CDRL D-002 Rec'd 9 AUG 1983

SAFE Project Plan
Contract No. 83B-805200-000
29 JULY 1983

CONCURRED BY _____
Harry E. Fitzwater
Deputy Director for
Administration

CONCURRED BY _____
[redacted] 25X1
Assistant Director for
Resources and Systems

CONCURRED BY _____
[redacted]
Director of Data
Processing

CONCURRED BY _____
[redacted] 25X1
Dep. Asst. Dir. for
DIA Systems

APPROVED BY _____
[redacted]
SAFE Project Director

APPROVED BY _____
[redacted] 25X1
Deputy SAFE Project
Director

Prepared By:

GEODYNAMICS CORPORATION

6551 Loisdale Ct., Springfield, Va. 22150 Suite 800

APPROVED BY _____
[redacted] 25X1
Geodynamics Corporation
QA Contractor

RCA Government Communications Systems

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

FIGURES

TABLES

GLOSSARY OF ACRONYMS AND TERMS

ADP - Automated Data Processing

AFB - Automatic File Build

AIF - Automated Intelligence File

AIM - Automatic Information Management

AIS - Defense Intelligence School

AISF - Analyst Intelligence Support functions are logical subsets of functions that pertain to the dissemination of incoming (or internally composed) intelligence messages and documents, and to the creation, storage, retrieval and exchange of documentary intelligence.

ASG - Analytic Support Group

AT - Acceptance Test

bpi Bits Per Inch

CCB - Configuration Control Board

CDR - Critical Design Review

CIA - Central Intelligence Agency

CM - Configuration Management

CMS - Conversational Monitor System (operator-command language interface)

COINS - Community On-Line Information Network System

COTR - Contracting Officer's Technical Representative

CPC - Computer Program Component

CPCI - Computer Program Configuration Item

CRD - Central Reference Division

CSD - Communication Security Division

CSG - Customer Support Group

CSPO - Consolidated SAFE Project Office

CSRD - Consolidated SAFE Requirements Document

CSS - Customer Service Staff

CTC - Channel-to-Channel

DA - Directorate of Administration

DAP - Dissemination Analysis Process

DASD - Direct Access Storage Device

DATEX - Data Exchange

DBMS - Data Base Management System

DCI - Director of Central Intelligence

DI - Directorate of Intelligence

DIA - Defense Intelligence Agency

DIAC - Defense Intelligence Analysis Center

DIAOLS - DIA On-Line System

DIOBS - DIA Order of Battle System

DND - Domestic Networks Division

DoD - Department of Defense

DoDIIS - DoDIIS is an integrated intelligence information handling system supporting the Unified and Specified commands, the Services and other members of the military intelligence

community. Military intelligence organizations at all levels of the comand structure provide information specific to the needs of their parent organization. DoDIIS is the collection of data processing systems developed and managed by these organizations plus the interconnecting telecommunications network.

DSSCS - Defense Special Security Communications System is responsible for handling all codeword message traffic between the SAFE system and AUTODIN subscribers. All communications functions necessary to interface with AUTODIN will be performed by DSSCS.

EC - Early Capability

ED - Engineering Division

ELINT - Electronics Intelligence

EMI - External Message Interface

FQT - Formal Qualification Test

GDIP - General Defense Intelligence Program

HASP - Houston Automatic Spooling Program

HUMINT - Human Intelligence

IC - Intelligence Community

ICD - Interface Control Document

ICDC - ICD Coordinator

IDF - Intelligence Data Files (Four DIA-unique file types)

INQUIRE - Indexed File DBMS

JCS - Joint Chiefs of Staff

JES - Job Entry Support Subsystem

M204 - Model 204 (Structured File) DBMS

MAP - Message Analysis Processing

MIS - Management Information System

MVS - Multiple Virtual Storage (operating system)

NFE - Network Front End

OC - Office of Communication

OCR - Office of Central Reference

OD - Operations Division

ODP - Office of Data Processing

OE - Operational Evaluation

OS - Office of Security

OSS - Operational Support Segment

OT&E - Office of Training and Education

PCTCS - Pentagon Consolidated Telecommunications Center System is responsible for handling all GENSER message traffic between the SAFE system and DoD network subscribers. All communications functions necessary to interface with DoD networks will be performed by PCTCS.

PDR - Preliminary Design Review

PERT - Project Evaluation and Review Technique

PMO - Pilot Mail Operation

PQT - Preliminary Qualification Test

QA - Quality Assurance

QAS - Quality Assurance Segment

RCM - Deputy Assistant Director for Communications

RSD - Deputy Assistant Director for Defense Intelligence Systems (DoDIIS)

RSE - Executive Director for DoDIIS Engineering

RSM - Executive Director for DoDIIS Management

RSO - Executive Director for DIA Systems

SAFE - Support for the Analysts File Environment

SDR - System Design Review

SDS - System Development Segment

SEC - SAFE Early Capability

SEG - Systems Engineering Group (within SDS)

SETA - Systems Engineering Technical Assistance

SMF - Support Management Facility

SOW - Statement of Work

SPD - System Programming Division

SS - System Services

SUIM - SAFE User Interface Manual

SURE - SAFE User Representative Element

TEMPEST - Electromagnetic isolation and sanitization security measures.

Transaction Files - Transaction files logically store updates (adds, changes, deletes) to the Central Index and Branch/Private Index Files.

UDB - User Data Base

UIRS - User Interface Requirements Specification

VM - Virtual Memory (operating system)

VP - Director of Foreign Intelligence

V&V - Validation and Verification

WBS - Work Breakdown Structure

SECTION 1

INTRODUCTION

1.1 Purpose

The purpose of the SAFE Project Plan is to define the SAFE system in terms of what is to be accomplished, who will perform the detailed tasks, how all SAFE activities will be managed, and when major events are scheduled for completion.

1.2 Scope

The SAFE Project Plan applies to all SAFE project participants and governs the technical development, project management, testing and implementation of the incremental deliveries, and training of user and maintenance personnel. The Plan defines roles, responsibilities, and interrelationships for all organizational entities including a description of project monitoring methods and controls which will be used to manage and evaluate the progress of SAFE. The plan further describes the first five incremental deliveries from two points of view. First, the plan summarizes capabilities in each incremental delivery from a high level perspective; secondly, the plan defines the development strategy for each delivery.

1.3 Description

The SAFE Project Plan is organized into five main sections and one appendix. The first section provides an introduction to the Project Plan by defining the purpose, scope and format of the document, to include a listing of related SAFE documentation.

Section Two presents the SAFE system objective from a functional requirements viewpoint, and describes the technical approach to project development.

Section Three contains a detailed description of the Consolidated SAFE Project Office (CSPO), user organizations, contributing contractors, and other organizations involved in the SAFE Project. This section also describes management responsibilities, control mechanisms and the interrelationships between organizations.

Section Four provides an overview of the SAFE system by describing the system and functional capabilities included in each of the incremental deliveries.

Section Five describes the methods for identifying and managing potential risk areas. Risk is divided into two broad categories: programmatic risk and technical risk. The discussion of each of the two risk categories includes a definition of the category and an identification of associated risk.

Appendix A addresses the project scheduling and monitoring for project control. Gantt charts are used to show activity milestones and time-lines. The framework for planning, scheduling, and reviewing project events is facilitated through use of a project management tool, PAC II, which provides a critical path analysis. The critical path analysis will reveal schedule sensitivities and will thus assist CSPO in optimizing project resources.

1.4 Assumptions and Restrictions

This plan is produced by the CSPO Quality Assurance Segment and is promulgated by the Director and Deputy Director of the CSPO. Strict adherence to the plan is required by all participants. Modifications to the plan must be approved by the Director or Deputy Director of CSPO.

1.5 Reference Documents

The following documents have been approved and placed under project configuration control. These documents should be referred to for additional detail regarding specific subjects.

SF-U-CA-G-003B	Quality Assurance Plan
SF-U-CA-G-001A	Configuration Management Plan
SF-U-CA-G-002A	Documentation Plan
SF-U-CE-001B-01	System Requirements Specification

SF-U-CE-7200E-01	User Interface Requirements Specification
SF-U-NE-0070-01	Requirements Traceability Matrix
SF-U-NE-0085-01	System Design Document
SF-U-NE-0089-01	Interface Control Document
SAF-D005A/79	Consolidated SAFE Requirements Document
SF-S-DE-0011-01	Conversion Requirements Specification (Vol. 1)
SF-S-DE-0011-02	Conversion Requirements Specification (Vol. 2)
SF-U-NE-0086-01	Hardware Configuration Document
SF-U-NE-0088-01	SAFE Project Conversion Plan
ECA-01	Early Capability Project Plan
ECD02	SAFE-C Project Early Capability Interface Specification to External Systems
ECD03	SAFE-D Project Early Capability Interface Specification to External Systems
ECD05	Early Capability Software Definition Document
ECD10	SAFE-C Communication Plan
ECD11	SAFE-D Communication Plan
ECL03	Early Capability Software Maintenance Plan

SECTION 2

PROJECT DEVELOPMENT

2.1 System Objective

The purpose of SAFE is to provide the needed data processing support to assist the intelligence analyst in coping with the myriad of sources and large quantities of data available on given subjects. Emphasis over the past few years has been given to providing more coverage, increased capacity and greater sophistication to our information collection capability. We have been so successful that in many instances the intelligence analyst has been overwhelmed with information. SAFE will assist the analyst in the time-consuming tasks of collecting, organizing, collating, editing and coordinating data.

To significantly improve the flow of intelligence, SAFE will provide automatic processing and dissemination of incoming electrical messages. Users of SAFE will develop lists of words or phrases called profiles which will be used to direct relevant traffic to the individual or office. These user profiles may also be structured to alert the analysts when specific intelligence data of topical sensitivity is received by their respective agency (CIA/DIA).

In addition to accelerating the dissemination of electrical messages, SAFE will provide the capability for a user to read, annotate, route (to other analysts or offices) and index intelligence electronic documents. SAFE will facilitate analysts' electronic communications with one another.

Individually created electronic work files will be provided. Work files can be defined and structured by the user to meet individual data storage and retrieval requirements. The user also can define output formats so that data presentation at the workstation focuses attention on relevant information.

By providing rapid communication between the managers of collection resources and the intelligence analysts, SAFE will provide, for DIA, the opportunity for more effective exploitation of collection resources.

Another major improvement to the analysts' environment provided by SAFE will be the provision of a single access language to support the current intelligence function as well as historical research of reference data. On-line access to reference data will allow the SAFE user to research not only the indexed files, structured records, order of battle files or installation files, but also to research abstracts of documents, and full texts of electrical messages, all through a single user language. The SAFE User Language (SUL) will provide rapid and effective query and file maintenance across diverse data bases.

The SAFE user interface is being developed based on a model of the intelligence analysts' work environment. The SAFE User Language will allow the user to perform background and foreground functions simultaneously, thus improving analytical efficiency by allowing greater attention to be paid to foreground analysis functions and less attention to background support tasks.

Many existing DIA data bases contain data duplication, and lack data standardization and data integrity. One of the objectives of SAFE is to integrate intelligence data bases where feasible in an effort to optimize on-line data base maintenance and retrieval while at the same time reducing data redundancy and the risk of data inconsistency.

Finally, SAFE will significantly improve the mechanism for producing finished intelligence. For both agencies, the user will have the capability to compose and print finished intelligence reports. The provision for on-line text composition will allow the user to write memoranda, articles, or reports, and then print the textual or structured data in a variety of output formats. The ability to route intelligence documents electronically to other analysts or supervisors will greatly facilitate the coordination process and will thus serve to compress the production cycle. In addition, the intelligence agencies will more effectively respond to ad-hoc requests for information through the more efficient on-line research, composition, and dissemination capabilities available in SAFE.

In summary, SAFE provides a needed set of processing tools to assist the analyst/manager in producing finished intelligence for national level policy makers.

2.2 Technical Approach

The fundamental precepts governing SAFE development are: maximum use of commercial and government available off-the-shelf software packages to satisfy SAFE requirements and incremental delivery of functional capabilities to the users. SAFE will be built utilizing government furnished IBM compatible hardware for the optimal use of applicable commercial and government software. The technical approach is predicated on SAFE's requirements bearing strong resemblance to commercial products in the areas of data base systems, electronic mail and text processing.

SAFE's requirements cannot be fulfilled soley by these sources, therefore software augmentations will be necessary to satisfy the total set of SAFE requirements. Augmentations to software packages will be made only after careful analysis of cost, schedule and technical risk, and the priority of the requirements which drive the software augmentations. Trade-offs will be developed in consultation with user-representatives (DIA-SAFE Users Group; Analytical Support Group/DI) as part of the decision process.

2.3 Development Approach

The following represents specific integration concepts/tasks necessary to support the SAFE system development approach:

- The incremental delivery of capabilities to the users involves the identification of software packages that provide some portion of the SAFE functions. A software package may require augmentation to achieve the desired functional capability. In turn, a set of packages may require integration to achieve some composite set of capabilities for each of the respective incremental deliveries. The development of each incremental delivery will be monitored by CSPO's System Development and Quality Assurance Segments for adherence to the project standards and responsiveness to requirements. Each delivery will be baselined upon acceptance and then turned over to the Operational Support Segment.

  The commercial market is expected to be active in solving many SAFE-like problems through improved performance of hardware and software; or through software with increased capabilities. The incremental development approach allows continuous monitoring of improved products and services.

Activities generally defined as system integration encompass the melding and testing on several levels of various pieces of software that make up a system. These activities range from the interweaving of small pieces of software into modules followed by the aggregation of modules into applications and finally the orchestration of the applications into a system. System Integration will assure that the incremental deliverables are introduced into the operational environment with maximum coordination and minimal disruption.

- In the SAFE Management Approach, the System Development Segment, with assistance from an integration support contractor, will be responsible for system integration.

- The development phases for integrating capabilities into the SAFE environment are shown in Figure 2-1. The diagram shows a classical software system development including the major design review milestones and delivery dates in a timeline-oriented chart.

2.4 System Hardware

The hardware supporting SAFE is expected to evolve and keep pace with expanding capabilities. The intent is to take full advantage of advances in technology where appropriate and feasible. As the SAFE user community expands, the system hardware will be upgraded. The initial SAFE system

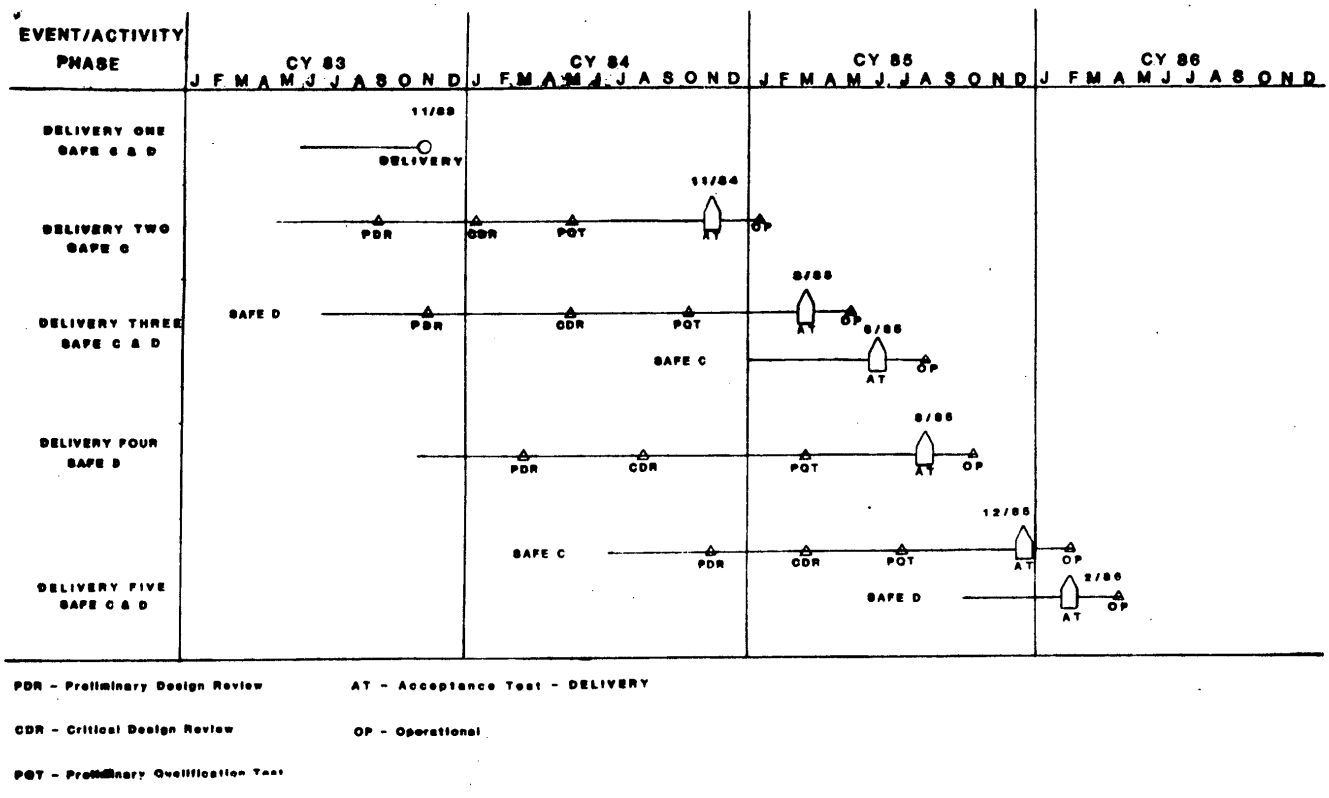

Figure 2-1 SAFE DEVELOPMENT SCHEDULE

hardware configuration, as described in the SAFE Hardware Configuration Document, is viewed as three separate systems: CIA (SAFE-C), DIA (SAFE-D) and this Development System. Figure 2-2 consists of the three views of this SAFE hardware configuration concept. Note that the Development System is a back-up, virtual memory system to the SAFE-D system. The hardware configuration document identifies the projected configuration for each delivery subsequent to the SAFE Early Capability.

a) SAFE-C SYSTEM

The initial hardware configuration for the SAFE-C system consists of three IBM 3083 model J processors. All three processors are used for production with two operating under control of the MVS operating system and one operating under the control of the VM operating system. One of the MVS processors also serves as the back-up VM machine. An IBM 3211 printer is switchable to any of the processors. The processors share access to a pool of eight IBM 3420 tape drives (6250/1600 BPI) through four IBM 3803 controllers. All remote communications facilities are provided through three COMTEN 3690 front-end processors, each with dedicated interfaces to each of the 3083 processors. The SAFE-C processors share the access to thirteen IBM 3380 direct access storage systems with a total of 32.5 gigabytes, sixteen IBM 3350 Direct Access Storage Devices (DASD) with a total of 9.6 gigabytes, and two STC 4305 solid state drum systems, each with 45 megabytes.

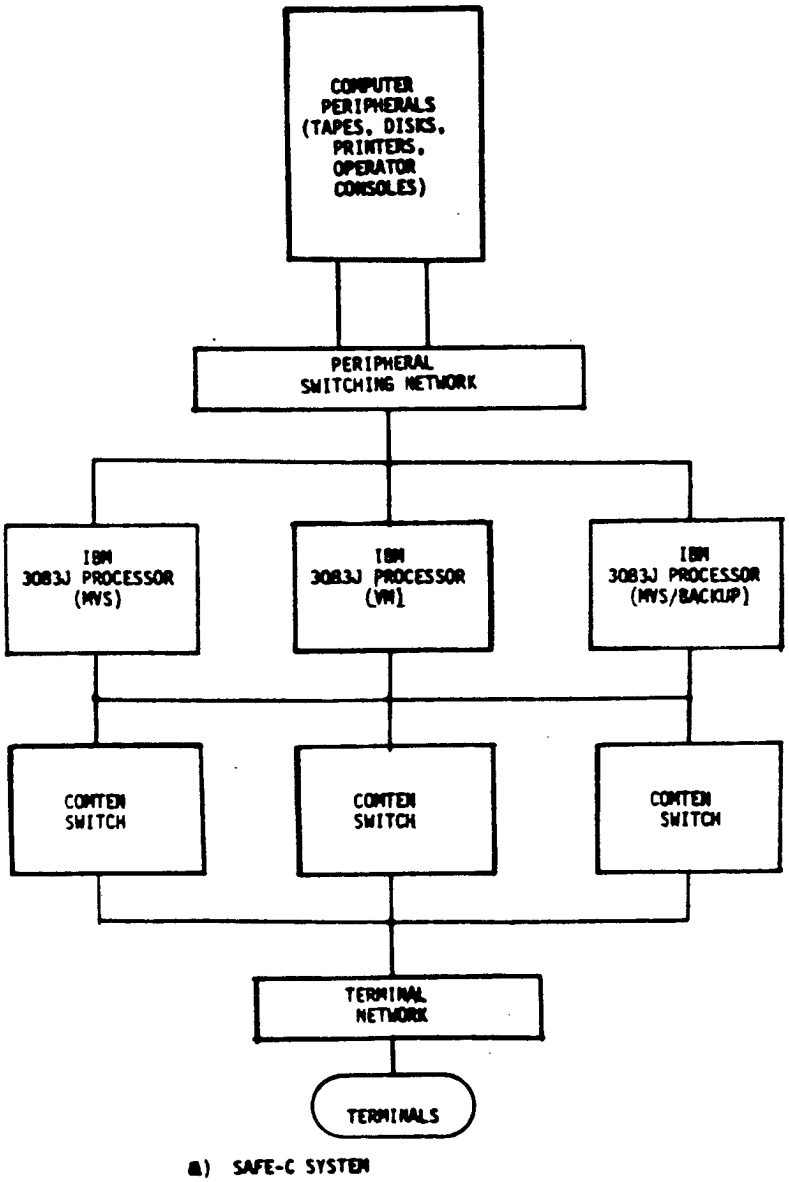

Figure 2-2 SAFE HARDWARE CONFIGURATION

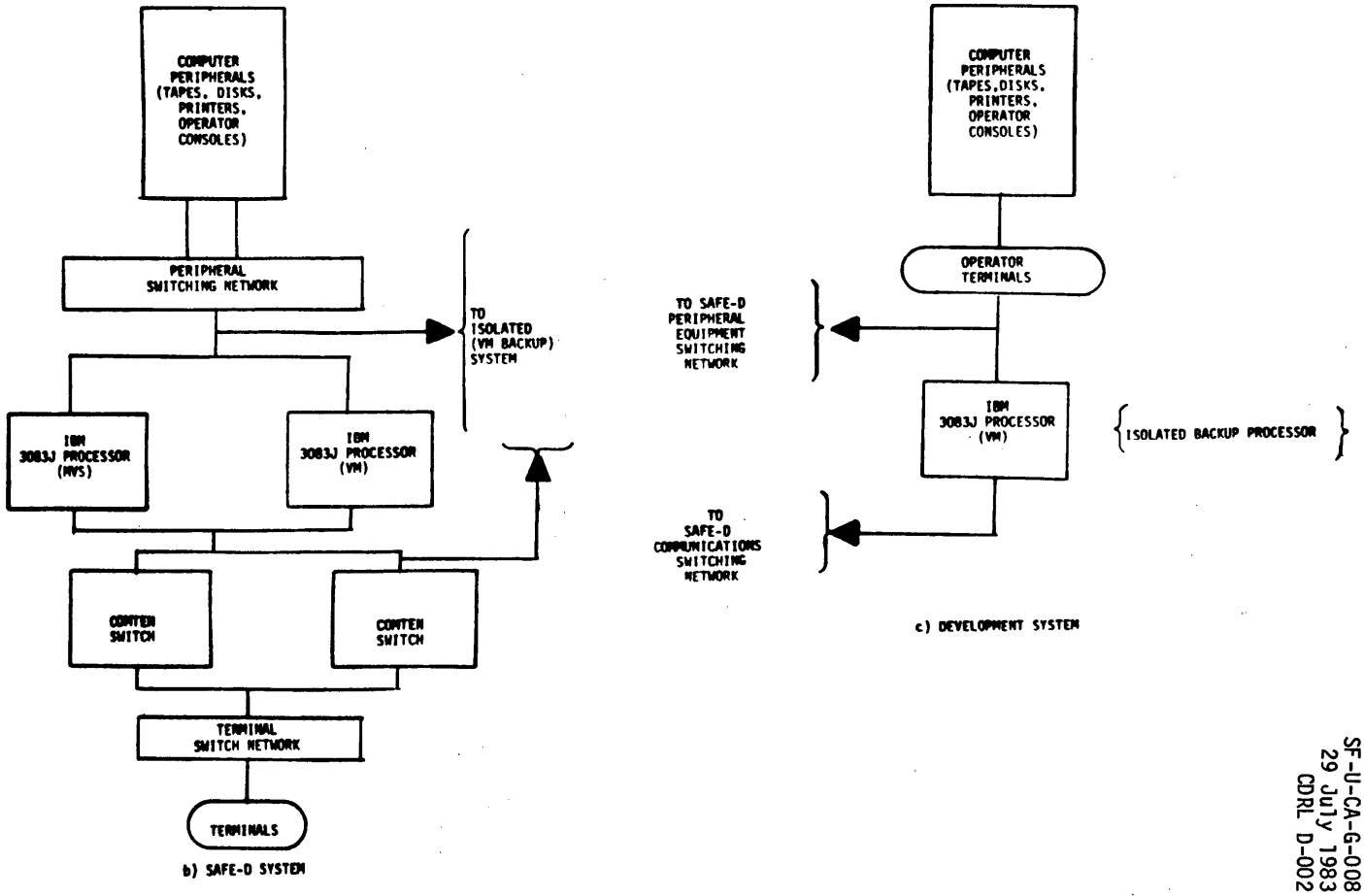

Figure 2-2 SAFE HARDWARE CONFIGURATION

b) SAFE-D SYSTEM

The SAFE-D system initial hardware configuration consists of two IBM 3083 model J processors. Both processors are used for production with one operating under control of the MVS operating system and one operating under the control of the VM operating system. An IBM 3211 printer is switchable with either processor, and a pool of eight IBM 3420 tape drives (6250/1600 BPI) are accessible through two controllers. Nine IBM 3380 storage systems with a total of 22.5 gigabytes, six IBM 3350 DASD with a total of 3.6 gigabytes, and two STC 4305 solid state drum systems with a total of 90 megabytes are shared by the DIA processors. The remote communications facilities are provided through two COMTEN 3690 front-end processors.

c) DEVELOPMENT SYSTEM

An additional IBM 3803 model J processor initially serves both as a DIA back-up processor and as a software development system for both the CIA and DIA systems. This processor runs in MVS mode under control of the VM operating system. This processor has access to four IBM 3420-8 tape drives, seven IBM 3380 storage systems with a total storage capacity of 17.5 gigabytes, four IBM 3350 DASDs with a total of 2.4 gigabytes, and an STC 4305 solid state drum system with total storage capacity of 45 megabytes. The development system utilizes the DIA front-end processors for communication.

2.5 Software Development

A key factor in managing the integration capabilities into the SAFE environment is the identification and control of individual software elements comprising a delivery. Standard development and configuration management policy and procedures define the Computer Program Configuration Items (CPCIs) and the Computer Program Components (CPCs) as elements for configuration accounting and management:

- Within the SAFE structure, CPCIs are software packages identified by specific procurement or development specifications and are separately testable. The definition, procurement/development, integration and test of each CPCI will be controlled by individual task agreements.

- Once software is completely designed, the total structure is decomposed into smaller, modular units called Computer Program Components. The CPCs facilitate the isolation of problems and help to ensure that modifications and upgrades do not have unforeseen consequences throughout the system. Development of the CPCs can be easily tracked and responsibilities for development can be clearly defined. These units are the basic blocks for which code is developed and integrated to form the completed CPCIs.

- The set of CPCIs comprising an application will be integrated and tested within the current baseline configuration. At the completion of the integration tests, formal turnover demonstration will be performed. Successful execution of the demonstration and benchmarks will verify the full system operation including the added capabilities.

2.5.1 Application Software

Application software is written to solve specific problems, generate specified reports, and/or to update designated files. SAFE applications software includes all of the CPCI modules directly involved in supporting the mission of SAFE. Table 2-1 lists the set of CPCIs comprising SAFE application software which will reside within the MVS system, while Table 2-2 lists those modules which will reside within the VM system.

Table 2-1. MVS Application Software

MVS HOST PROCESS	CPCI
Message Input (EMI)	Message Analysis Process (MAP)
Message Analysis	Message Analysis Process (MAP)
Mail	Dissemination Analysis Process (DAP)
Profile Compilation	Dissemination Analysis Process (DAP)
Data Base Management	
o Index Files	INQUIRE
o Structured Files	M204
Special Output Control	Data Management

Table 2-2. VM Application Software

VM HOST PROCESS	CPCI
User Interface Process	Data Management Message Analysis Process (MAP)
User Data Process	User Data Base (UDB) INQUIRE
Network Communications Process	System Services Message Analysis Process (MAP)
Automatic Information Management	AIM Data Base
Service Process	System Services Management Information Systems (MIS)
DoDIIS Network Interface	DoDIIS Communication

2.5.2 Operating System Software

System software is concerned with the translation, loading, supervision, maintenance, control, and running of computers and computer programs. A distinction is usually made between operating system software and application software, although this distinction is not always obvious nor clearly defined. The operating system software supporting SAFE consists of components of the IBM Multiple Virtual Storage (MVS) and Virtual Memory (VM) systems assisted by the Job Entry System (JES), Management Information System (MIS), Support Management Facility (SMF), and a Tape Management System (TMS). Communications switching is handled by the NCR/COMTEN 3690 Communications Processor.

2.5.2.1 Multiple Virtual Storage (MVS)

MVS provides support for batch usage on a large virtual storage environment. MVS is a large-scale operating system, designed to handle multiprocessor configuration.

2.5.2.2 Virtual Machine/System Product (VM/SP)

VM/SP consists of the Control Program (CP) and Conversational Monitor System (CMS) components. Each user of VM/SP has the functional equivalent of a real, dedicated computing system. Virtual machines and virtual

storage are provided with each virtual machine referring only to its own virtual storage. This restriction protects each virtual machine's storage from the activities of other virtual machines. The size of each virtual storage space is defined in the virtual machine directory entry and may differ among virtual machines.

2.5.2.3 Management Information System/Support Management Facility (MIS/SMF)

The MIS/SMF provides timely information to the parent agencies for security audit and operational management.

2.5.2.4 Job Entry Subsystem (JES)

The Job Entry Subsystem acts as the scheduler for computer jobs, controlling the time and space resources within the system. All data destined for the system will be routed through the JES subsystem, which provides networking protocol for machine-to-machine communications.

2.5.2.5 Tape Management System

A UCC One automated Tape Management System protects data stored on magnetic tape and automates functions associated with controlling and managing the tape library in OS and OS/VS installations.

2.5.2.6 Communications Processor

NCR/COMTEN 3690 Communications Processors provide the network control for the on-line user community.

2.5.2.7 Houston Automatic Spooling Program/Channel-to-Channel(HASP/CTC)

The CIA currently supports the HASP protocol that communicates between the VM and MVS processors via Comten processors using a bisynchronous interface. This inter-machine communication facility will be replaced by an IBM 3088 C-T-C device. The 3088 device provides a larger number of subchannels for communication flexibility to handle all of SAFE's growth and a much higher data rate than currently provided by the Comten bisynchronous interface.

2.6 Integration and Test

For each SAFE delivery, two or more development contractors are tasked to design, code, unit test and debug specific subsets of the software required for the delivery. These subsets of software are then formally tested by the respective development contractors. Tests performed at this time are designed to satisfy CSPO that the contractors have implemented their design, satisfying all functional requirements included in

their respective tasking agreements. Integration and test of all software for each delivery is then performed to assure compatibility of its component parts and to assess the capability of the integrated software to meet desired performance requirements.

The formal test milestones and Operational Evaluation are described in the following subparagraphs.

2.6.1 Preliminary Qualification Test (PQT)

The PQT is a formal test performed by each development contractor for each SAFE incremental delivery.

Objectives of the PQT include:

- validation that the development contractor has implemented his design to meet the functional requirements included in his tasking agreement for each delivery

- demonstrating readiness of the software to be integrated with previously and/or concurrently delivered software.

Following successful completion of the PQT, software will be placed under control by Configuration Management (CM). Controlled copies of all software media will be available to the system integration support contractor only through the CM process. Test plans, procedures and reports will be utilized by CM personnel to conduct required configuration audits.

2.6.2 Formal Qualification Testing (FQT)

The FQT is a formal test conducted by the system integration support contractor after all delivery software has been integrated. The FQT plan will be developed as a part of the Integration Plan required for each SAFE delivery. The FQT procedure is also prepared by the system integration support contractor and will use test cases from the PQTs, modified as needed, to reflect the presence of working interfaces between the software component parts.

Objectives of the FQT include validation that CPCIs, as built, satisfy all of the functional requirements specified for the delivery and that deficiencies in interface compatability are identified and resolved. FQT will be performed using software media compiled and certified by the CM process. These software media will contain all approved changes implemented since the conclusion of PQT. Having passed the FQT, the integration and test phase shifts in orientation toward demonstrating that the heretofore delivered components perform under system-load conditions.

The Quality Assurance Segment assumes responsibility for testing, signifying the completion of the system test phase and the beginning of the acceptance test phase.

2.6.3 Acceptance Testing (AT)

The AT is a formal test conducted by QAS personnel following the system test phase. The AT Plan and procedures are prepared by the Chief, QAS. The detailed test cases will be similar to those developed for FQT with added stress testing intended to simulate the operational environment.

Objectives of the AT are to demonstrate the readiness of the integrated delivery software for operational use and to assess the capability of the software to meet desired performance requirements.

The AT will be performed using software media compiled and certified by the CM process. These software media will contain all approved changes implemented since the conclusion of PQT.

2.6.4 Operational Evaluation

Following the Acceptance Test is a 45-day period of system operational evaluation conducted by QAS personnel with support from the user community. The object of this evaluation is to demonstrate the capability of

the software to perform in the actual user environment. This can be both qualitative and quantitative.

2.7 Operations and Maintenance

Support of hardware and software for SAFE during the operational phase of each delivery requires careful planning. Procedures currently in effect for CIA computer operations must be reviewed by the Operations Division, Office of Data Processing (see 3.3.1.1.3) to ensure optimum compliance with SAFE operational requirements. An Operations and Maintenance Plan will reflect current, applicable CIA computer operations procedures and, as required, will detail procedures for DIA to effect an efficient change-over to the DIA operations.

2.8 Training

SAFE training will have to be accomplished for several components; the requirements for which differ significantly. Training will have to be provided for CIA, for DIA, and for DoDIIS users external to DIA. Training will also have to be provided for functional users, system operators, and maintenance personnel. The complexities and scope of the training required precludes reliance on traditional classroom instruction or on-the-job training. It is anticipated that SAFE training will include mobile training teams, self-paced text, classroom instruction, video tape presentations, computer aided instruction, and the SAFE system itself.

The Chief, QAS will produce a SAFE Training Plan identifying the specifics of training responsibilities; including types of courses, numbers of trainees, locations, and type of material required. The Chief, QAS will designate a SAFE training coordinator to work with all other project elements in defining and implementing the SAFE Training Plan.

SECTION 3

PROJECT MANAGEMENT

3.1 User Organizations

The Consolidated SAFE Project Office, under the auspices of the CIA's Deputy Director of Administration and the DIA's Assistant Director for Resources and Systems, is developing the SAFE System to support the analytical requirements of the intelligence analysts within the CIA, DIA and DoDIIS. The user organizations within the respective agencies are the CIA's Directorate of Intelligence and primarily the DIA's Directorate of Foreign Intelligence with DIA users also in the offices of the Assistant Vice Director for Collection Management, the Assistant Director for JCS Support, and the Assistant Director for Resources and Systems. This section delineates the responsibilities of these organizations.

3.1.1 CIA Directorate of Intelligence

The Directorate of Intelligence (DI) is the research, analysis, and production element of the CIA and supports the U.S. national security policy process by providing relevant and timely intelligence products.

3.1.1.1 Analytic Support Group/DI

The Analytic Support Group (ASG) of the Directorate of Intelligence will represent all DI users. As such, it will identify DI's SAFE requirements, obtain DI support for development and maintenance activities, and serve as the point-of-contact for DI user acceptance of each incremental delivery. ASG, in coordination with CSPO's Quality Assurance Segment, will review and approve all implementation planning that impacts DI users. This includes certification (via user testing) that the respective system deliveries and any future enhancements to the SAFE system are acceptable based on the criteria specified in the QAS-developed Acceptance Test Plan. Desired enhancements, resulting from user experience with the SAFE system, will be documented and prioritized by ASG and submitted to the SAFE Configuration Control Board as recommendations for incorporation into the SAFE system.

3.1.2. DIA-SAFE User Group

The DIA SAFE Users Group will represent all DIA and DoDIIS users and will be the point of contact for DIA user acceptance of each incremental delivery. In particular, in coordination with CSPO's Quality Assurance Segment, the DIA-SAFE Users Group will review and approve all implementation planning that impacts DIA and DoDIIS users. This includes certification (via user testing) that the respective system deliveries and any

future enhancements to the SAFE system are acceptable based on the criteria specified in the QAS-developed Acceptance Test Plan. Desired enhancements, resulting from user experience with the SAFE system, will be documented and prioritized by the DIA-SAFE Users Group and submitted to the SAFE Configuration Control Board as recommendations for incorporation into the SAFE system.

3.2 CSPO Organization and Responsibilities

The Consolidated SAFE Project Office is responsible for the development and delivery of the SAFE System in accordance with the CIA and DIA user requirements as defined and validated by each Agency in the Consolidated SAFE Requirements Document (CSRD). This effort encompasses not only common requirements, but also those unique to each agency. The effort is directed toward maximizing cost savings through common development, procurement and service for both Agencies.

CSPO is jointly staffed by CIA and DIA, is housed within CIA facilities, and is administratively supported by CIA. As shown in Figure 3-1, CSPO is organized with a Project Director, Deputy Project Director, Quality Assurance Segment, System Development Segment and Operations Support Segment. There is also a support staff and a contracting officer to handle administrative and formal contractual matters related to SAFE.

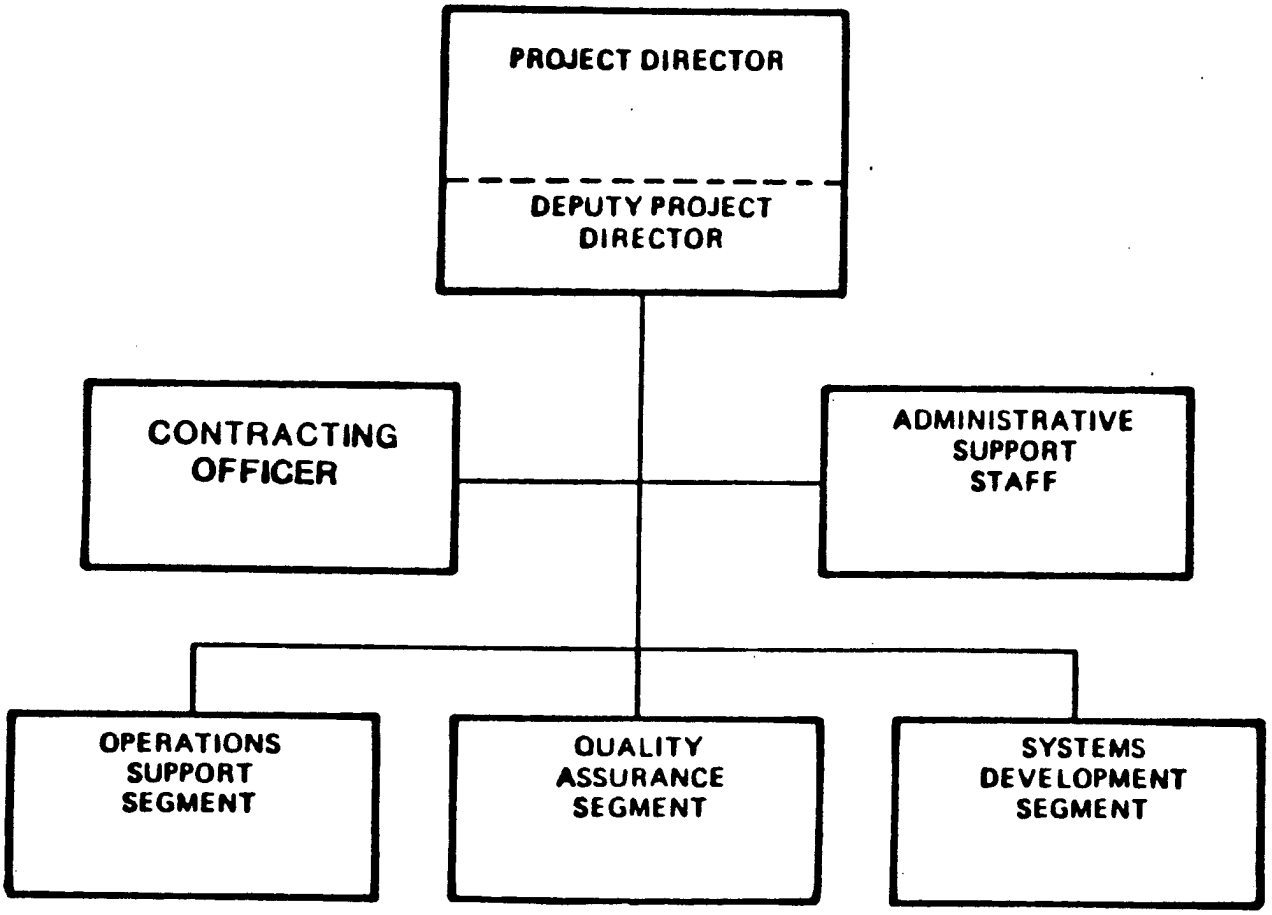

Figure 3-1. CSPO Organizational Structure

The Director and Deputy Director of CSPO have the authority and responsibility to manage all aspects of the SAFE Project. Development contractors from private industry and from other government organizations external to CSPO have been tasked to support this effort. Formal contractual agreements (memoranda of understanding for government organizations), backed by detailed statements of work for development contractors, will provide the basis for CSPO control over all development contractors.

In order to effectively manage contractual tasks, the Director of CSPO has assigned contracting officer technical representatives (COTRs) to each development contractor. Each COTR is responsible for closely monitoring and reporting the status of all tasks within his assigned area. To avoid misunderstandings and possible conflicts in day-to-day direction, the COTR will be the single point of contact for development contractors on all technical issues.

3.2.1 CSPO Project Director/Deputy Director

Management responsibility for the development of the SAFE System rests with the CSPO Project Director and the CSPO Deputy Project Director.

3.2.2 System Development Segment (SDS)

The Chief of the System Development Segment is responsible for managing the acquisition and integration of off-the-shelf software packages and the development of software to achieve required SAFE capabilities. In this capacity, Chief, SDS will oversee the execution of the development contractors' project tasks required to place in operation each of the system deliveries. A principal contractor will support the Chief, SDS in performing the necessary engineering for software integration, user interface design, testing, file conversion, software installation, appropriate engineering specifications and planning for the respective system deliveries.

The Chief, SDS is responsible for identifying and evaluating available software packages that meet SAFE requirements. Analyses will be performed to determine what augmentations are required to bring the package into compliance and when packages do not meet SAFE requirements. Users will participate in evaluating trade-offs when required augmentations are considered not feasible or when they impact cost and schedules.

The development of each delivery will be monitored by an SDS delivery manager to insure adherence to project standards and responsiveness to requirements. The delivery will subsequently be placed under configuration management and turned over to the Operational Support Segment.

3.2.3 Quality Assurance Segment (QAS)

The Chief of the QAS, with support from the QA Contractor, is responsible for administering the quality assurance program and will use contractual support for the various quality assurance functions, to include Configuration Management (CM), Validation and Verification (V&V), and System Engineering and Technical Assistance (SETA). The Chief of QAS is responsible for insuring that appropriate system design and software development standards are adhered to by SAFE Development Contractors. This segment will maintain all software and documentation baselines. Acceptance testing will be conducted to insure that the deliveries meet the requirements baseline. The QA Contractor is responsible for defining and executing acceptance test plans and procedures. The Chief of QAS will also maintain liaison with user organizations within both the CIA and the DIA. There will be a single point of contact within the CIA and DIA for user requirements. Areas of liaison will include training requirements, terminal allocation, user feedback from operational system usage, user language scenarios in support of interface prototyping, and the identification of new or changed functional requirements.

The Chief of QAS will be the executive secretary to the project's Configuration Control Board (CCB). The QA Contractor will provide support to the Chief of QAS in administering the SAFE Project's CCB and executing the SAFE Configuration Management Plan. The SAFE CCB will be chaired by the Director of the Consolidated SAFE Project Office. The Deputy Director of CSPO will be the Vice Chairman. The board will consist of the Chief and Deputy Chief of the SDS, the Chief of CIA's Analytic Support Group, the Chief of the DIA SAFE User Group, and the Quality Assurance Segment Chief, assisted by the Quality Assurance Contractor.

The QA Contractor, will prepare and maintain a master schedule, i.e., Program Evaluation and Review Technique (PERT) for all project activities. Progress against the master schedule will be reported to CSPO management at least monthly, or as requested by the Project Director (see Section 3.6).

3.2.4 Operational Support Segment (OSS)

The Chief of the OSS is responsible for operating and maintaining the hardware/software deliveries developed by SDS and accepted by QAS. The Chief, OSS will be the COTR for all SAFE operations and maintenance contracts. Operations and maintenance contracts will be written and executed by this segment. At the appropriate time (to be determined) responsibility for operating and maintaining SAFE-C and SAFE-D will be accepted by CIA (ODP) and DIA (RSO) respectively.

3.2.5 Support Staff

The Chief of the Support Staff is responsible for providing budget, financial program, and resource accounting support; and for producing an audit trail for the expenditure of funds to the respective agencies when requested. The Chief of the Support Staff is also responsible for maintaining a project library for document control, and for facility planning. In addition, the Chief of the Support Staff will provide appropriate reports (congressional, status, etc.) in support of the Project Director and Deputy Director. He will also be responsible for office administration and personnel and physical security.

3.2.6 Contracting Officer

The Contracting Officer is assigned to CSPO from the Procurement Division, Office of Logistics and serves as a member of the management staff. In this capacity, the Contracting Officer participates in the realignment of Development Contractors from subcontractor status to associate contractor status based on SAFE redirection. In addition, the Contracting Officer negotiates and administers resulting contracts.

3.3 CSPO Supporting Organizations and Responsibilities

The Director and Deputy Director of CSPO are responsible for coordinating matters relating to SAFE with appropriate organizations within the CIA and/or the DIA. Coordination will be through comments on appropriate documents, management reviews, technical reviews, participation in various standing and ad hoc committees and boards, and other appropriate vehicles to insure smooth transition of SAFE into the respective agencies.

When direct support, such as personnel resources of an organization within CIA or DIA is required, a contractual arrangement will be established with the organization external to the CSPO. The vehicle for this contractual arrangement will be a memorandum of understanding and/or project tasks, which will identify the kind of support, amount of resources and schedule for which the support is required.

Those organizations within CIA and DIA which will be affected appear in the following subparagraphs (list not all inclusive and will change as necessary).

3.3.1 CIA Organizations