as well.

**4.2.6.2 Initial Training**

In the past, a combination of schoolhouse training and Mobile Training Teams (MTTs) have been used to provide initial GCCS training. Schoolhouse training has been (and will continue to be) the primary means for training new GCCS users. Schoolhouse training will be updated NLT 1 January 98. All persons attending schoolhouse training after that date will be trained on version 3.0.

MTTs have been used to provide “delta” training for new GCCS releases to the existing GCCS user community (i.e., by bringing the training directly to the users’ sites). However, for many reasons, MTT-provided training is now generally regarded as inefficient and is the least preferred

method for providing “delta” training. If used at all, MTTs will most likely be employed for select Block 1 training (i.e., system and database administrators at select sites only). It is unlikely that MTTs will be used for Block 2 training.

The inefficiencies of MTTs have caused the training community to investigate alternative methods for providing delta training to existing GCCS users. Among the alternative methods are training videos, interactive CD-ROMs, and web-based training.

**4.2.6.2.1 Transition Team Initial Training (DISA Supported Sites Only)**

This training will be provided at the OSF with limited seating due to the number of available terminals. As indicated in section 4.2.6.1.1, the cost of teaching the course is included in the estimate for course development. No TDY costs are assumed necessary for DISA personnel.

**4.2.6.2.2 Block 1 Initial Training (DISA Supported Sites Only)**

System and database administration training costs directly attributable to fielding GCCS version 3.0 are primarily associated with the following:

- Solaris 2.5.1
- Oracle 7.3.2.3
- Common Desktop Environment (CDE) 3.1
- TP Edit
- TARGET

The following number of administrators support operations at the NMCC and ANMCC:

| | **No. Personnel NMCC** | **No. Personnel ANMCC** |
|---|---|---|
| System Administrator (Military/Civilian) | 21 | 10 |
| System Administrator (Contractor) | 8 | 2 |
| DBA | 2 | 1 |
| JOPES DBA/JOPES Application Administrator | 27 | 0 |
| GSORTS Administrator | 4 | 0 |
| Communications Specialists | 5 | 0 |
| Security | 3 | 1 |

| | | |
|---|---|---|
| Totals: | 70 | 14 |

At this stage, it is not clear whether MTTs or alternative media methods will be used to provide Block 1 training to DISA-supported operational sites. However, in order to be conservative, use of MTTs are assumed for system and database administration personnel at the NMCC and ANMCC. Approximately three weeks of MTT training at $13,700.00 per week is assumed ($41,100.00 total). This training will most likely be conducted at the OSF (15 terminals with two persons per terminal). No TDY costs are assumed.

**4.2.6.2.3 Block 2 Initial Training (DISA Supported Sites Only)**

For the purpose of this analysis, an estimate of $350,000.00 is provided for the production of an exportable, interactive CD-ROM training package that covers transition issues and the differences of GCCS 3.0. This cost covers not only the initial Block 2 training requirement for operational users at the NMCC and ANMCC, but also the cost of Block 2 training for the majority of GCCS users in DOD.

## 4.3 Assumptions for Navy-Sponsored Sites

### 4.3.1 Scope - Navy

The Navy is responsible for supporting the operation and maintenance of the following sites:

Primary Server Sites: Have Sun 1000 database servers installed, along with at least two Sparc 20 application servers. These sites are:

US Atlantic Command (USACOM), Norfolk, VA (only Navy supported JOPES Database site)

US Pacific Command (USPACOM), Camp Smith, HI

Commander-in-Chief Atlantic Fleet (CINCLANTFLT), Norfolk, VA

Commander-in-Chief Pacific Fleet (CINCPACFLT), Makalapa, HI

CNO/Navy Command Center (NCC), Washington, DC

Commander-in-Chief Naval Forces Europe (CINCUSNAVEUR), London, UK

Commander, Navy Central Command (Forward) (NAVCENTCOM), Bahrain

HQ, US Forces Japan (USFJ), Yokota AB, Japan

Secondary Server Sites: Have at least one application servers (Sparc 20s) installed. These sites are:

Commander, Iceland Defense Forces (COMICEDEFOR), Keflavik, Iceland

Commander, US Forces Azores (COMUSFORAZ), Lajes Field, Portugal

Commander, Special Operations Forces Atlantic Command (COMSOCACOM), Norfolk, VA

Remote Sites: Typically have two TAC-4 workstations and connect back to a JOPES database site via an applications server site. These sites are:

Caribbean Reconnaissance Operation Center (CARIBROC), Key West, FL

Commander, Naval Reserve Forces (COMNAVRESFOR), New Orleans, LA

Commander, Naval Air Forces Atlantic (COMNAVAIRLANT), Norfolk, VA

Commander, Amphibious Group Two (COMPHIBGRU2), Little Creek, VA

Commander, Carrier Group Six (COMCARGRU6), Jacksonville, FL

Commander, Cruiser Destroyer Group Twelve (COMCRUDESGRU12), Mayport, FL

Commander Task Force 72 (CTF 72), Kamiseya, Japan

Commander, Logistics Group Western Pacific (COMLOGWESTPAC), Singapore

Tactical Training Group Pacific (TACTRAGRUPAC), San Diego, CA

Commander, Naval Forces Japan (COMNAVFORJAPAN), Yokosuka, Japan

Commander, Submarine Group Seven (COMSUBGRU7) (CTF 74), Yokosuka, Japan

Commander, Amphibious Group One (COMPHIBGRU1) (CTF 76), Okinawa, Japan

Commander Naval Engineering Facility Command (COMNAVFACENGCOM), Alexandria, VA

Naval Ordnance Center (NAVORDCEN), Indian Head, MD

Commander Western Hemisphere Group (CWHG) Mayport, FL (FY 97)

Commander Navy Central Command (Rear), Tampa, FL

Ships: These ship types have one PC loaded with MAGTF II, Netscape, and IRC installed to support their GCCS requirements:

CV/CVN

LCC/AGF (Fleet Flagships)

LHD

LHA

LPH

4.3.2 Hardware Upgrades and Maintenance - Navy

The hardware assumptions used to estimate the Navy's costs for the new increments of functionality are provided in the following sections.

**4.3.2.1 GCCS COE Version 2.2 to DII COE Version 3.0 - Navy Hardware**

- No new servers are assumed necessary to support Transarc DCE (i.e., SUN servers) or WINDD (i.e., PC servers) at the Navy sites.

**4.3.2.2 Integrated Intelligence Capabilities - Navy Hardware**

- The costs for UCP, MIDB and IPA servers at the Navy sites have not been included.
- The cost of two additional Sparc 20 servers is assumed in FY98 at USACOM and USPACOM for local imagery manipulation via an Imagery Transformation Service (ITS). One high resolution printer is also assumed to be required at each site.
- Eight Sparc 5 workstations to support MCM are assumed to be procured in FY98 for ACOM, PACOM, LANTFLT, and PACFLT because MCM is not HP compatible.

**4.3.2.3 Joint Planning and Execution Toolkit (JPET) - Navy Hardware**

- No additional JPET hardware is assumed necessary for the Navy sites

**4.3.2.4 Joint Total Asset Visibility (JTAV) - Navy Hardware**

- No additional JTAV-specific hardware is assumed necessary for the Navy sites

**4.3.2.5 Joint Personnel Asset Visibility (JPAV) - Navy Hardware**

- No additional JTAV-specific hardware is assumed necessary for the Navy sites

**4.3.2.6 Meteorology and Oceanography (METOC) - Navy Hardware**

- No additional METOC-specific hardware is assumed necessary for the Navy sites.

**4.3.2.7 Web-Based Access to Mission Applications - Navy Hardware**

- One HP J210 JOPES application server is required at ACOM, PACOM, USFJ, CINCLANTFLT, and CINCUSNAVEUR to support Enhanced AIRFIELDS and these are assumed to be procured in FY97.

**4.3.2.8 Theater Battle Management Core System (TBMCS) - Navy Hardware**

- No TBMCS-specific hardware is assumed necessary for the Navy sites.

### 4.3.3 Software Assumptions - Navy

The software assumptions used to estimate the cost of each new increment of functionality at Navy sites are provided in the following sections.

**4.3.3.1 GCCS COE Version 2.2 to DII COE Version 3.0 - Navy Software**

- New license/maintenance costs for the following COTS products are assumed for every client machine at Navy sites.
  - Triteal CDE
  - Transarc DCE client
- New license/maintenance costs for the following COTS product are assumed for SUN and HP application servers at the Navy sites.
  - Transarc DCE Cell Directory Service
  - Transarc DCE Security Service

**4.3.3.2 Integrated Intelligence Capabilities - Navy Software**

- MCM will be supported on 8 machines Navy-wide.
- Approximately $500K per year is required for corrective and perfective maintenance of the TBMD segments.

Current assumption is that the Navy will fund this cost element.

#### 4.3.3.3 Joint Planning and Execution Toolkit (JPET) - Navy Software

- No GCCS-specific software costs are assumed for JPET at Navy sites.

#### 4.3.3.4 Joint Total Asset Visibility (JTAV) - Navy Software

- No GCCS-specific software costs are assumed for JTAV at DISA sites.

#### 4.3.3.5 Joint Personnel Asset Visibility (JPAV) - Navy Software

- No GCCS-specific software costs are assumed for JPAV at Navy sites.

#### 4.3.3.6 Meteorology and Oceanography (METOC) - Navy Software

- No GCCS-specific software costs are assumed for METOC at Navy sites.
- Approximately $758K is required for corrective and perfective maintenance of the Navy's Joint METOC Segment (JMS). Current assumption is that the Navy will fund this cost element.

#### 4.3.3.7 Web-Based Access to Mission Applications - Navy Software

- New license/maintenance costs for the following COTS product are assumed for five SUN database servers at ACOM, PACOM, USFJ, CINCLANTFLT, and CINCUSNAVEUR.
    - Oracle Web Server

#### 4.3.3.8 Theater Battle Management Core System (TBMCS) - Navy Software

- No GCCS-specific software costs are assumed for TBMCS at Navy sites.

### 4.3.4 Communications - Navy

No changes to existing communications costs at Navy sites are assumed as a result of the new increments of functionality.

### 4.3.5 System, Network, and Security Administration - Navy

No changes to existing levels of system administration at Navy sites are assumed as a result of the new increments of functionality.

### 4.3.6 Training - Navy

No costs were estimated for this cost category.

## 4.4 Assumptions for USMC-Sponsored Sites

### 4.4.1 Scope - USMC

The Marine Corps GCCS program consists of a total of 4 Sparc 1000 database servers, 223 Sun Sparc 20 application server/workstations, and 52 NT Pentium PCs; geographically dispersed from the CONUS to Hawaii, Okinawa Japan, and Germany. These application servers are pointed to JOPES DB servers owned and operated by the other Services and DISA. The Marine Corps groups its sites into enclaves using Motorola Network Encryption Systems (NES) for intra-enclave encryption and provides SIPRNET access from the enclaves to the DISA provided SIPRNET point-of-presence. This architecture provides a completely IP routed solution.

No provision for growth is contained in the USMC estimate.

### 4.4.2 Hardware Assumptions - USMC

The Joint hardware refresh cycles are assumed for any incremental hardware associated with this EPIP:

#### 4.4.2.1 GCCS COE Version 2.2 to DII COE Version 3.0 - USMC Hardware

- No new servers are assumed necessary to support Transarc DCE (i.e., SUN servers) or WinDD (i.e., PC servers) at USMC sites.

#### 4.4.2.2 Integrated Intelligence Capabilities - USMC Hardware

- The costs for MIDB and IPA servers at USMC sites have not been included.
- High resolution printers are required (22).
- Multimedia hardware to support MCM is assumed to not exist at USMC application server sites (37) and is assumed to be procured in FY97.

#### 4.4.2.3 Joint Planning and Execution Toolkit (JPET) - USMC Hardware

- Multimedia hardware to support JPET is assumed to not exist at USMC sites and is assumed to be procured in FY97. However, since the same multimedia hardware costs are included under the intelligence section, they are not included as part of JPET costs.

#### 4.4.2.4 Joint Total Asset Visibility (JTAV) - USMC Hardware

- No JTAV-specific equipment will be necessary.

**4.4.2.5 Joint Personnel Asset Visibility (JPAV) - USMC Hardware**

- No JPAV-specific equipment will be necessary.

**4.4.2.6 Meteorology and Oceanography (METOC) - USMC Hardware**

- No METOC-specific equipment will be necessary.

**4.4.2.7 Web-Based Access to Mission Applications - USMC Hardware**

- No additional hardware is required to support Enhanced AIRFIELDS or DARWIN.

**4.4.2.8 Theater Battle Management Core System (TBMCS) - USMC Hardware**

- AF only application; therefore, no additional hardware is required to support TBMCS.

4.4.3 Software Assumptions - USMC

The primary guiding assumption used by the Services in developing cost estimates for this EPIP is that the Services are responsible for all software license and maintenance costs. DISA-provided licenses are not assumed at any USMC sites.

**4.4.3.1 GCCS COE Version 2.2 to DII COE Version 3.1 - USMC Software**

- Assume all garrison sites (52) and deployable sites (26) will need 1 WinDD server (10 user pack).
- All 223 Sun clients require the following:
  - Netscape Navigator (or Communicator) browser licenses.
  - Triteal CDE
  - Transarc DCE client
  - WinDD client
- New license/maintenance costs for the following COTS products are assumed for every USMC PC client (56)

- New license/maintenance costs for the following COTS product are assumed for SUN application servers.
  - Transarc DCE Cell Directory Service
  - Transarc DCE Security Service
- An upgrade to Solaris 2.5.1 for all SUN machines (227) is assumed to be required in FY97. An upgrade of the

SUN operating systems are assumed every two years thereafter.

- Netscape Proxy Server is assumed to be required at the USMC's 4 database sites
- An upgrade of Netscape is assumed to be required every 2 years after initial purchase.

**4.4.3.2 Integrated Intelligence Capabilities - USMC Software**

- MCM will be supported on 37 USMC application servers.
- MIDB access is assumed for 37 USMC application servers, thus, Sybase SQL server licenses are needed. Sybase licenses are assumed to currently exist at the 223 USMC application servers operating on GCCS v2.2.2.

**4.4.3.3 Joint Planning and Execution Toolkit (JPET) - USMC Software**

- Objectivity and Orbix COTS licenses are required at 37 USMC application servers to support JPET.

**4.4.3.4 Joint Total Asset Visibility (JTAV) - USMC Software**

- No special COTS licenses are required to support JTAV.

**4.4.3.5 Joint Personnel Asset Visibility (JPAV) - USMC Software**

- No special COTS licenses are required to support JPAV.

**4.4.3.6 Meteorology and Oceanography (METOC) - USMC Software**

- No special COTS licenses are required to support METOC.

**4.4.3.7 Web-Based Access to Mission Applications - USMC Software**

- No special COTS licenses are required to support AIRFIELDS or DARWIN.

**4.4.3.8 Theater Battle Management Core System (TBMCS) - USMC Software**

- No special COTS licenses are required to support TBMCS.

**4.4.3.9 Joint Force Requirements Generator - USMC Software**

- Current assumption is that DISA will fund this cost element per Memorandum of Agreement among DISA, USMC, and the Joint Staff.

### 4.4.4 Training Assumptions - USMC

The GCCS program funds the development of new courses to train for new functionality, then turns it over to the training organizations to incorporate into their curricula. AETC POMs for training courses to support the estimated training requirement. The JTO also operates with its own budget line. The cost incurred by the Services for training is generally for TDY.

## 4.5 Assumptions for Army-Sponsored Sites

### 4.5.1 Scope - Army

The ARMY is responsible for supporting the operation and maintenance of GCCS at the following sites: FORSCOM, ARCENT, ARPAC, AREUR, HQDA, EUCOM, SOUTHCOM, USARSO, EUSA, USFK, LOGSA, MTMC, and the AWC. Numerous remote workstation are connected to these sites.

### 4.5.2 Hardware Upgrades and Maintenance - Army

- Hardware procurement, upgrade, and maintenance costs will increase with the growth of GCCS to include fielding GCCS to the Army Corps.
- Hardware maintenance costs were calculated at an industry standard of 10% of procurement cost annually.
- Technology insertion is required every three years as older hardware becomes obsolete.
- All maintenance for materials & communications equipment are included in the annual hardware maintenance costs estimates.
- All Sun Sparc 5 workstations fielded in FY95 run GCCS applications.
- Half of the Sun Sparc 20 servers run GCCS applications.
- All database servers (i.e., 1000,2000,4000) run GCCS applications.
- All PC based workstations run AGCCS applications.
- Specific hardware and software configurations for each Army site are available upon request.
- The Army will purchase 13 Sparc 1000, 13 Sparc 20 WAN servers, 94 Sparc 20 LAN servers(V1), 47 Sparc 20 LAN servers (V2)and 951 Pentium workstations in FY97.
- Hardware maintenance costs for FY97 and out are $700,000 annually.

**4.5.2.1 GCCS COE Version 2.2 to DII COE Version 3.0 - Army Hardware**

- Because of version 3.0, all database servers require main memory and disk storage upgrades
- All Army 1000/2000 Sun database servers require RAM & secondary storage upgrades for GCCS Version 3.0

**4.5.2.2 Integrated Intelligence Capabilities - Army Hardware**

- The Army will use the Intelligence database and Imagery Access functions beginning in FY98. Current estimate is $400K per year

**4.5.2.3 Joint Planning and Execution Toolkit (JPET) - Army Hardware**

- Multimedia hardware to support JPET is assumed to not exist at Army sites and is assumed to be procured in FY97. However, since the same multimedia hardware costs are included under the intelligence section, they are not included as part of JPET costs.

**4.5.2.4 Joint Total Asset Visibility (JTAV) - Army Hardware**

- No JTAV-specific equipment will be necessary.

**4.5.2.5 Joint Personnel Asset Visibility (JPAV) - Army Hardware**

- No JPAV-specific equipment will be necessary.

**4.5.2.6 Meteorology and Oceanography (METOC) - Army Hardware**

- No METOC-specific equipment will be necessary.

**4.5.2.7 Web-Based Access to Mission Applications - Army Hardware**

- No additional hardware is required to support Enhanced AIRFIELDS. The Army will not use AIRFIELDS at Army sites. If the Army CINC sites (EUCOM, SOUTHCOM and FORSCOM/AOC) require AIRFIELDS, the costs will be adjusted.

**4.5.2.8 Theater Battle Management Core System (TBMCS) - Army Hardware**

- No costs are associated with TBMCS.

### 4.5.3 Software Upgrades and Maintenance - Army

- The majority of the funding is used for DII COE software licensing.
- Software maintenance costs were calculated at an industry standard of 15% of procurement cost annually.
- GCCS 3.0-related software costs = $3.5 million in FY97 and $2.1 in FY98.
  - Software maintenance is $600,000 annually based on the current configurations at Army sites This also includes equipment at Armies and four Corps.

#### 4.5.3.1 GCCS COE Version 2.2 to DII COE Version 3.1 - Army Software

- Procurement of GCCS DCE packages are included in this increment.

#### 4.5.3.2 Integrated Intelligence Capabilities - Army Software

- No specific assumptions.

#### 4.5.3.3 Joint Planning and Execution Toolkit (JPET) - Army Software

- JPET software is estimated at $50K per year beginning in FY98. The Army Operations Center and FORSCOM will be the first sites fielded.

#### 4.5.3.4 Joint Total Asset Visibility (JTAV) - Army Software

- No special COTS licenses are required to support JTAV.

#### 4.5.3.5 Joint Personnel Asset Visibility (JPAV) - USMC Software

- No special COTS licenses are required to support JPAV.

#### 4.5.3.6 Meteorology and Oceanography (METOC) - Army Software

- No special COTS licenses are required to support METOC.

#### 4.5.3.7 Web-Based Access to Mission Applications - Army Software

- No special COTS licenses are required to support AIRFIELDS. The Army will not use AIRFIELDS at Army sites. If the Army CINC sites (EUCOM, SOUTHCOM and

FORSCOM/AOC) require AIRFIELDS, the costs will be adjusted.

#### 4.5.3.8 Theater Battle Management Core System (TBMCS) - Army Software

- No special COTS licenses are required to support TBMCS.

### 4.5.4 Communications - Army

- SIPRNET costs for communications are operations & maintenance are paid by each Army site.
- Bandwidth requirements for GCCS will increase. Therefore SIPRNET WAN bandwidths and site LAN segment bandwidths will increase.
- Version 3.0 communications upgrade costs are difficult to estimate until the system is fielded. However, a PM estimate for upgrading one third of communications infrastructure annually at each site is $1 million annually to operate GCCS at all Army sites.

### 4.5.5 Network and System Administration - Army

- All site GCCS network and administration cost for salaried personnel, system administration, and facilities maintenance are Army site incurred
- All sites previously provided input to GCCS network and administration costs

### 4.5.6 Training - Army

- GCCS Version 3.0 will be provided by DISA mobile training teams or at the GCCS training site. Army sites will provide TDY training costs which are estimated at $350K in FY97.

### 4.5.7 Funding Perspective - Army

- The Army’s current FY97 funding profile provides for GCCS Version 3.0 integration at Army sites.

## 4.6 Assumptions for Air Force-Sponsored Sites

### 4.6.1 Scope - Air Force

A list of Air Force supported sites is available upon request. As of April 1997 over 140 units have been installed. New installations are expected to progress at a rate of 30 - 40 units per year.

### 4.6.2 Limitations - Air Force

- The costs in this EPIP are based upon bottom-up estimates of the number of servers, workstations, and applications running at various sites throughout DOD. The number of workstations and applications running at any given site were best estimates at a given point in time. Installation, however, have continued throughout FY97. Estimates are subject to change.
- The cost of network communications devices (routers, LANs, WANs, cables, and associated equipment) are not included.
- SIPRNET charges are not included.
- Resources used to support the GCCS Management structure established by CJCSI 6721.01, *GCCS Management Structure*, are not included.
- Program Management Office (PMO) costs are not included.
- The cost of initial training is not included.

### 4.6.3 Hardware Assumptions - Air Force

The following hardware refresh cycles are assumed for any incremental hardware associated with this EPIP:

- Workstations and associated cables and non-printing peripherals are replaced on a three year cycle. One third of the inventory of these devices is replaced each year after initial procurement of all devices in year 1 (FY 1998).
- Servers, printers, and non-network communications devices are replaced on a three year cycle. The full inventory is replaced every three years after initial procurement in year 1 (FYs 2001, 2004, and 2007).

#### 4.6.3.1 GCCS COE Version 2.2 to DII COE Version 3.0 - Air Force Hardware

- No new servers are required to implement DCE.
- WinDD server is required at all AF sites except those that have PCs only. Despite the fact that WinDD is being added with the introduction of GCCS version 3.0,

the Air Force's position is that, due to user demand, they would have implemented WinDD regardless of version 3.0. Therefore, WinDD servers are assumed to be part of the Air Force's version 2.2 baseline.

- New ACTDs, GSORTS (Enhanced), Oracle Advanced Networking Option, will not be incorporated into V3.0
- No additional hardware required for C2PC.
- Hardware maintenance costs are not included. Majority of GCCS hardware has been incorporated into existing maintenance contracts covered by the MAJCOMs/FOAs/DRUs.
- Ten year projection assumes 50 low-end additional sites will be added each year per current AF projections.
- Ten year life cycle projections assumes no reduction in hardware requirements.

**4.6.3.2 Integrated Intelligence Capabilities - AF Hardware**

- MIDB server required at large AF sites to reduce SIPRNET traffic/bandwidth requirements and provide local storage capability.

**4.6.3.3 Joint Planning and Execution Toolkit (JPET) - AF Hardware**

- JPET (TARGET) will require Sun Video card & camera and will be added to an existing Sparc 20 at sites with either Sparc 1000 or 2000s. Assume this multimedia equipment can be shared by other applications which require multimedia capability, such as JDISS MCM (these costs are broken out separately under FY97)

**4.6.3.4 Joint Total Asset Visibility (JTAV) - AF Hardware**

- JTAV servers will be provided by the Global Combat Support System (GCSS).

**4.6.3.5 Joint Personnel Asset Visibility (JPAV) - AF Hardware**

- JPAV servers will be provided by the Global Combat Support System (GCSS).

**4.6.3.6 Meteorology and Oceanography (METOC) - AF Hardware**

- Although the data storage requirements for METOC call for at least 2GB of disk space, it is assumed that sufficient storage capacity exists to handle this with existing assets.

**4.6.3.7 Access to Web-Based Mission Applications - AF Hardware**

- No additional hardware is required to support Enhanced AIRFIELDS.

- Oracle Web Server, required for DARWIN, will only be installed at the JOPES server site on the existing DB server.

#### 4.6.3.8 Theater Battle Management Core System (TBMCS) - AF Hardware

- No additional hardware is required to support TBMCS.

### 4.6.4 Software Assumptions - Air Force

#### 4.6.4.1 GCCS COE Version 2.2 to DII COE Version 3.0 - Air Force Software

- Assume all sites (except PC only sites) will need 1 WinDD server (10 user pack) and additional WinDD server 10 user packs based on the number of SUNs. For example, a site with 40 SUNs needs 1 Win DD server + 3 WinDD additional 10 user packs.
- All PCs require X-terminal software and Netscape Navigator (or Communicator) browser licenses.
- Any site with a SUN 1000 or 2000 requires a Netscape Enterprise server and would also have a Newsgroup, which requires Netscape News Server, and Netscape Mail server. A Netscape Proxy server is also required at these sites.
- The following software, which is not covered by maintenance agreements, will require upgrades every two years:
    - Solaris
    - HP/UX
    - Netscape
- Microsoft Office is required for all SUN workstations, excluding AMHS server.
- Although the access to MicroSoft Office applications is being provided by GCCS 3.0 (via a WinDD implementation), the need for Applix Office Automation software is not eliminated. Many GCCS applications have dependencies on Applix for the display of data.
- Assume that the only additional S/W COTS required for Joint GCCS 3.0 are:
    - Triteal CDE (all SUNS)
    - Transarc DCE client (all SUNS)
    - Transarc server (sites with either Sparc 1000 or 2000s)

- Netscape Proxy Servers (sites with either Sparc 1000 or 2000s)
- MSQL (all SUNS)
- Oracle Web Server (JOPES sites only)
- Orbix (sites with either Sparc 1000 or 2000s, add'l SW needed for TARGET 2.3)
- WinDD Server and additional license packs (1 per site plus additional 10 user packs based on # of SUNS except sites with PCs only)
- CMDS, Stalker, and Secret Agent security packages
- MCM (needed for Intel Collaboration)
- 32 user Sybase SQL server (needed for MIDB) (these costs are broken out separately under FY97)

- Assume the 50 additional sites which will be added each year will require the SW licenses listed below and sites already installed will remain under maintenance for SW listed below:
  - For all SUNS only
    - Triteal CDE
    - Transarc DCE client
    - Microsoft Windows & Office
  - For all SUNS & PCs
    - Applix
    - Oracle
    - Gain Momentum Runtime
    - Netscape Navigator
    - Verity TOPIC
  - For all Sparc 1000 or 2000s
    - SUN Backup
    - SUNNet Manager
    - Objectivity & Orbix (for TARGET)
  - For all sites with either a Sparc 1000 or 2000
    - Netscape News Server
    - Netscape Mail Server
    - Netscape Enterprise Server
    - Netscape Proxy Server
    - Sybase SQL Server 16 user license (except JOPES & COMPES sites require 32 user license)
  - For all servers
    - Empire UNIX System Mgmt Agent
  - For JOPES server sites

    - Legent DB agent (which DISA purchased for AF JOPES sites)
    - Oracle Web Server, 32 user license
  - For all PCs
    - X-terminal software (PC Xware)
  - For all Printers
    - Newsprint software
  - One Netmetrix Power agent is required at each site
  - GCCS will fund WinDD server licenses which will be utilized to access these applications along with others.
- Assume ESC/AVN will procure Solaris 2.5.1 for unit cost of $175 for all old H/W which was either purchased by DISA, or by the sites themselves. ESC/AVN's current H/W purchases include Solaris 2.5.1 and ESC/AVN has a waiver letter from SUN to cover all H/W for Solaris 2.5.1 purchased by ESC/AVN
- Assume all PCs procurements will continue to come bundled with NT operating system and Office Pro.
- Assume no new mature ACTDs (Leading Edge insertions), GSORTS (Enhanced), Oracle Advanced Networking Option will be included in GCCS 3.0, which may require additional SW COTS

**4.6.4.2 Integrated Intelligence Capabilities - Air Force Software**

- Sybase licenses are required to support the MIDB segment.
- An MCM COTS license is required to support the Intelligence Collaboration segment.
- Assume no new sites will require additional JDISS licenses and will remote to a host site with this capability if required.

**4.6.4.3 Joint Planning and Execution Toolkit (JPET) - Air Force Software**

- Objectivity and Orbix COTS licenses are required to support JPET.
- Assume no new sites will require additional JDISS licenses and will remote to a host site with this capability if required.

**4.6.4.4 Joint Total Asset Visibility (JTAV) - Air Force Software**

- No special COTS licenses are required to support JTAV.

**4.6.4.5 Joint Personnel Asset Visibility (JPAV) - Air Force Software**

- No special COTS licenses are required to support JPAV.

**4.6.4.6 Meteorology and Oceanography (METOC) - Air Force Software**

- No special COTS licenses are required to support METOC.

**4.6.4.7 "Web-Based Mission Applications" - Air Force Software**

- AIRFIELDS will be accessed via the GCCS 3.0 Java version thereby eliminating the need for the ADA-SQL Connect COTS product.
- DARWIN requires Oracle Web Server at JOPES DB sites.
- C2PC (NT-based Unified Build) will not require additional licenses.

**4.6.4.8 Theater Battle Management Core Systems - Air Force Software**

- Approximately $200K per year (FY 98-06) is required to perform corrective and perfective maintenance on the Joint TBMCS segments. Current assumption is that the Air Force will fund this cost element.

**4.6.5 Training Assumptions - Air Force**

- In addition to the AETC and JTO courses which will be scheduled, the Air Force is planning to procure minimum essential commercial classes to conduct “difference training” for technicians. We do not anticipate that AETC will be able to rapidly develop and field classes to support the number of students who will rapidly require “difference” training. The following commercial classes will be required
    - Solaris 2.5 System Administration
    - Oracle 7.3 New Features
    - Transarc DCE
- Five instances of each course will be required @ $100K per course.
    - Three CONUS-based
    - One in PACAF
    - One in USAFE

- Estimated tech support training (min. essential) required for V3.0: $1.5M. These costs are included under the DII COE increment in FY97.

- A training plan to support functional requirements is not available, consequently associated training costs could not be determined at this time.

(INTENTIONALLY BLANK)

ANNEX K TO ENCLOSURE 2

RISK ANALYSIS

## 1. Risk Areas Overview.

The risks for GCCS Version 3 can be placed in five categories: 1) Management, 2) Development, 3) Technical, 4) Security, and 5) Transition risk. Overall risk for GCCS Release 3.0 is assessed as medium after consideration for the mitigation plans.

## 2. Management.

The overall management risk for GCCS Release 3.0 is assessed as medium with consideration for the listed mitigation activities. The specific management risk areas are as follows:

**2.1 Matrix organization for Program Management.** Because of the uniqueness of the GCCS program and the evolving GCCS management structure, a matrix management structure exists for program management. The GCCS program manager is responsibble for program execution, however, for acquisition approach relies on participation from severl organizations. To make the managment of the program go smoothly it requires frequent intereration amoung ASD/C3I, DISA Program Management and Engineering Offices, and Joint Staff Operations and C4 directorate representatives. An Oversight Integrated Product Team (OIPT) structure approves the final program execution strategy.

**2.1.1 Risk.** Conflicting directions, inability to proactively manage resources and risk, failure to meet scheduled events, and not having a single accountable agent directly impacts cost, schedule, and performance. Once the initial GCCS cadre is replaced - the inertia and momentum of the GCCS success may become unmanageable and eventually splinter.

**2.1.2 Mitigation Plan.**

- Maintain active GCCS Integrated Product Teams (IPTs) to mitigate effect of no clear accountable and responsible agent.
- Reaffirm EPIP process with senior level endorsement.
- Maintain User-Developer-Sponsor working groups participation.
- Track multiple thresholds to ensure effort is on track, report up the management chain if thresholds are broken (e.g. SOR target

slips by 1 week alert DISA management, SOR target slips by 2 weeks alert Joint Staff and Services, SOR slips by 4 weeks alert Services, SOR slips 6 weeks alert GCCS Review Board, SOR slips 8 weeks alert GCCS Advisory Group, SOR slips 10 weeks alert ASD(C3I)).

- Minutes from OIPT and lower level working groups clarify decisions and communications (document all decisions, commitments and any associated changes).
- Web pages and electronic mail facilitates communication.
- Documented baselines in form of version EPIP, Joint Staff Priorities, and GCCS related CJCS instructions and manuals defines foundation and roles.
- Formalize the requirements definition, justification ("operational utility") prioritization, and funding, and interoperability (data element standardization, targeting DII COE, and synchronization of data collection methods and data use) processes.
- Foster continuous communication and open dialogue (teamwork).
- Conduct timely GCCS and DII/COE Technology Forums and User Conferences.
- Maintain active OIPT with all stakeholders.

**2.2 Concurrency version release schedules not maintained.** Simultaneous development and release of GCCS 3.0 while maintaining GCCS Top Secret (GCCS(T)and GCCS Release 2.2 activities introduces resource conflicts. New concerns such as century transitions (frequently referred to as Y2K) require additional testing and impact critical resources. A finite resource must be spread to maintain all activities, as well as continue support to the previously fielded GCCS.

**2.2.1 Risk.** Multiple demands on resources and integrating develop/test activities may become overwhelming. Schedule may be impacted as well as some cost impacts for premature fielding. Program credibility at issue if schedule slips become the norm.

**2.2.2 Mitigation Plan.**

- Establish OIPT to initially prioritize actions.
- Track progress via Engineering status meetings.
- Define releases so they have well defined beginning and ends and structured build lists.

- Require Developer's Y2K correction plans and timelines for all Y2K deficiencies.
- Establish Y2K Risk Evaluation Team to "quantify" risk and impact of Y2K issues with each major application developer.

- Assign priorities for work on releases and work those priorities, include Y2K as part of the priorities to be tested (assess the magnitude of the problem, so it can be addressed in a focused manner in future releases).

**2.3 Requirement Creep/Change.** CINC requirement changes, re-directions, and priority shifts are anticipated. This area is especially vulnerable to change using an evolutionary approach.

**2.3.1 Risk.** Failure to establish control mechanisms to properly process changes could lead to program instability and increases in cost/schedule.

**2.3.2 Mitigation Plan.**

- Firmly commit to resource constrained release objectives (e.g. GCCS Release 3.0 Stage 1 moves baseline capability into the DII COE, while GCCS 3.0 Stage 2 targets adding MIG, METOC, JPET, J-FRG, and enhanced communications capabilities, with GCCS follow-on still to be defined by the GCCS Requirements process).
- Establish active user representation within OIPT, resolve requirement change at working levels.
- Keep running list of requirements (as they are identified) that are beyond the scope of the current defined releases, so the "new" requirements get a queue for evaluation and prioritization.
- Use Working Groups to prioritize requirements within a C2 functional community and assign "operational utility ratings," and develop associated Functional Economic Analysis (FEA) for new capabilities.
- Have GCCS Guidance Bodies mediate between C2 function communities to prioritize application segments within GCCS (GCCS Review Board, with inputs from the functional community, prepares the plan for preferred candidates and presents the Approval Decision Package to the GCCS Advisory Group).

**2.4 Event Driven vs. schedule driven program too subjective.** To react to critical user demands and funding, the GCCS activity is to manage/build to a success-oriented, event-driven schedule rather than a resource bounded, priority driven schedule.

**2.4.1 Risk.** Without scheduled milestones, formal progress maybe difficult, especially if targeted events slide to accommodate approved requirement changes. The appearance of sliding milestones jeopardize program support and credibility.

**2.4.2 Mitigation Plan.**

- Establish OIPT to provide a forum for mutual set of targets (e.g., Release date for GCCS Release 3.0).
- Document targets within EPIP and track all delta changes and expected impacts.
- Check impact of delta changes on the established thresholds to alert appropriate management levels of reasons for shifting the threshold(s).
- Use target release date and "Earned Operational Utility" to determine whether a schedule slip is necessary in order to get a specific capability to the field, or if moving the requirements to the next release is a better choice in order to get other available operational utility to the field quickly.

The incorporation of both OIPT (formal working group) and the EPIP (formal documented agreement) provides acceptable progress tracking. The use of a target release date and "earned operational utility" provide a management technique to get the most operational capability to the field in the most efficient manner without losing track of requirements that border releases.

**3. Technical.**
The overall technical risk for GCCS Release 3.0 is assessed as medium with consideration for the listed mitigation activities. The specific technical risk areas are as follows:

**3.1 GCCS-DII/COE interoperability not established**. The GCCS Release 3.0 is implemented and must interoperate with the evolving Defense Information Infrastructure and Common Operating Environment. GCCS 3.0 is the initial fielding of GCCS within the DII/COE. Interoperability with DII/COE includes the operating system Y2K compliance.

**3.1.1 Risk.** Without interoperability, a major goal of the GCCS program will not be accomplished thus increasing cost and decreasing system performance. Delays in fielding DII/COE suite, increases testing/performance risks. Delays in fielding "Y2K compliant" DII COE increases integration/testing, and performance risks.

**3.1.2 Mitigation Plan.**

- Early release of engineering version DII/COE for GCCS lab demonstrations for early identification of potential problems.
- Engineering walk-throughs prior to delivery of segments to DISA.
- Requiring Y2K compliant correction plans and timelines for Y2K deficiencies.
- Co-location of GCCS and DII/COE engineering offices.

**3.2 Technology limitations.** GCCS strategy utilizes “industry standard” hardware and software as the “best of breed” GCCS environment. However, interoperability (use of standardized data elements and synchronization of data collection/usage targets) and multiple level security challenges may be constrained by today’s technology.

**3.2.1 Risk.** System performance may not be achieved because of a technology or design constraint.

**3.2.2 Mitigation Plan.**

- Track “specific” technologies to avoid surprises or premature selection of technical solutions.
- Track data element standardization efforts across C2 functional communities and press for standardization of the most critical shared data elements via the C2 Functional Data Administrator.
- Engage user community in data collection/usage analysis.

**3.3 Database synchronization problems.** Multiple releases and differing versions may cause unacceptable database synchronization issues.

**3.3.1 Risk.** System Performance degraded and corrupted databases.

**3.3.2 Mitigation Plan.**

- Test a little, field a little. Implement initially at test sites to minimize the risk.

- Implementation plan incorporates minimizing synchronization impact techniques .

**3.4 Interfaces not adequately defined.** Data interfaces and external system interfaces must be maintained to meet system performance. GCCS must be hosted on a multiple set of hardware configurations. Targeted environments must be determined for operations and plausible testing.

**3.4.1 Risk.** System Performance degradation/denial of service

**3.4.2 Mitigation Plan.**

- Document data elements per segment, highlighting standardized elements and key elements that need to be standardized (key shared elements or data that is exchanged with other segments or applications).
- Document interfaces and dependencies per segment.
- Establish beta test sites to minimize risk (MDT Stage III at laboratory sites prior to OT&E at operational sites).
- Establish and lead technical evaluations with each developer.
- Document/Validate site configurations.

**3.5 Shortfalls in hardware/software capacity**. As an evolutionary acquisition, the potential to exceed hardware and software capacity at some point is highly likely.

**3.5.1 Risk.** Failure to adequately forecast excess capacity for future system upgrades. Exceeded capacity (or near exceeded capacity) degrades system performances.

**3.5.2 Mitigation Plan.**

- Design open architectures to provide hardware/software growth path.
- Proactive sizing.
- Track key site utilization metrics.
- Report metrics within Performance Plans.
- Use site performance metrics as basis for pre-production testing and require equal or better performance for similar configurations.

**4. DEVELOPMENT.**

The overall development risk for GCCS Release 3.0 is assessed as low with consideration for the listed mitigation activities. The specific development risk areas follow below.

**4.1 Development/testing schedule goals not met and inadequate testing.** Premature completion of testing or failure to adequately test provides increase risk of performance problems.

**4.1.1 Risk.** Failure to achieve or complete testing on-schedule impacts version release date. Cost and performance can also be affected. Failures not found in development testing significantly impacts cost.

**4.1.2 Mitigation Plan.**

- Establish test and evaluation working group to address issues.
- Establish intermediate segment testing and walk-through process.
- Limit GCCS 3.0 Stage 1 Release to move the baseline functionality to the new environment plus TPEDIT and four security segments (SeComp, Secret Agent, CMDS, and Stalker).
- Put clearly defined new applications in GCCS 3.0 Release Stage 2 and take the time to use CONOPS and other sources to develop appropriate test procedures for high risk areas.
- Less well defined new capabilities become candidates for later release based on the requirements prioritization process.

**4.2 Operational testing fails. System performance not met.** Operational testing identifies a critical operational issue that cannot be fully met due to unrealistic expectations, failures in development, poor testing methods, and/or technology limitation. Failures found in operational testing are extensively costly (both time and resources).

**4.2.1 Risk.** Failure to adequately complete OT increases the likelihood of unexpected failures in the field and degradation of system performance.

**4.2.2 Mitigation Plan.**

- Maintain Test Working Groups.
- Coordinated and documented test and evaluation strategy.
- Build contingency planning.
- Establish preliminary testing and user assessment evaluations

- Proactively manage user expectations for each release (e.g. by publishing goals per release, tracking new requirements and identifying when they will be met, publicizing requirements prioritization process).

**4.3 Development does not satisfy user's expectations.** Developing an application that falls short of meeting user requirement or expectation is primarily due to poor communications (user-to-developer) and inadequate documentation.

**4.3.1 Risk.** Failure in operational testing, unexpected system degradation, and performances not as advertised.

**4.3.2 Mitigation Plan.**

- Maintain testing working groups.
- Accomplish Incremental testing, preliminary testing and user assessments.
- User participate within OIPT and EPIP development.
- Document requirements jointly (User/Developer).
- Proactively manage user expectations for reach release (e.g. by publishing goals per release, tracking new requirements and identifying when they will be met, publicizing requirements prioritization process).

**4.4 Shortfalls in contractor development and/or testing capability.** Inadequate resources (equipment, personnel, training, tools, compilers, time....), miscommunications, misunderstandings, and faulty assumptions jeopardize release performance and schedules success.

**4.4.1 Risk.** Bottlenecks in testing, schedule slips, increased regression testing, and degraded system performance.

**4.4.2 Mitigation Plan.**

- Track developer engineering status to prioritize development/testing activities.
- Use developer engineering assessments and compliance evaluation "tiger teams".
- Provide developers with compliance checklists that they must pass at their own facility before delivery to the DISA.
- Use a Modified Developmental Test Readiness Review (MDTRR) to ensure GCCS 3.0 is fully prepared to undergo MDT Stage III at the Laboratory sites.

## 5. SECURITY.

The overall security risk for GCCS Release 3.0 is assessed as medium with consideration for the listed mitigation activities. The specific security risk areas are as follows:

**5.1 Security Accreditation not established.** Accreditation strategy, criteria, and testing must be accomplished and approved, targeting a baseline environment never before used (DII COE).

**5.1.1 Risk.** System Performance degradation and/or denial of service(s).

**5.1.2 Mitigation Plan.**

- Specifically track critical technology that may impact security concerns (SeComp).
- Maintain security concern working group forum.
- Develop a Security CONOPS and Annex E to the EPIP (provide security philosophy, cover section 2 of updated Trusted Facility Manual).
- Check out as many of the DII COE security functions as possible before integrating with the GCCS mission application segments (part of the ST&E strategy).
- Ensure GCCS 3.0 software baseline is available at least two weeks prior to ST&E.
- Use multiple site participation to establish user 'buy-in' for methodology, procedure, and test.
- Assign dedicated security manager within PMO.
- Identify DISA LSO.
- Ensure that DISA LSO provides a cohesive and complete ST&E test plan and procedures at least 30 days prior to ST&E.

## 6. TRANSITION:

The overall transition risk for GCCS Release 3.0 is assessed as low with consideration for the listed mitigation activities. The specific transition risk areas follow below.

**6.1 Training requirements for fielded system not met.** With incremental fielding of GCCS, training prior to release becomes a potential problem. Maintaining an aggressive schedule further exasperates the potential.

**6.1.1 Risk.** Field administration and operations of GCCS with inadequate training impacts system performance and potentially overwhelms the trouble desk.

**6.1.2 Mitigation Plan.**

- Assign full-time training manager within PMO.
- Develop a Training CONOPS as Annex G to this EPIP.
- Maintain Mobile Training Team (MTT) as crisis team.
- Coordination between JS, JTO, AETC, and DISA training office (training working groups).
- Establish on-line, automated training system strategy.
- Track training metric.

**6.2 Maintenance requirements (personnel/budget) increase on fielded system.** GCCS maintenance and supportability must be within the previous Worldwide Military Command and Control System (WWMCCS) budgets. Recognizing increasing functionality needs, Joint command and control system operations must be controlled within a shrinking budget. Life Cycle Costs (LCC) for licenses, upgrades and training must be identified and justified.

**6.2.1 Risk:** Unmanaged command and control development and proliferation of CINC stovepipe systems significantly impacts costs.

**6.2.2 Mitigation Plan:**

- Address maintenance costs with each EPIP Economic Analysis.
- Maintain common operating system and open system architectures.
- Aggressively target duplicative service unique C2 systems for elimination.
- Use Functional Economic Analysis to highlight source of funds for new capabilities.

ANNEX L TO ENCLOSURE 2

ACRONYMS and DEFINITIONS

**List of Acronyms**

| | |
|---|---|
| ADP | Automated Data Processing |
| AHQ | Ad Hoc Query |
| AMC | Air Mobility Command |
| AMHS | Automated Message Handling System |
| APPLIX | Applixware Office Automation Software |
| ARPA | Advanced Research Projects Agency |
| ASET | Automated Security |
| ATO | Air Tasking Order |
| ATOCONF | Air Tasking Order Confirmation |
| AUTODIN | Automated Digital Network |
| | |
| CAP | Crisis Action Planning |
| CCAPPS | Command Center Applications |
| $C^2$ | Command and Control |
| $C^3I$ | Command, Control, Communications, and Intelligence |
| CESP | Civil Engineering Support Plan |
| CHATTER | Unix Talk |
| CHRONLOG | Chronological Log |
| CINCs | Commanders-in-Chief |
| CJTF | Commanders Joint Task Force |
| CNTRY | Country Code/Long Name File |
| COA | Course of Action |
| COE | Common Operating Environment |
| COLSM | Coliseum |
| COMNAVRESFOR | Commander Naval Reserve Force |
| CONTROL | System Controller |
| COTS | Commercial off-the-shelf |
| CTAPS | Contingency Theater Automated Planning System |
| | |
| DART | Dynamic Analysis and Replanning Tool |
| DB | Database |
| DBIF | DB Interface |
| DB SLCT | Select Oracle database |
| DICTION | Data Dictionary |
| DISPLAY | Custom Display |
| DMA | Defense Mapping Agency |
| DMAAC | Defense Mapping Agency Aerospace Center |

| | |
|---|---|
| DMS | Defense Message System |
| DNS | Domain Name Server |
| DoD | Department of Defense |
| DoDIIS | DoD Intelligence Information System |
| DSRS | Defense Software Repository System |
| DTG | Date-Time-Group |
| | |
| ECP | Engineering Change Proposal |
| ELVIS | Enhanced Linked Virtual Information System |
| EM | Executive Manager |
| ESI | External System Interface |
| EUCOM | European Command |
| EVAC | Evacuation System |
| | |
| FAPES | Force Augmentation Planning and Execution System |
| FDDI | Fiber Distribution Data Interface |
| FLTCINCs | Fleet Commanders-in-Chief |
| FRAS | Fuel Resource and Allocation System |
| | |
| GARC | GCCS Air Tasking Order (ATO) Review Capability |
| GBYTES | Gigabytes |
| GCCS | Global Command and Control System |
| GEL | Gain Extension Language |
| GEOFILE | Geographic Location File |
| GEOLOC | Geographic Location |
| GOTS | Government off-the-shelf |
| GRIS | GCCS Reconnaissance Information System |
| GSORTS | GCCS Status of Resources & Training System |
| GSPR | GCCS Software Problem Report |
| GTN | Global Transportation Network |
| GUI | Graphical User Interface |
| | |
| HMI | Human Machine Interface |
| HP | Hewlett-Packard |
| HTML | HyperText Markup Language |
| HTTPD | HyperText Transfer Protocol Daemon |
| | |
| IFD | Integrated Feasibility Demonstration |
| IMRAS | Individual Manpower Requirements and Availability System |
| IMS | Information Management Subsystem |
| IMS/RFM | Information Management Subsystem/Reference File Manager |
| IP | Internet Protocol |
| IPA | Imagery Product Archive |
| IRC | Internet Relay Chat |

| | |
|---|---|
| IRM | Information Resource Manager |
| | |
| JCS | Joint Chiefs of Staff |
| JDC | Joint Deployment Community |
| JDISS | Joint Deployable Intelligence Support System |
| JEPES | Joint Engineer Planning and Execution System |
| JFAST | Joint Flow and Analysis System for Transportation |
| JIC | Joint Intelligence Center |
| JMCIS | Joint Maritime Command Information System |
| JNAV | JOPES Navigation |
| JOPES | Joint Operations Planning and Execution System |
| JPEC | Joint Planning and Execution Community |
| JRS | Joint Reporting Structure |
| JS | Joint Staff |
| JSPS | Joint Strategic Planning System |
| JTF | Joint Task Force |
| | |
| LAN | Local Area Network |
| LGTO | Legato |
| LFF | Logistics Factors File |
| LOGSAFE | Logistics Sustainment Analysis and Feasibility Estimator |
| LSA | Logistics Sustainability Analysis |
| LVIS | Linked Virtual Information System |
| | |
| MAIL | APPLIXware Mail |
| MB | Mega Bytes |
| MEPES | Medical Planning and Execution System |
| MIB | Management Information Base |
| MM | Message Manager |
| MOE | Map Overlay Editor |
| MONITOR | System Monitor |
| MPM | Medical Planning Module |
| MSC | Military Sealift Command |
| MSVCS | Mail Service |
| MTF EDIT | Message Text Format Editor |
| MTMC | Military Traffic Management Command |
| | |
| NETEX | Network Executive |
| NETM | Netmetrix |
| NFS | Network File Server |
| NIS | Network Information Service |
| NMS | Network Management Stations |
| NPG | Non-Unit Personnel Generator |
| NRF | Naval Reserve Force |

| | |
|---|---|
| NURC | Non-Unit-Related Cargo |
| NEWSMKGRP | NewsMaker Group |
| OPLAN | Operation Plan |
| PACOM | Pacific Command |
| PC | Personal Computer |
| PDR | Pre-Defined Reports |
| PHONE | Telephone List |
| PI | Planning Initiative |
| PLOG | Position Log |
| POSF | Ports of Support File |
| PPP | Point-to-Point Protocol |
| PROFILES | Profiles Function |
| RDA | Requirements Development and Analysis |
| RDBMS | Relational Database Management System |
| RDP | Rapid Deployment Planning |
| RFADB | Reference File Administration Data Base |
| RFM | Reference File Manager |
| RFA | Reference File Administration |
| RIPS | Reconnaissance Information Processing System |
| RREM | Run Remote |
| RTSS | Reserve Training Support System |
| RUDRS | Reserve Unit Data Resource System |
| S&M | Scheduling and Movement |
| SECURITY | Security Manager |
| SIPRNET | Secret Internet Protocol Router Network |
| SIQS | SORTS Interactive Query System |
| SNMP | Simple Network Management Protocol |
| SORTS | Status of Resources & Training System |
| SQL | Structured Query Language |
| SRB | Software Release Bulletin |
| SRO | Sensitive Reconnaissance Operations |
| TARGET /DCP | Theater Analysis and Replanning Graphical Execution Toolkit/Distributed Collaborative Planning |
| TCC | Transportation Component Command |
| TCCESI | Transportation Component Command External System Interface |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TEDIT | Template Editor |
| TPFDD | Time-Phased Force Deployment Data |
| TIP | Technology Insertion Program |

| | |
|---|---|
| TUCHA | Type Unit Characteristics File |
| UB | Unified Build |
| USMTF | United States Message Text Format |
| USTRANSCOM | United States Tranportation Command |
| VDD | Version Description Document |
| WAN | Wide Area Network |
| WinDD | Windows Distributed Desktop |
| WIS | WWMCCS Information System |
| WWMCCS | Worldwide Military Command and Control System |
| WWS | WIS Workstation |
| XTERM | X-Terminal |
| XTP | External Transaction Processor |
| XRN | NewsGroups-X-Windows Read News |

## Definitions

*C2 Core Data Model:* Data model based on integration of all data models from across the five C2 Functional Activities.

*C2 Data Architecture:* Identifies the data common or shared across Joint Task and C2 Functional Activities, per DOD 8320.1-M-X.

*C2 Enterprise Framework:* Consists of four elements: C2 Enterprise Model, the C2 Process Framework, and C2 Interoperability Framework, and Echelons of Command.

*C2 Enterprise Model:* Identifies the universal processes of exercising Command and Control across all echelons of command (Strategic, Operational, and Tactical). The model was developed from the viewpoint of a Commander, excluding activities outside "Exercise Command and Control" context. The processes with "Exercise Command and Control" are: 1) Force Development, 2) Intelligence, 3) Sustainment, 4) Mobility and Survivability/Protection, and 5) Employ Forces/Firepower.

*C2 Process Framework:* Reflects the achievements of individual Functional Process Improvement projects towards data interoperability. It maps the activities within a Functional Area and across echelons of command in terms of Functional Management Process as defined in DOD 8020.1-M Change 1 (e.g. program implementation steps: define, analyze, evaluate, plan, approve, execute).

*C2 Interoperability Framework:* Identifies qualitative relationships of Programs within C2 Functional Activities and across echelons of command, in terms of interoperability. The factors that hinder interoperability are: incompatible hardware and software platforms (e.g. an IBM mainframe with a COBOL application that needs to communicate with an Oracle database on a Unix-based SUN platform), incompatible data formats (e.g. employee numbers in one system allows for alpha and numeric characters, while it is limited to only numeric on another system), and incompatible applications (e.g. the remote system collects data by project whereas the local system collects data by month).

*C2 Functional Areas:* There are five C2 Functional Areas: 1) Force Development, 2) Intelligence, 3) Sustainment, 4) Mobility & Survivability, and 5) Employ Forces/Firepower. These are the activities performed by a Commander at Strategic, Operational, or Tactical levels.

*echelons of command:* The three level of command are Strategic, Operational, and Tactical. Strategic covers National Military Command functions (monitor and assess situation, determine mission, coordinate with Congress, issue warning/execute order, select course of action, and monitor deployment) and Theater (CINC) functions (conduct detailed planning, develop COA, posture forces, issues OpOrds, monitor and coordinate deployment, update force status and SitRep for NCA). Operational covers the Joint Task Force functions (plan component support, disseminate orders, coordinate across components, apply forces and resources, and report mission status). And Tactical covers the Component functions (plan utilization and sustainment, disseminate orders, and coordinate/move forces).

*employ forces/firepower:* The activities involved in the application of military forces (unified, joint, service, and combined) in a way designed to accomplish objectives and strategy (to include but not limited to: disaster relief, control of civil disturbances, drug enforcement, combating terrorism, and integrated fire). Firepower is employed through the use of collective systems and coordinated use of target acquisition data, direct and indirect fire weapons, armed aircraft of all types, and other lethal and non-lethal means against ground targets in support of maneuver force operations. This task includes artillery, mortar, and other non-line-of-sight fires, naval gun fire, close air support, and electronic countermeasures and deception. It includes strike, air defense, anti-air/surface/sub-surface defense and naval surface support, counter air, and air interdiction fires. Fire includes all types of ordnance.

*force development:* The translation of projected military department and service resources-manpower, fiscal, and material into time-phased programs, and structure necessary to accomplish alliance, national security, national military, and theater strategy and service assigned missions and functions. Some activities performed include planning, training, wargaming, R&D, sizing forces, and developing force structure.

*intelligence:* The intelligence which is required for the planning, development, and conduct of strategy and campaigns and operations within an Area of Responsibility (AOR). Intelligence and related systems concentrate on the collection of information and the analysis of that information (to include meteorology, topography/mapping, charting, and geodesy), which will lead to the identification and location of high-payoff targets or centers of gravity that if successfully attacked, will achieve the assigned aims and objectives.

*Joint Personnel Asset Visibility:* Provides the ability to identify, locate and track US Forces by unit and/or individual tasked to support mission requirements identified in a plan/TPFDD or deployment order. Entering into, in and redeploying out of the JTF AOR. US Forces include active,

reserve, military units/personnel; DoD Civilian, contractor personnel, other US non-DoD government personnel, non-US Forces tasked to support the JTF staff or AOR and NEO personnel within the JTF AOR.

*Joint Total Asset Visibility:* DoD's JTAV program provides CINCs, JTF Commanders and service and agency personnel with access to a wide range of logistics data. JTAV provides timely and accurate information on the location, movement, status and identity of units, personnel, equipment and supplies across all DoD components. JTAV will also provide users with the capability to act on this information through access to decision support tools designed to improve the overall performance of DoD's logistics practices.

*mobility & survivability/protection:* The capability of the force that permits freedom of movement relative to the enemy while retaining the ability to fulfill its primary mission. This function also includes those measures the force takes to remain viable and functional by conserving the fighting potential of a force so that it can be applied at the decisive time and place. This activity includes such actions taken to counter the enemy's firepower and maneuver by making soldiers, systems, and formations difficult to locate, strike, and destroy. Survivability and protection includes protecting joint and combined air, space, land, and sea forces; bases; and LOCs from enemy maneuver and attack, natural occurrences, and terrorist attack. This task also pertains to survivability and protection of forces, systems, and civil infrastructure of friendly nations and groups in operations other than war.

*operational utility rating:* The rating level assigned by the C2 functional community which establishes the relative value of a requirement for fielding. High values will tend to cause a release be held until that requirement is met. Low values will tend to allow the release to proceed in order to get the rest of the capabilities to be fielded quickly. Used to manage "requirements creep," and realistically manage user expectations.

*release date:* date that segments (software and documentation) are determined to be ready for fielding and is available on proper distribution media.

*release notification:* date segments are determined to be ready for fielding (software and documentation may not be available yet on proper distribution media)

*sustainment:* The activities carried out in order to maintain the necessary level and duration of military activity to achieve objectives. This operating function is the activity of providing, maintaining, and transporting (transportation includes movement of the sick and wounded) those levels of force, material, and consumables necessary to support the military strategy and promotes relations across the continuum of U.S.

agencies and friendly nations military operations. In operations other than war, supporting and enabling tasks to this joint task pertain to support of U.S. forces and agencies and the advisory and training assistance to a host nation regarding those activities (i.e. humanitarian assistance).