Version 1.0a

Operations Concept
for the
Joint Service Imagery Processing System - Navy
(JSIPS-N)
Concentrator Architecture (JCA)

Prepared for:

Command and Control Systems Program (PMA281)

Program Executive Office Cruise Missiles and Joint Unmanned Aerial Vehicles

(PEO(CU))

Prepared by:

Lockheed Martin Corporation

Management and Data Systems

https://jca.external.lmco.com

September 1999

Table of Contents

1 Introduction

1.1 Purpose

The purpose of the Joint Service Imagery Processing System – Navy (JSIPS-N) Concentrator Architecture (JCA) is to provide a network based architecture to support the dissemination of Near Real Time (NRT) and archived imagery, imagery products and imagery support data to and from the Naval Fleet, Rapid Deployment Suites (RDS) and supporting shore locations.

The JCA is being delivered to the Navy Fleet by the Command and Control Systems Program (PMA281) Program Executive Office Cruise Missiles and Joint Unmanned Aerial Vehicles (PEO(CU)) as the follow-on to the National Input Segment (NIS) functionality of the JSIPS-N.

1.2 Scope

This document provides the User community with an understanding of the operation of the system in its entirety, and information supporting the operation of each associated sub-component. It presents a typical operational mission flow of the system data as it is to be used during normal operations. Finally, this document serves as the framework for the development, implementation, test, training, and ultimately, acceptance of the system.

This document contains a high level description of the functions of the system and the interaction of the hardware, software, and aspects of the Human Machine Interface (HMI). Additionally, it distinguishes between the operational capabilities of the JCA at Initial Operational Capability (IOC) and proposed capabilities for Full Operational Capability (FOC).

1.3 Document Organization

This document is organized into seven sections. Section 1, the introduction, addresses the purpose of the JCA, defines its deployment plan and migration from the NIS, and lists premises considered in the operation of the JCA. Section 2 lists applicable reference documents. Section 3 provides a description of the JCA and its components as well as the interfaces and/or supporting elements pertaining to the system. Section 4 provides a description of JCA system operations and defines the flow of data throughout the JCA. Section 5 provides a description of JCA Backup Concentrator (BUC) system operations and defines its composition. Section 6 provides a high level description of the logistics, operations, and maintenance functions within JCA. Section 7 is a list of acronyms used throughout this document.

1.4 JCA Deployment Plan

The scope of the JCA at IOC includes a single imagery source (Source), a single Navy controlled central data repository (Concentrator) to receive and disseminate imagery, three operational Navy sites (Sites) that will use the imagery received via the JCA, and the Communications architecture between each component. The JCA at IOC is depicted in figure 1.4-1.

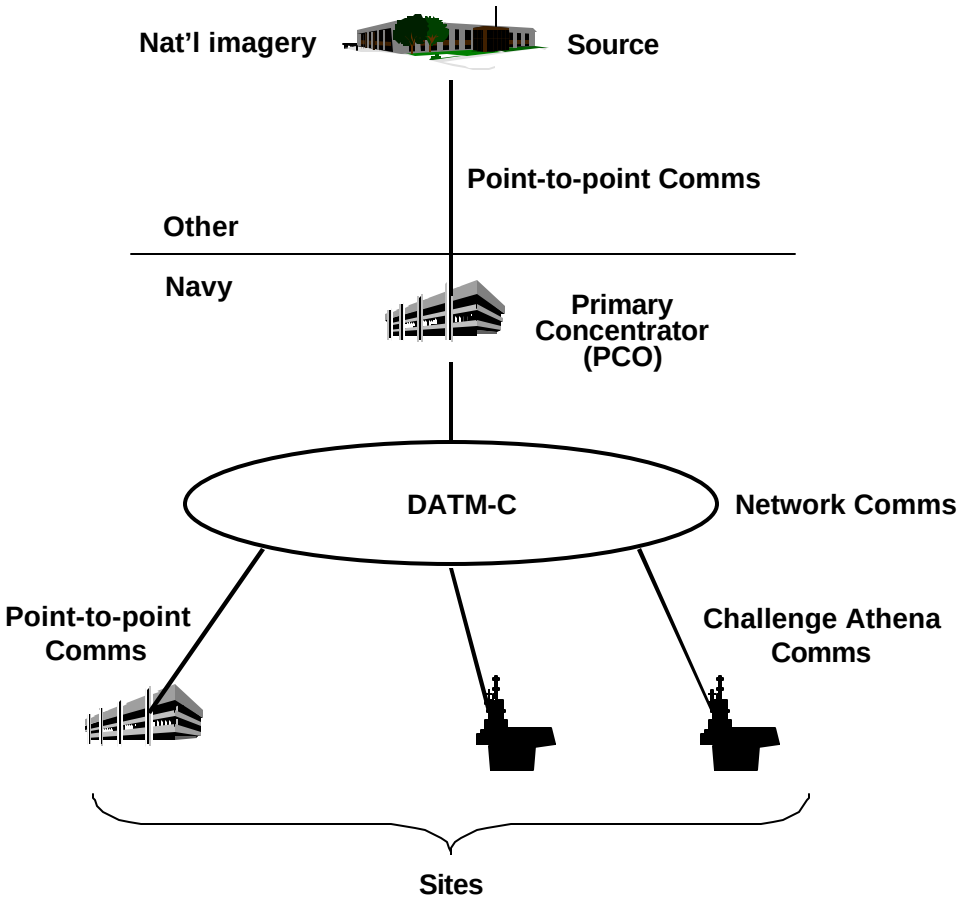

Figure 1.4-1 JCA at IOC

The Users of the JCA are comprised of Fleet, RDS and shore activities that rely on the use of imagery and imagery products to conduct their mission. These activities are referred to herein, and throughout all JCA documentation, as "Sites". The IOC of the JCA is currently planned for March 2000.

The transition between IOC and FOC will include the addition of new Sites, new Sources (if available) and a Backup Concentrator (BUC). During the transition period both JCA and the existing NIS architecture will be operational in the fleet.

After JCA IOC is declared, the current NIS architecture will be replaced with the JCA on a per ship basis as ships prepare to start their workups for a future deployment.

At FOC the JCA will support a maximum of 45 Sites with the architecture sized to provide near real-time dissemination to a maximum of 22 concurrent transmissions from those Sites. The JCA will have two Concentrators, a primary and backup, and the communications architecture to connect all Sites to the Concentrators. It is anticipated that this will be accomplished approximately 12-18 months after IOC. Additional Sources may also be available through the JCA as required by the Fleet.

The JCA architecture at FOC is depicted in figure 1.4 - 2.

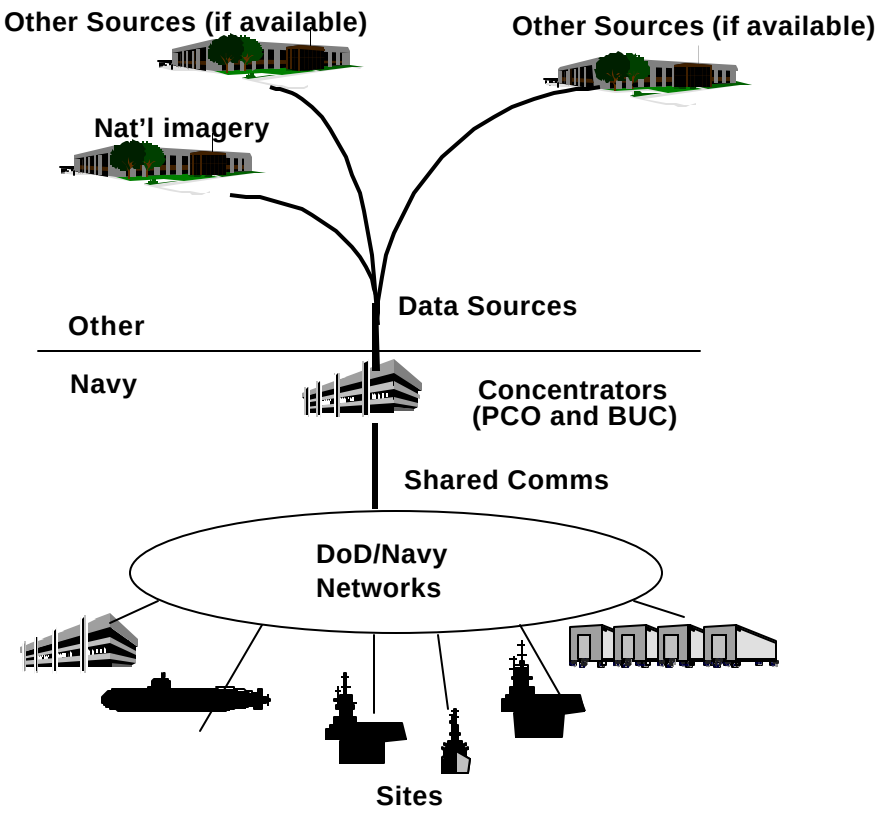

Figure 1.4-2 JCA projection at FOC

2 Applicable Documents

1) D3-Receive Segment-to-Host Database (D3-RSHD)

2) Defense Dissemination System, Enhanced Processing Segment to Receive Segment, Interface Control Document (IF20DO8P), 12 November, 1993

3) JSIPS-N Concentrator Architecture (JCA) Configuration Management Plan

4) JSIPS-N Concentrator Architecture (JCA) Critical Design Review, 19 February, 1998

5) JSIPS-N Concentrator Architecture (JCA) Test, Verification and Implementation Plan

6) JSIPS-N System Concept and Requirements for Imagery Related Intelligence Dissemination, 21 November, 1997

3 System Description

3.1 Background

The JSIPS-N NIS is currently deployed in the Fleet and provides the mechanism for the request and dissemination of NRT primary national imagery. In 1996, the JSIPS Block III initiative was introduced which established that JSIPS systems would be upgraded to be Common Imagery Ground/Surface System (CIGSS) and Year 2000 (Y2K) compliant. The JCA supports these requirements and is being delivered as the follow-on to the NIS.

The JCA offers an alternative approach for imagery dissemination than that of its predecessor, the NIS. The fundamental premise for this new architecture is the introduction of network based standard file transfer protocols that open the system to support more than the current NRT imagery requirement.

At IOC, the JCA will have at a minimum, the same capability as the NIS architecture. Further, the JCA has been designed as a United States Imagery and Geospatial Information System (USIGS) migration system. It will become a fully compliant USIGS system upon successful integration of the National Imagery and Mapping Agency (NIMA) Library (NL).

At FOC, the JCA will take advantage of the network based standard file transfer protocols to provide access to additional imagery and imagery support sources as they become available and are required by the Fleet.

3.2 Architecture Overview

3.2.1 Source

The Source component provides imagery and imagery-based strike support products to the Battle Force Commander. These products are essential to support exploitation, targeting, mission planning and rehearsal, amphibious assault and special operations.

The Source component for the JCA at IOC is the Enhanced Processing System (EPS). The EPS is currently the only source available to provide near real-time electronic dissemination of National imagery. The EPS disseminates imagery via a National image source interface (IF20D08P), at the Secret level. During the transition from IOC to FOC, additional Sources will be added as required to support fleet requirements for imagery support products that are able to be stored in compliance with the National Imagery Transmission Format (NITF)

standard. These sources may include commercial imagery, tactical imagery, the Digital Point Positioning Database (DPPDB), and other geospatial products.

3.2.2 Concentrator

The Concentrator component is the central receiving and storage area for imagery and imagery related data within the JCA. It is essentially a gateway between the Source and the Site components where data is stored, retrieved, and disseminated to the Sites. The Concentrator provides a centralized injection point for fleet imagery and products as well as a localized archive with a storage capacity of five years of national imagery. It is protected by a firewall to ensure the integrity of Fleet information and to prevent unauthorized access.

The primary function of the Concentrator is to provide information requests between the Site and the Sources via message traffic and to provide imagery and related data via File Transfer Protocol (FTP). The operation of the Concentrator will be as automated as possible, requiring little or no human intervention. The Primary Concentrator (PCO) is located at the Office of Naval Intelligence (ONI) in the National Maritime Intelligence Center (NMIC). The Backup Concentrator (BUC) is located at the Washington Navy Yard in the Washington Planning Center (WPC).

The sub-components of the Concentrator are the Dissemination Element (DE), the Imagery Exploitation Support System (IESS) server, the Concentrator Open Primary Server (COPS), the Firewall, and the Global Access Library (GAL). The Concentrator sub-components work together to support automatic dissemination of requested information from the Site and to support User-initiated data transfer from the Concentrator to the Site. For automated dissemination, the sub-components at the Concentrator will receive electronic message commands from the Site and electronically forward them to the Source. The Concentrator will then receive the image data from the Source and pass it automatically (push) to the Site as requested. For Site-initiated data transfer (pull), the Site uses the Concentrator as a library by initiating queries for information and initiating information transfer from the Concentrator to the Site.

There is no approval process at the Concentrator for Site imagery needs. The Site is the sole authority of imagery requests and dissemination. Concentrator personnel are available to assist Site personnel at their request and to maintain the operational readiness of the Concentrator.

3.2.2.1 Dissemination Element (DE)

The DE is the front-end interface from the Concentrator to the EPS and the dissemination point for Near Real Time (NRT) National imagery dissemination

to the Sites. The DE interfaces to the other Concentrator sub-components via an Asynchronous Transfer Mode (ATM) local area network (LAN). The DE is configured to support fail-safe processing by data disk mirroring with a 20-minute recovery timeline requirement. The main functions of the DE are as follows:

1) Receive imagery requests from the IESS.

2) Forward imagery requests to the EPS.

3) Receive imagery sent by the EPS.

4) Forward the imagery in NRT to the Sites.

5) Forward imagery to the COPS for archive.

The DE interfaces within the JCA are as follows:

1) DE-IESS via the D3-Receive Segment-to-Host Database (D3-RSHD).

2) DE-EPS via IF20D08P protocol for National imagery dissemination.

3) DE-COPS via FTP.

3.2.2.2 Concentrator Open Primary Server (COPS)

The COPS is the central library and archived imagery dissemination point for the JCA. It operates as a client-server with the client installed at each of the Sites and the server residing at the Concentrator.

The COPS receives compressed Image Products (IMPs) and related support data from the EPS via the DE or from tape ingest via RSP-2150. The COPS supports the processing, management and storage of the data received in accordance with the Tape Format Requirements Document (TFRD). The COPS also supports imagery expansion, minification, database cataloging, and a Hierarchical Storage Management (HSM) capability that controls the storage and migration of data for the on-line (RAID), near-line (jukebox) and off-line (shelf) storage devices.

The COPS stores all of the support data in a relational database. The COPS client that is installed on the IPL hardware at each JCA Site can access the database to assist the Site with imagery research. Requested imagery is transmitted from the COPS to the Site via FTP.

3.2.2.3 Imagery Exploitation Support System (IESS)

The imagery dissemination management sub-component in the Concentrator is the IESS. Imagery requirements in the context of the JCA are defined as the

established and recorded statement of need for imagery of a particular type on a clearly delineated geographic place. Imagery requirements are registered within the Concentrator architecture by the creation of a local exploitation requirement (ER) in the IESS. These requirements do not drive collection of the imagery by the Source, rather they ensure that when the imagery related to a particular ER is made available from the Source, it will be automatically requested and disseminated to the Site.

3.2.2.4 Firewall

The Firewall sub-component stops unauthorized access to the inner LAN while allowing full network interoperability between authorized computers through the firewall. The firewall protects the DE, IESS and COPS at the Concentrator from unauthorized access while allowing JCA users to interface with the IESS and COPS. There are two firewalls located at the PCO, one is active and the other is a near line spare.

3.2.2.5 Global Access Library (GAL)

The Global Access Library (GAL) is a medium-sized Image Product Library (IPL). The GAL resides at the Concentrator and is outside the firewall that isolates critical data from unauthorized access. At IOC, the GAL will serve as a simulated Site located at the Concentrator and as a “victim host” to monitor attempts of unauthorized Users to gain access to the Concentrator.

3.2.3 Site

The basic function of the Site is to request and receive imagery and imagery products to satisfy local requirements, and provide access to archived products at the Concentrator. At IOC, the Site will have a receive-only capability from the Concentrator. During the migration to FOC, the capability to pass products from the Site to the Concentrator will be added to the architecture.

The Site is comprised of four functional sub-components that reside on a single workstation: the IPL, the IESS client, the COPS client, and Matrix. The IPL provides local library and archive functions for the Site. The IESS client provides Site access to imagery request and research functions at the IESS Server. The COPS client provides access to imagery and automated imagery dissemination functions at the COPS Server. Matrix provides a means of viewing imagery. The IESS and COPS clients can be accessed on the IPL hardware or from an IT-21 NT personal computer (PC) using X-window sessions. The IPL can be accessed from any computer on the LAN that has Netscape.

The operations concept for the Site at IOC is to maintain the IPL as the local library containing all operational support data produced locally and received from the Concentrator. Upon refining operational requirements, Site Users will search the IPL to determine if data requirements can be satisfied locally. If the search is not satisfied, the User activates the COPS client to query the COPS server at the Concentrator. If the imagery is available at the Concentrator it is disseminated to the Site as requested. If the COPS query is not successful, the Site can create an imagery requirement in the IESS Server by using the IESS client. If the IESS does not have knowledge of imagery that would satisfy the User request then the User may consider waiting for imagery to become available or initiate a collection nomination through standard Site processes.

The interfaces between the COPS and IESS servers are limited at each Site to prevent overuse of the communications circuits between the Concentrator and the Site. The access to the Concentrator is limited to 4 User accounts per Site at IOC. Those Users with access to the Concentrator define the Site imagery requirements on the IESS server and/or initiate queries for imagery on the COPS Server.

The Sites include ships with bandwidth allocated for imagery dissemination, Rapid Deployment Suites (RDS) and shore sites such as the Washington Planning Center (WPC), the Naval Strike and Air Warfare Center (NSAWC), and the Navy and Marine Corps Intelligence Training Center (NMITC).

3.2.3.1 IPL

The IPL hardware consists of a SUN Enterprise 4500 workstation with RAID configured into a single 19-inch equipment rack with software that provides a local library function to the Site Users. The client for IPL access, named Broadsword, enables the Site Users to search for and retrieve image data from the IPL.

3.2.3.2 IESS Client

The IESS client is installed on the IPL hardware and interfaces with the IESS server located at the Concentrator. The IESS interface provides authorized Users with access to National imagery dissemination management, History of Coverage (HOC) research, and the ability to create National imagery requests.

3.2.3.3 COPS Client

The COPS client permits authorized Users to query and request data from the COPS server that is located at the Concentrator. The COPS Image

Queue function displays all images, with status, that the User has queued for download. It also allows the User to query the image database on a variety of fields. The COPS Image Download function defines the boundaries of the image to be downloaded via the COPS Imagery Boundary Selection (IBS) function. The User can select to download an entire image, a pre-set target boundary, or a User defined boundary defined by dragging the cursor over a desired area. Additional COPS client capabilities at IOC include the preview of overview images used in the chipping process. This capability can be accomplished via X-windows sessions on an NT workstation.

The COPS server can also be accessed by a web based client. Currently, the web-based client does not contain all the functionality of the UNIX client. JCA will transition to the web-based client after IOC when the client functionalities are upgraded to support JCA tasks. The greatest benefit of using a web-based client is that there is no software install activity at the Site.

3.2.3.4 MATRIX

The MATRIX software is packaged with the COPS client software for imagery viewing. The application is also installed on other JSIPS-N equipment such as the Precision Targeting Workstation (PTW). MATRIX can expand and view TFRD imagery that is received. It can also display NITF expanded imagery that is stored on the IPL.

3.2.4 Communications

The Communications component of the JCA provides the network infrastructure required to transfer data throughout the system. At IOC, JCA communications is a combination of point-to-point circuits and Wide Area Network (WAN) connections. Dedicated T3 landline circuits connect the Source to the Concentrator and the Concentrator to Defense Information System Agency (DISA) ATM - Classified Network (DATM-C). The JCA communications architecture supports separate paths to the Atlantic and Pacific Fleets. Ships of the Atlantic Fleet will be supported via the DATM-C connection at NCTAMSLANT, and Pacific Fleet ships will be supported through the DATM-C connection at NCTS San Diego. The satellite communications interface between the shore and the Site is the existing Challenge Athena (CA) system. The JCA network architecture is also scaleable to allow bandwidth increases for additional Challenge Athena Users and access to the GBS/JBS (Post IOC). The JCA Communication architecture at IOC is depicted in figure 3.2.4-1.

During transition from IOC to FOC, additional Sites and Sources will be added as they become available. The JCA communications architecture will support the

transition to FOC with the addition of a T3 landline connection to the Backup Concentrator (BUC) and additional DATM-C connections to new Sites. At FOC, Communications circuits will connect the PCO and BUC to the each other and to the DATM-C. The communications architecture will also support the connectivity between the Concentrators and up to 45 Sites via the DATM-C. The JCA Communication architecture concept at FOC is depicted in figure 3.2.4-2.

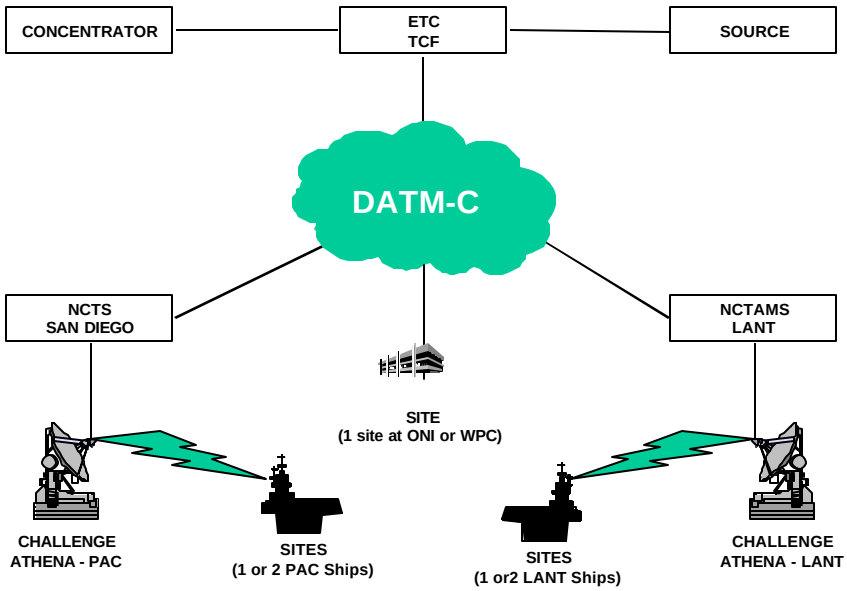

Figure 3.2.4-1 JCA Communications Architecture at IOC

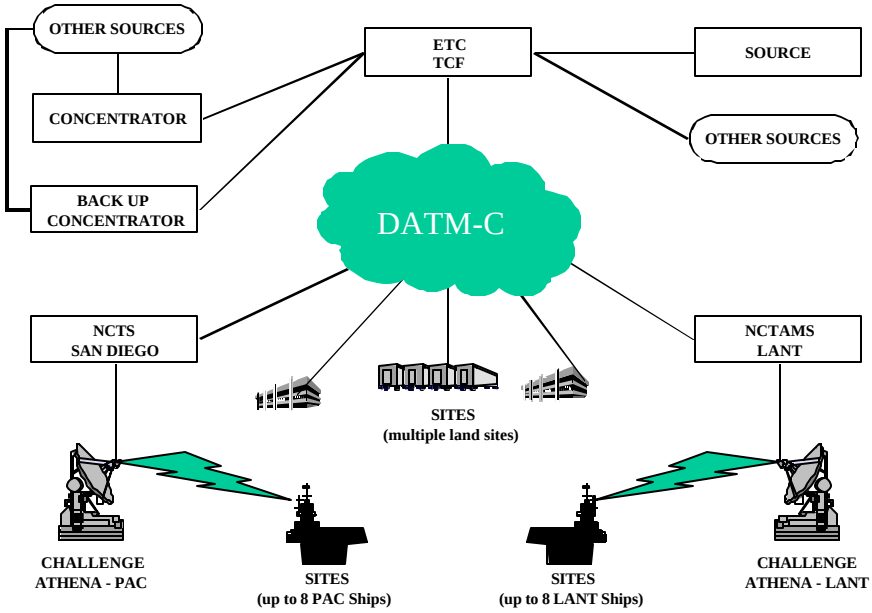

Figure 3.2.4-2 JCA Communications Architecture Concept at FOC

3.3 Physical Description

3.3.1 Concentrator Hardware

The DE sub-component of the Concentrator is a SUN Enterprise 5500 server, four 250 MHz Ultra processors, ½ GB of RAM and 75 GB of RAID storage.

The IESS server sub-component at the Concentrator will be hosted on two DEC AlphaServer 4100 servers (for redundant processing) with eight RAID devices totaling 170 GB storage.

The COPS sub-component of the Concentrator includes an SGI Origin 2000 Fail-safe configured server with eight redundant (16 total) R10K 250 MHz CPUs and 2.0 GB of system RAM. A 1.41 Terabyte raw-storage RAID (1.1 TB usable), an O2 console workstation and ATM, FDDI, and Ethernet LAN interfaces are shared between the two Origin 2000s. The robotics tape library is the EMASS AML/E with a Quadro Data tower with up to 48 TB of storage that will be increased when higher density 3590 tapes become available. Media ingest devices include an Exabyte 8mm 8505 tape drive, a Mountain Gate RSP-2150i S-VHS tape drive and CD-ROM capability.

The GAL sub-component of the Concentrator is a medium-sized IPLwith 288 GigaBytes RAID, on a SUN Enterprise 4000 system. The GAL will interface to the Concentrator from outside the firewall over the ATM network.

There is a firewall sub-component at the Concentrator for security purposes. The firewall is a Sun Ultra II using NAI Gauntlet software. Each Ultra II has dual 400 MHz processors, 512 MB of RAM, and OC-3 ATM connections to the inner and outer networks.

The Concentrator Network sub-component consists of a FORE Systems ASX-200BX ATM switch and a PowerHub 7000 multi-layer switch; 155 Mbps multi-mode fiber ATM ports, and 10/100 Mbps Ethernet ports for local systems.

3.3.2 Concentrator Software

The Concentrator software consists of the DE version 2.2, COPS server software version 1.0 (PPS version 7.0), and IESS server software version 4.0.

3.3.3 Site Hardware

Site hardware consist of the IPL Suite, a SUN Enterprise 4500 unit with four Ultra SPARC 250 MHz processors. RAID storage consists of two CIPRICO RAID arrays with a total capacity of 288 GigaBytes. The IESS and COPS client software

at the Sites will also by hosted on the IPL server hardware. The hardware is mounted on a standard TAC-4 rack that measures 72 inchesx24 inchesx34 inches.

3.3.4 Site Software

The Site software suite consists of the IPL 2.1 server software, the Broadsword version 2.0M client application, the IESS 4.0 client software, the COPS client application (PPS version 7.0) and MATRIX version 5.3.1.

3.3.5 Communications Hardware

The Earth Terminal Complex (ETC) Technical Control Facility (TCF) has a JCA-installed KG-81 cryptographic device, a high speed serial interface (HSSI)-to-RS530 converter, a FORE ATM switch, a Cisco 4500 router, and a KG-95-2 cryptographic device. The TCF also has a laptop computer for monitoring system operations.

Both the Naval Computer and Telecommunications Station (NCTS) in San Diego and the Naval Computer and Telecommunications Area Master Station - Atlantic (NCTAMS-LANT) have JCA-installed Cisco routers and space allocated for up to 10 KIV-7 cryptographic devices (8 for ships and 2 redundant). These stations also have laptop computers to monitor system operations.

The TCF at the National Maritime Intelligence Center (NMIC) has a KG-95-2 cryptographic device to support JCA Concentrator communications.

The JCA Site installations (using Challenge Athena) each have a JCA-installed Cisco router and two KIV-7 cryptographic devices (primary and a spare).

3.3.6 Communications Software

The communications software consists of the HP Openview application that supports network monitoring. Other Communications software are as follows:

a) TBS

4 Primary System Operations

4.1 System Operational Functions at the Concentrator

The Concentrator is the central hub for data receipt from the Sources and data dissemination to the Sites within the JCA. The sub-components of the Concentrator provide the functionality to request, receive, manipulate, store, and disseminate imagery and related support data for the Fleet. These services include Internet services, file manipulation, source interfaces, product ordering, dissemination management, data archiving, image processing, image product conversion, and system monitoring. Table 4.1-1 shows the breakdown of these functions among the sub-components of the Concentrator.

	DE	IESS	COPS	GAL	Firewall
Interface to Source	X				
Product Request	X	X			
Dissemination Management	X	X			
Data Archiving			X		
Image Processing	X		X		
Image Product Conversion			X		
Internet Services			X		
File Manipulation			X	X	
System Security	X	X	X	X	X

Table 4.1-1 JCA System Functionality by Sub-Component

4.1.1 Interface to Sources

The Concentrator interfaces with the EPS at IOC and with additional Sources, if any, by FOC. Non-Standard Source interfaces are terminated at the Concentrator so that the Sites receive standardized file-based data. JCA personnel at the Concentrator provide the maintenance and operations support for the interfaces

to the Sources in order to ensure timely delivery of imagery and related data to the Sites.

4.1.2 Product Request

The Concentrator provides the physical connectivity between the Sites and the Sources. Imagery requests from the Sites are sent to the Sources via the Concentrator and the resulting imagery and support data are forwarded to the Concentrator for dissemination to the Sites. Concentrator personnel can assist Site personnel in the creation of imagery requests.

4.1.3 Dissemination Management

The IESS and the COPS servers provide the dissemination management function. The dissemination management functionality records data to assist in the request of products from the Sources and timely delivery of the requested products to the Sites. Although the requests for products at the Sources are sent from the Concentrator, it is the Sites that are responsible for the imagery requests that generate the dissemination of products. It is important to note that the Concentrator is only a mechanism for the receipt, storage and dissemination of imagery as requested by the Site. The JCA Concentrator personnel are not responsible for review or approval of imagery requests originating from the Sites.

4.1.4 Data Archiving

The EMASS Tape Robotic and SGI RAID, operated by the COPS, are the major data archives at the Concentrator. Data archiving is necessary for retaining volumes of long term data for potential Site use. Data storage is managed according to inherent attributes such as age and last time of access and importance of the data as established by the requester. Such attributes indicate how the data will be stored: on-line, near-line in a jukebox-like device or off-line on tape media. Depending on the source of the data, products are accepted either electronically or from media into the JCA at the Concentrator. Data storage at COPS is managed via HSM devices. The COPS image data is also appropriately indexed to aid in the rapid retrieval from off-line data archives.

4.1.5 Image Processing

The COPS supports the extraction (chipping) of sub-regions from a stored image to provide efficient use of Site bandwidth and archive storage. When a portion of an image is extracted, the support data is updated to reflect the information that pertains to the smaller section of the image. Sites with small bandwidth or limited storage capabilities can query data at the Concentrator and extract only

those portions that are needed by that Site. Local procedures should dictate that when repetitive chipping is required, the User should redefine the target boundaries within IESS. This would alleviate the need to chip images on a regular basis.

4.1.6 Image Product Conversion

At IOC, there are no product conversion requirements at the Concentrator. However, the COPS is capable of converting imagery from 4.3 TFRD to 1.3 TFRD and from TFRD to NITF JPEG. After IOC there may be new sources that require format conversions in order to be useful to the Fleet. Format conversion will take place at the Concentrator within the COPS sub-component.

4.1.7 System Monitoring

The JCA provides system monitoring of the communications architecture and the hardware sub-components to provide quick and effective trouble resolution and reduction of System down time. HP Openview software is used to provide information to personnel at the Concentrator as well as to personnel at the Navy TCFs. The Concentrator is the central point for JCA system monitoring. Any problems noted by the monitoring software are recorded and taken for action by JCA Concentrator personnel.

4.1.8 Internet Services

The JCA Internet services residing on the COPS provide e-mail, Domain Name Service (DNS), and web server functions along with a variety of other server processes supporting the requirements of the system.

4.1.9 File Manipulation

Data residing within the JCA is file based and can be manipulated with standard file management tools. The tools include copy transfer functions, file naming, directory organization and file deletion.

4.2 System Operational Functions at the Site

The Site is the end User of the JCA. The main operational functions at the Site consist of queries for required imagery and related products or initiation of dissemination requests for imagery that has not yet been stored at the Concentrator. Table 4.2-1 shows the breakdown of these functions among the sub-components at the Site.

	IESS Client	MATRIX	COPS Client	IPL
Interface to Concentrator			X	X
Imagery Research	X		X	X
Product Request	X		X	
Dissemination Management				X
Data Archiving				X
Image Processing		X		X
Image Product Conversion				X
File Manipulation		X		X
Interface to Site Systems				X

Table 4.2-1 JCA Site Functionality by Sub-Component

4.2.1 Interface to Concentrator

The IPL provides the interface from the Site to the Concentrator. It receives imagery that is sent by the COPS or DE and provides User inputs from the IESS and COPS clients at the Site to the Servers at the Concentrator.

4.2.2 Imagery Research

Sites may use any of three methods (IPL, COPS or IESS) to research for imagery coverage. The IPL contains information on imagery resident at the local IPL. The COPS client has information on the archived holdings at the Concentrator but the IESS client provides a much broader scope of information pertaining to all National Imagery. Table 4.2.2-1 provides an overview of the three methods of acquiring imagery. It is expected that when imagery is not available through any Source and must be submitted for collection, the process to request collection will remain the same as today. Sites will be required to submit nominations for collection through established procedures for their Site.

JCA Sub-component	When to use	How to Use
IPL	Initial search for imagery.	Use the IPL via the Broadsword client application. The User researches the Site IPL to see if the imagery available.
COPS	If imagery is not available at the Site IPL.	Use the COPS client to determine if the imagery is available at the Concentrator. If available, request delivery through COPS Client.
IESS	If imagery is not available on the COPS and the IPL	Use the IESS client to research the imagery coverage database. If imagery requirement can be met by imagery available at the source, initiate a *FAF Block Recalculation. If imagery is not available input a new requirement for future dissemination and provide the imagery requirement to the Imagery Officer for possible collection request.
*FAF Block Recalculation is the process for requesting imagery for a target that was not ordered when originally made available. This function allows the Site to enter the image and target information and send the request to the DE for forwarding to the Source. The IMP is calculated and processed by IESS, the DE and the Source and the resultant imagery is delivered to the Site		

Table 4.2.2-1 Methods of Imagery Acquisition at the Site

4.2.3 Product Requests

Product requests are initiated at the Site by creating imagery requirements in the IESS via the IESS client or by initiating imagery push from the COPS in response to queries made by the Site via the COPS client.

Product requests are not collection requirements. They are requests for delivery of imagery that has already been collected. JCA does not support collection requests or nominations.

4.2.3.1 Imagery Requirements Management

The Site initiates the creation of Exploitation Requirements (ERs) by using the IESS client to access the IESS server at the Concentrator. The use of a Site Code uniquely identifies those requirements within the IESS server. The IESS server performs Target-to-Image Correlation (TIC) and Requirements-to-Image Correlation (RIC) on the Exploitation Support Data (ESD) in IESS to determine if an imagery requirement can be satisfied. The IESS server then initiates the imagery request and states the Site destination for the image.

4.2.3.2 Creation of Local Exploitation Requirements

To create a local requirement, the Site, using the IESS client, activates the local requirements list function. Creating a requirement initiates a process that enables the User to define a requirement by a large number of parameters and queries to include geographic area, Basic Encyclopedia (BE) number, Category Code, Country Code (CC), start and stop dates, and frequency of the need. This is also where the Site specifies the imagery characteristics that are considered minimal to satisfy the requirement. Finally, the Site needs to ensure that the proper Site Code, Free Text Name, and Essential Elements of Information (EEI) statement are entered. The requirement activates the IESS database for searches against all future imagery availability information processing.

Using this process allows the Site to have complete control over the establishment, maintenance and status of their ERs.

4.2.4 Dissemination Management

Dissemination Management at the Site is supported by the IPL. The IPL can forward imagery files to a workstation User via profiles or at the User's request. The User also controls the dissemination management of the imagery that is ordered via IESS for that Site.

4.2.5 Data Archiving

The IPL is the central archive for Site imagery and imagery related data. The Site imagery workstations may have different requirements for image formats and data compression. The IPL V2.1 and later can be used to expand and/or decompress images for the Site User if necessary. The web browser technology of the IPL allows for the ease of transferring data to the appropriate workstation. Typical usage of imagery at the Sites includes RRDS creation, product generation (e.g., targeting support), strike planning, indications and warning, battle damage assessment, and special operations forces support.

4.2.6 Image Processing

The IPL supports the extraction of sub-regions from a stored image to provide efficient use of Site LANs, tape generation, and archive storage. When a portion of an image is extracted the support data is updated to reflect the information that pertains to the smaller section of the image. Workstations with limited storage capabilities could query data at the IPL and extract only those portions that are needed by that workstation User.

4.2.7 Image Product Conversion

The IPL can provide image product conversion but it is currently not anticipated to be a requirement at IOC because the 1.3 TFRD imagery format is a common format that is currently in use within the Fleet.

4.2.8 File Manipulation

Data residing within the JCA applications at the Site will be file based and can be manipulated at minimum with standard file management tools. The tools include copy transfer functions, file naming, directory organization and file deletion.

4.2.9 Interface to Site Systems

Within the JSIPS-N, the Precision Targeting Workstation (PTW) and the Digital Imagery Workstation Suite (DIWS) require imagery support from the IPL. The GENSER PTW can receive imagery from the IPL electronically. The SCI PTW and DIWS have to receive tapes generated by the GENSER PTW until the Enhanced SCI Isolation System (ESIS) is approved to provide electronic transfer of imagery between different security levels.

Other non-JCA systems can interface to the IPL for imagery by conforming to the imagery formats that are supported by the IPL and by being a part of the LAN architecture that the IPL resides on.

4.3 Communications Architecture

The Communications component of the JCA provides the network infrastructure required to transfer data throughout the system. At IOC, JCA communications is a combination of point-to-point circuits and Wide Area Network (WAN) connections. Dedicated DS-3 landline circuits connect the Source to the Concentrator and the Concentrator to Defense Information System Agency (DISA) ATM - Classified Network (DATM-C). The JCA communications architecture supports separate paths to the Atlantic and Pacific Fleets. Ships of the Atlantic Fleet are supported via the DATM-C connection at NCTAMSLANT, and Pacific Fleet ships are supported through the DATM-C connection at NCTS San Diego. The satellite communications interface between the shore and the Site is the existing Challenge Athena (CA) system. The JCA network architecture is also scaleable to allow bandwidth increases for additional Challenge Athena Users and access to the GBS/JBS (Post IOC). Figure 4.3-1 shows the Communications architecture at IOC.

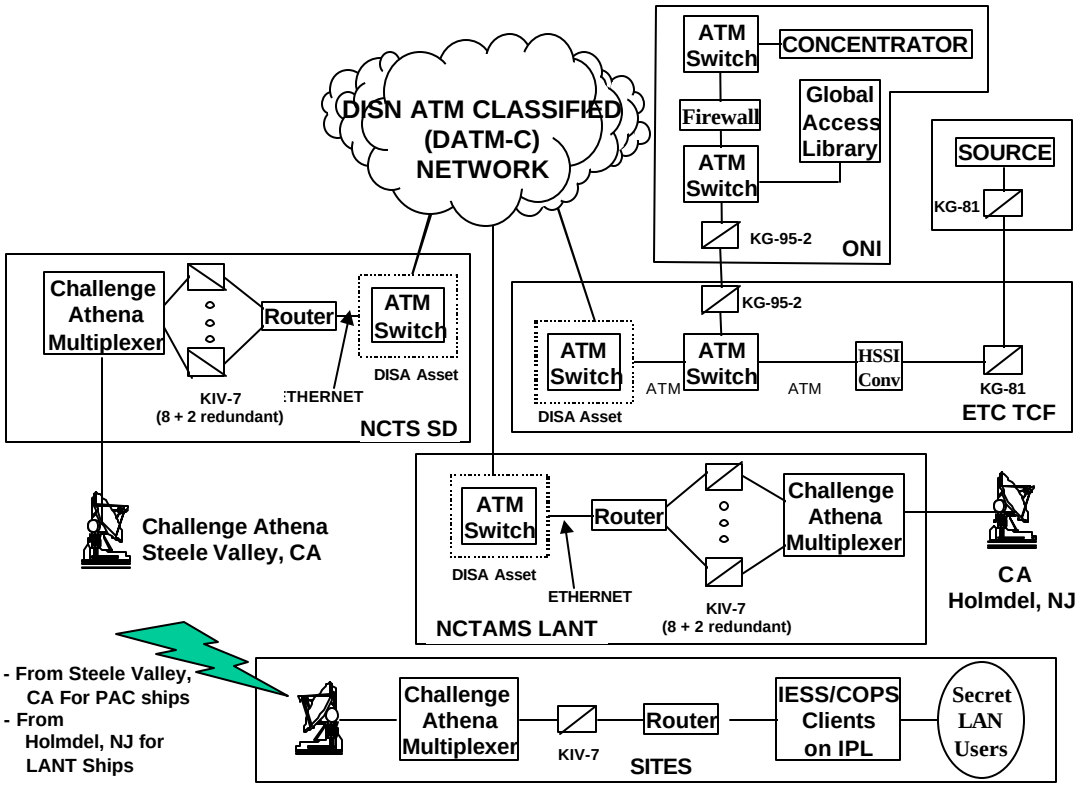

Figure 4.3-1 JCA Communications Architecture (IOC)

During transition from IOC to FOC, additional Sites will come on-line and additional Sources will be available. The JCA communications architecture will support the transition to FOC with the addition of a dedicated DS-3

landline connection to the Backup Concentrator and bandwidth increases to support the addition of Sites to the DATM-C network. At FOC, JCA will consist of two Concentrators (primary and backup), up to 22 concurrently active Sites (16 ships - eight from each coast and six shore facilities), 45 maximum Users, and connectivity to GBS/JBS via the DATM-C network (if available and required by the Fleet).

4.3.1 Source to Concentrator Communications Architecture

The Communications architecture between the Source and the Concentrator provides the mechanism for transfer of messages that support the request, status, and near-real time delivery of imagery from the Source to the Concentrators (Primary and Backup). The communications component also provides for the delivery of the requested imagery to the Sites. The communications equipment supports the conversion of the IF20D08P data stream to standard TCP/IP over ATM. Data is encrypted at the Source and delivered to the ETC TCF where it is decrypted and converted to ATM. The data is then re-encrypted using a KG-95 and sent to the Concentrator via a DS-3 point-to-point circuit and decrypted using a KG-95.

Messages that are created at the Concentrator are transferred to the Source via the DS-3 circuit and converted from ATM to IF20D08P and sent to the Source for processing.

4.3.2 Concentrator Component Communications Architecture

Within the Concentrator, the communications architecture is designed around a firewall that protects the mission critical components from unauthorized access. The sub-components on the inner, or protected, LAN are the DE, IESS, and COPS (including the EMASS tape storage device). The GAL is the only Concentrator sub-component that is outside the Firewall because it is used as a test Site. There are two LANs used at the Concentrator, the inner and outer LANs. Both networks are 155 Mbit ATM and connect the sub-components and peripherals to one another, provide access to the firewall for interfaces between the Concentrator and the Source, and transfer data to and from the Sites.

4.3.3 Concentrator to Site Communication Architecture

The communications architecture between the Concentrator and an afloat Site is a combination of point-to-point circuits, the DATM-C, and the Challenge Athena (CA). Data at the Concentrator is transferred to the ETC TCF via the same DS-3 circuit that transfers information between the Concentrator and the Source. At the ETC TCF, the data is uplinked to the DATM-C for transmission to the appropriate Navy TCF supporting the CA

interface to the Fleet. Data is transferred to NCTS SD if the ship is under PAC CA support and to NCTAMS LANT if the ship is under LANT CA support. The data is transferred from the appropriate Navy TCF to their respective CA uplink terminal. The uplink terminals are located in Steele Valley, CA for PAC and in Holmdel, NJ for LANT. The data is encrypted for JCA using KIV-7 cryptos and then multiplexed for transfer to the afloat Site via CA. Once the data reaches the ship, it is de-multiplexed and sent to the JCA spaces where it is decrypted using a KIV-7 and sent to the IPL. The return path for messages and information being transferred from the Site to the Concentrator is the exact reverse of the path from the Concentrator to the Site.

For land Sites, access to the JCA is via the DATM-C. Each land Site is responsible for getting communications connectivity between their IPL and the DATM-C. The interface between the Concentrator and the DATM-C is the same for all Sites. The only change to the Concentrator to DATM-C architecture that will need to be made is expansion of the bandwidth to accommodate additional Sites.

4.3.4 Site Communications Architecture

At the Site, the JCA communications architecture consists of the following sub-components: communications circuit from CA to the JCA KIV-7 and a router that provides network access to the IPL. The Site communications architecture provides the mechanism to transfer information between the CA downlink and the IPL.

4.3.5 Communications Monitoring System

The JCA communications architecture is monitored via HP Openview from a central post at the Concentrator. Monitoring stations are available at the Concentrator, NCTS SD and NCTAMS LANT. The monitoring software allows the support personnel to visually inspect the JCA communications circuits for problems. Visual indicators change color to indicate potential problems. Rapid identification of problem areas in the communications architecture will reduce individual Site and overall System down time.

4.4 System Security

There are two considerations in JCA system security: protection of the mission critical Concentrator sub-components and protection of the shipboard LAN. JCA uses a combination of physical security, host security, and network security to protect the Concentrator sub-components and the shipboard LAN.

4.4.1 Physical Security

To prevent unauthorized physical access to the JCA, all critical equipment and unencrypted data transfers are physically located within a SCIF. All personnel granted access to JCA critical equipment and unencrypted data will possess, at a minimum, a SECRET security clearance.

4.4.2 Host Security

To prevent unauthorized login and access to unencrypted data (cracking), each computer component of the JCA conforms to established DoD Host security policies. These policies include; single User accounts with password aging, shadow passwords, login audit trails, Security Banners, Consent to Monitoring warnings, virus detection software, restricted directory and file permissions, and TCP Wrappers. In addition to DoD Host security policies, JCA Site IPLs function as Bastion Hosts to prevent data transfer from the JCA network connection to the shipboard LAN network connection and vice-versa (IP forwarding). IP forwarding on the dual-homed IPL is prevented by the proper configuration of Operating System specific files: /etc/hosts, /etc/netrc, etc/services, /etc/inetd.conf, and /etc/.rhosts. Additional security measures, as identified by Fleet Security agents of PMW-161, will be implemented as necessary.

4.4.3 Network Security

Unauthorized network access to critical sub-components of the Concentrator is prevented with firewalls between the inner and outer LANs. Network traffic through the firewalls is limited to only those services required for JCA operation, all other services are expressly denied. Unauthorized network access to the Sites is prevented by implementation of an ATM Secure Emulated LAN, ATM NSAP Port filtering at the DATM-C uplink locations, and Access Control Lists (ACLs) on all JCA managed network devices.

Post IOC, JCA will migrate to the Fleet managed firewalls and implement Virtual Private Networks (VPNs) to pass firewall encrypted data between the Concentrator firewalls and the Fleet firewalls.

4.5 System Operational Flows at IOC

4.5.1 Imagery Request Flow

The Site initiates requests for imagery dissemination in one of three ways: local query of imagery available at the IPL, image query of the COPS file holdings or imagery request via IESS. Figure 4.5.1-1 provides a flow chart of the progression through the JCA options available to the Site User.

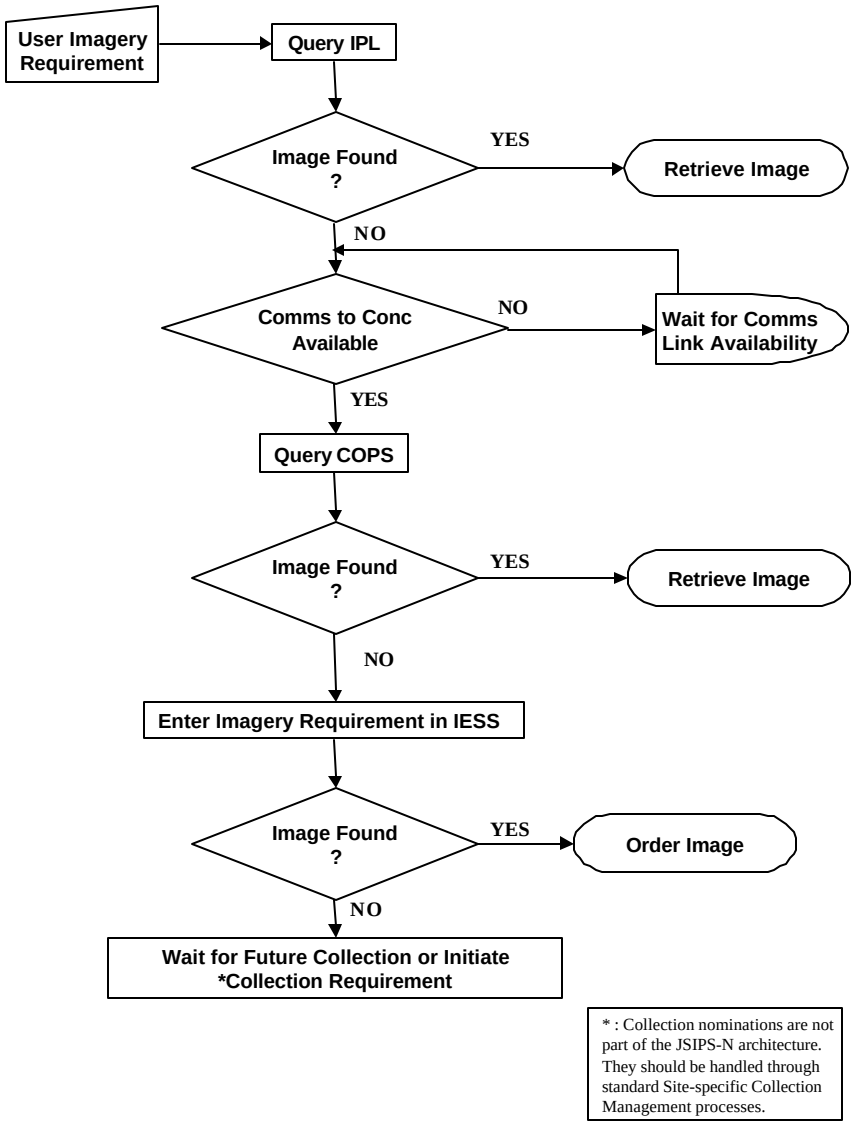

Figure 4.5.1-1 JCA Site Operational Concept

4.5.1.1 Imagery Requests using IPL

When a Site User receives a request for imagery or a task that requires imagery, the IPL should be the starting point for the imagery research. The User logs into the IPL via the Broadsword and initiates a query of the IPL holdings. If the query is successful, the User can select the imagery that satisfies the requirement and have that imagery transferred to a workstation.

If the image requirement cannot be satisfied by the local imagery holdings on the IPL, the User will need to expand the search to include the Concentrator assets.

4.5.1.2 Imagery Requests using COPS

The COPS client can be used to query the imagery holdings at the Concentrator. Since the Concentrator is a compilation of the imagery requests of all the Sites, the User may find the required imagery at the Concentrator. If the imagery is located in the COPS archive, the User can transfer the imagery to the Site IPL using the COPS client.

Site User access to the COPS server should be limited to a few authorized Users who have the responsibility to order imagery for the Site. If too many Users have access to the Concentrator, the Site bandwidth allocated for imagery receipt may be over utilized and cause a delay in the near real time imagery delivery to that Site.

If the required imagery does not exist at the Concentrator, the Site User may research imagery availability using the IESS client to access the IESS server at the Concentrator.

4.5.1.3 Imagery Requests using IESS

If imagery is not available at the Site or Concentrator, the Site User enters a new requirement into the IESS to determine if an image exists that could satisfy the new requirement. If an image is found, the User can request the image. If no imagery is available, the User can keep the new requirement in the database so that any matching imagery received in the future will be automatically sent to the Site.

If an image cannot be found after trying the IPL, COPS and IESS then the User should verify all parameters to ensure that the imagery request is correct. After that verification, the User should consider generating a collection requirement using the site-specific collection management process because JCA does not support collection nomination.

4.5.1.3.1 Imagery Requests for Standing IESS Requirements

The IESS client at the Site provides access to the IESS server at the Concentrator. The Site can initiate an imagery request in the IESS that is automatically disseminated to the Site when it becomes available at the Concentrator.

Imagery requests are stored as local requirements against targets within the IESS target database. Once an image requirement has been established, the IESS server monitors the Exploitation Support Data (ESD) files sent from the EPS via the DE. When the ESD indicates that imagery will be available to satisfy the requirement, the IESS sends an Image Definition Message (IDM) to the DE to request the image. The DE receives the IDM, saves the dissemination information, and forwards the ordering information in a Product Request Message (PRM) to the EPS. Figure 4.5.1.3.1-1 shows the flow of imagery and messages within JCA for imagery requests made within the IESS and satisfied by the EPS.

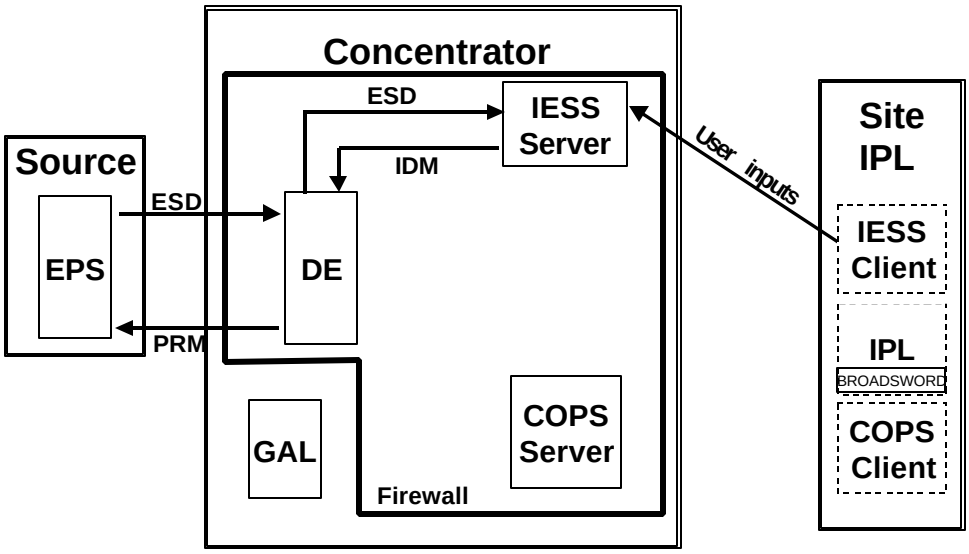

Figure 4.5.1.3.1-1 IESS Imagery Request Flow (IOC)

4.5.1.3.2 Imagery Research for a New Imagery Requirement

It is possible to order an image that did not previously have an active dissemination requirement in IESS. The requested image must be in the standard AOI for the Concentrator, which is most of the world. First, the User initiates a "Query Database" for the target. This returns a list of images that intersect the target. Images from the previous 30-60 days (depending on how the site's purge capability is set up) can be ordered from

the EPS. The User takes the image ID and enters it into "FAF Block Recalculation" on the IESS. The User is then given a list of targets on the image and can order an image based on the target that the User was looking for. The User requests the image by initiating a manual IDM and sending it to the DE. From that point on the procedure would be the same as requesting imagery from an existing IESS requirement.

4.5.2 Dissemination Flow

When the Site requests imagery, the EPS provides Sort Status Messages (SSM) to the IESS via the DE that provide the status of the imagery request until it is satisfied. Requested imagery is provided to the DE at the Concentrator from the EPS via the IF20D08P interface in TFRD format compressed to 1.3 bits per pixel (bpp). When imagery is received at the DE, it sends a Product Status Message (PSM) to the IESS server to notify the IESS of the imagery receipt. The DE then sends the 1.3 TFRD image to the COPS via FTP. The DE uses the dissemination information provided by IESS to FTP the image to those Sites that requested it. Figure 4.5.2 - 1 depicts the IOC dissemination flow of imagery for a single Site.

During the transition from IOC to FOC, the imagery format for JCA will change from compressed TFRD to compressed NITF. When the EPS is capable of

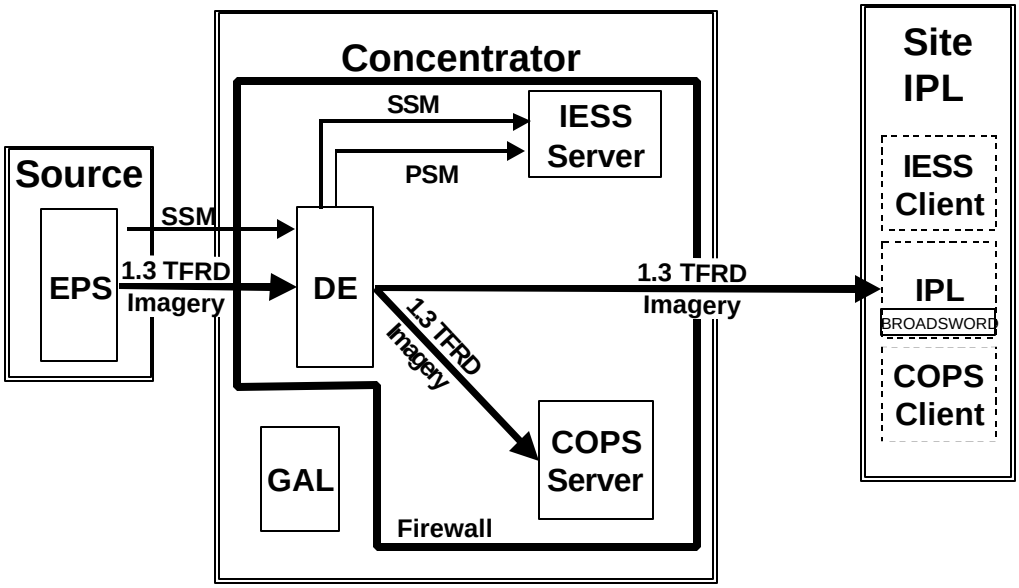

Figure 4.5.2-1 Imagery Dissemination Flow (IOC)

generating NITF compressed imagery the JCA will transition to NITF compressed imagery as its standard format.

4.5.3 Archive and Retrieval

The JCA provides archives at the Site (IPL) and at the Concentrator (COPS) for the storage of imagery and image-related data. The archives provide different functions within the JCA.

The IPL provides storage of Site-specific imagery and imagery related data for use by the Site. The storage capacity on the IPL is 288 Gigabytes (maximum at IOC). When that storage capacity becomes critical, the Site must manually move imagery to tape (8mm), and delete unnecessary or less critical imagery. The IPL software version 2.1 has an automated off-line storage capability to the 8 mm tape drive on the SUN. IPL is currently being configured to provide an archive capability to an RSP-2150 tape recorder.

When a local query of the IPL does not satisfy an imagery request or the Site requires imagery it previously deleted, a query of the Concentrator archive is initiated by the Site using the COPS client. If the query is successful, the imagery is requested by the Site and delivered to the IPL for local storage on the IPL archive.

Shipboard Users that require imagery may retrieve it from the IPL server at the Site. If imagery is not available to meet a requirement, the User provides an imagery request to the personnel that are designated to provide imagery from the Concentrator. Once the imagery is located, it is requested and delivered to the IPL. The User can then retrieve the imagery from the IPL for use at a Site workstation.

Other Site systems that require imagery should interface directly with the IPL for standardized archive and retrieval of imagery and imagery products.

5 Back-up Concentrator System Operations

5.1 Background

The Washington Planning Center (WPC) is the site of the backup JCA Concentrator, which is officially designated as the Backup Concentrator (BUC). The BUC will be brought into service and made fully operational when the PCO is inoperable for greater than 8 (TBR) hours or when subsequent JCA software releases and/or hardware changes require test and evaluation before being fielded. The BUC is staffed by WPC personnel when operating in a standby mode, and by WPC and ONI JCA personnel when the BUC is activated and in an operational mode. The transition from the Primary Concentrator to the BUC is completed within 4 (TBR) hours at which time the BUC is fully capable of performing operational support to the Fleet, 24 hours a day, seven days a week.

5.2 Functional description

5.2.1 Overview

The BUC provides system redundancy for the near-real time imagery requirements of the Fleet. It is composed of sub-components similar to those of the Primary Concentrator with the exception of the tape robotics used at the PCO for near-line archiving.

During normal PCO operations, the BUC equipment will be powered on and available for possible transition activities. The BUC will also maintain a small bandwidth link to the EPS to ensure link availability for contingency operations. The WPC will operate as a Site on the PCO by using its IPL and connectivity to the Classified DISA ATM network (DATM-C) to order and receive imagery. The BUC IPL will receive all imagery from the PCO for use at the WPC and for use as a limited archive (COPS RAID) during BUC operations.

BUC operations are initiated upon failure of the PCO to provide support to the Fleet or for test and evaluation of new hardware and/or software versions. The Library archive at the PCO is not available during BUC operations. Consequently, during these periods of operation, the BUC provides a limited on-line archive of imagery and the capability to request new imagery. Specifically, the archive is limited to the contents of the COPS RAID.

Whenever the PCO is available to resume normal operations, the BUC will transition historical information to the PCO via database synchronization or

message traffic. The PCO will require an average of 4 (TBR) hours to update its component databases prior to resuming its normal activities.

Test activities at the BUC are coordinated with the associated Sites and with affected NIMA components so that support can be assured during testing, if required. When the BUC is used for test and evaluation of new hardware and/or software, the PCO EPS link is set to a message receive mode only and the majority of the JCA Bandwidth is allocated to the BUC for the duration of the test activity. The PCO still receives and processes Site imagery requests but it does not receive imagery from the EPS until its bandwidth is returned from the BUC.

5.3 Synchronization Between the PCO and BUC

The COPS and IESS sub-components of both the PCO and BUC must be synchronized to provide operations support to the Fleet. The DE does not require synchronization because it can get its information from the IESS. The function of synchronization within the JCA architecture is accomplished through a combination of message traffic, manual operations, and computer automated functions.

5.3.1 COPS Synchronization

The COPS databases will be synchronized whenever a change is made and the communications path between the PCO and BUC is active. If the link is not active, the updates will be stored for future synchronization. The synchronization of the COPS databases ensures that whichever Concentrator is activated can satisfy Site requests. Synchronization is accomplished via Sybase replication software and scripts.

5.3.2 IESS Synchronization

The IESS databases that support dissemination management and target information are synchronized whenever a change is made and the communications between the PCO and BUC is active. If the communications link is not active, the synchronization activity will be suspended until the link is re-established. Synchronization is accomplished via Sybase replication software and scripts.

5.3.3 Security Administration Synchronization

Security administration for the PCO and BUC will be manually coordinated as necessary to maintain the User base on the JCA. A new Site will be added to the PCO and BUC during the Site's installation activity. The administrators for the PCO and BUC will verify their information regularly to ensure that both Concentrators are able to support Fleet operations.

5.4 Concentrator Transitions

Transitions between the PCO and BUC are approved by PMA281 upon the request of the Concentrator personnel. A Standard Operations Procedure (SOP) is available to the Concentrator personnel, which outlines the potential reasons for a request to transition and the procedures for transitions from the PCO to the BUC and from BUC to PCO.

5.4.1 Transition from PCO to BUC

The transition from the PCO at ONI, to the BUC at WPC, essentially consists of switching ports at the EPS from one Concentrator to the other. This is accomplished via telecommunications or, as a secondary means, via a critical message to the EPS. Communications links are then opened to enable Sites to pass product request messages from their IESS client or COPS client to the IESS server or COPS server at the BUC. Full time WPC connectivity to the DATM-C network will allow database synchronization activities of the IESS and COPS. This will ensure that the BUC is current on all PCO imagery information.

5.4.2 Transition from BUC to PCO

When the PCO is once again ready to assume its role as the Concentrator for JCA, the BUC to PCO Transition is initiated. The BUC terminates message traffic to and from the EPS and terminates imagery receipt from EPS. The BUC Site Representative contacts the EPS and requests that the imagery in the BUC queue be transferred to the PCO queue (TBD).

The communications link between the PCO and the BUC is established so that the IESS and COPS can perform database synchronization and security administration updates. When the IESS and COPS synchronization is complete, the bandwidth is re-allocated to the PCO (TBD). The PCO Site Representative initiates the activation of the circuit to the EPS and activates imagery and message transmissions.

Before the PCO assumes its operational role to the Fleet, it needs to capture the messages and subsequent imagery that were handled by the Backup Concentrator. The IESS Operator requests all missed message traffic, and IESS processes orders for imagery that were handled by the Backup Concentrator. The COPS dissemination to the Fleet is not activated at this time, because the imagery that the PCO is recovering has already been disseminated to the Fleet from the BUC. When the imagery is disseminated from the EPS to the PCO, it is stored in the COPS for future archive actions. When the messages have been processed and the imagery received, the COPS is activated for Fleet dissemination and the IESS begins processing new messages.

5.5 Physical Description

5.5.1 BUC Hardware

The BUC, as previously stated, is comprised of sub-components that are either equivalent to or scaled-down versions of those sub-components that are resident at the PCO.

5.5.1.1 BUC Imagery Exploitation Support Segment (IESS)

The BUC IESS is hosted on two DEC AlphaServer 4100 servers each configured with an 8mm tape drive, diskette, CD-ROM, and 7 tape stacker. The BUC IESS utilizes the same RAID configuration as the Primary Concentrator (with the redundant controllers). However, a 15 GB hard drive and an extra 25 GB RAID have been added to the BUC IESS configuration to support Sybase replication. In addition, the BUC IESS will incorporate an IT-21 personal computer. The workstation will consist of a 17" monitor, keyboard, mouse, 64 MB RAM, CD-ROM, ATM and Ethernet NIC cards, 8 MB Video RAM, and a Pentium II processor.

5.5.1.2 BUC Concentrator Open Primary Server (COPS)

The BUC COPS, as with the primary COPS, consists of an SGI Origin 2000 server configured with 4mm and 8mm tape drives, an S-VHS tape drive, but no robotic tape library. Additional storage of the BUC COPS will consist of 5 extra hard drives with a total capacity of 25 GB, and a total of 600 GB of RAID.

5.5.1.3 BUC Dissemination Element (DE)

The BUC DE will be identical to the primary at ONI.

5.5.2 BUC Software

There are no significant software differences between the sub-components of the BUC, and those of the Primary Concentrator.

5.5.3 Communications Hardware

The communications architecture of the BUC is reliant upon the same communications architecture as the PCO. Consequently, all sites achieve connectivity to WPC Concentrator through the DATM-C network. Connectivity to the TCF is achieved via a dedicated T-3 communications circuit to the WPC.

6 Logistics, Operations and Maintenance

6.1 Problem Resolution

The JSIPS-N Help Desk (JHD), located at the Space and Naval Warfare Systems Center Systems Center San Diego Detachment, Philadelphia (SPAWAR Phila.), is the single Point of Contact (POC) for all JCA trouble calls. JHD Staff are available 7 X 24 hours to accept Fleet trouble calls and initiate trouble resolution. The JHD personnel coordinate problem resolution for the Fleet that includes contacting hardware vendors, contacting software developers, and acting as the coordinator between the Fleet and those contractors. The JHD may have some procedures to assist in basic troubleshooting but they are not be held responsible for the final resolution of a trouble call.

When trouble calls are logged for JCA, the JHD calls the active Concentrator to start trouble resolution. The Concentrator personnel contact the Site to proceed with trouble resolution. Concentrator personnel have tools available to determine communications outages as well as server failures and can proceed with the resolution of those issues before the Site registers a trouble call.

The JCA Concentrator personnel have several communication avenues open to the Sites. The Concentrators support e-mail between the IPL at the Site and the Servers at the Concentrator, SIPRNET, and unclassified e-mail and telephone communications. Any trouble calls that are not resolved will be entered into the JSIPS-N Discrepancy Report (DR) system and categorized by importance to the Site Users ability to operate the system.

6.2 Document Distribution and Access

Documentation that pertains to the operation and maintenance of JCA components and sub-components will be made available to the Site in hardcopy during the installation or training phase. Updates to those hardcopy documents will be via unclassified web site access. It is anticipated that JCA related documentation of a classified nature would be made available through a SECRET website or directly disseminated to each Site from the active Concentrator via e-mail.

6.3 JCA Training

JCA training will be incorporated into the currently active JSIPS-N Dissemination Managers' Course that is performed by the NMITC personnel. Until JCA is incorporated into the training curriculum, JCA personnel will train personnel at each Site. Training will consist of a system overview, IPL operator/System

Administrator training, COPS operator training, IESS operator training and communications architecture and troubleshooting training.

6.4 System Administration

System Administration procedures are required at the Concentrators and at each Site. System Administration activities include ensuring that system control and access (security) is maintained, coordination of system down time for maintenance activities, preventative maintenance, and system backups. Whenever possible, scripts will be written to simplify the System Administrator tasks at the Site.

Concentrator System Administration is the responsibility of the JCA Concentrator Site Representatives. Site administration is the responsibility of those individuals specified as System Administrators by the Site. JCA System Administration requirements will be incorporated into established Standard Operating Procedures (SOPs) for the Sites.

7 Acronyms

ACL	Access Control List
AOI	Area of Interest
ATM	Asynchronous Transfer Mode
BE	Basic Encyclopedia
BUC	Back Up Concentrator
CA	Challenge Athena Communications System
CBT	Computer Based Training
CC	Country Code
CD-ROM	Compact Disc - Read Only Memory
CIGSS	Common Imagery Ground Surface System
COPS	Concentrator Open Primary Server
CPU	Central Processing Unit
D3-RSHD	DDS-3 Receive Segment to Host Database
DATM-C	DISA ATM-Classified
DDS-3	Defense Dissemination System-3
DE	Dissemination Element
DEC	Digital Equipment Corporation
DIA	Defense Intelligence Agency
DISA	Defense Information System Agency
DNS	Domain Name Service
DoD	Department of Defense
EEI	Essential Elements of Information
EPS	Enhanced Processing Segment

ER	Exploitation Requirement
ESD	Exploitation Support Data
ESIS	Enhanced SCI Isolation System
FAF	Fast Access Format
FDDI	Fiber Distributed Data Interface
FOC	Full Operational Capability
FTP	File Transfer Protocol
GAL	Global Access Library
GB	Gigabyte (1024 Megabytes)
GBS	Global Broadcast System
GENSER	General Service
HMI	Human Machine Interface
HOC	History of Coverage
HP	Hewlett Packard
HSM	Hierarchical Storage Management
HSSI	High Speed Serial Interface
IBS	Imagery Boundary Selection
IDM	Imagery Definition Message
IESS	Imagery Exploitation Support System
IMP	Image Product
IOC	Initial Operational Capability
IP	Internet Protocol
IPL	Image Product Library
IT21	Information Technology - 21st Century
JBS	Joint Broadcast System

JHD	JSIPS-N Help Desk
JCA	JSIPS-N Concentrator Architecture
JPEG	Joint Photographic Experts Group
JSIPS-N	Joint Service Imagery Processing System - Navy
LAN	Local Area Network
MATRIX	Modular Automatic Target Recognition For Interactive Exploitation
MB	Megabyte
MHz	Mega Hertz
MIDB	Modernized Integrated Data Base
NCTAMS LANT	Naval Computer and Telecommunications Area Master Station - Atlantic Command
NCTS - San Diego	Naval Computer and Telecommunications Station - San Diego
NIMA	National Imagery and Mapping Agency
NIS	National Input Segment
NITF	National Imagery Transmission Format
NMIC	National Maritime Intelligence Center
NMITC	Navy and Marine Corps Intelligence Training Center
NRT	Near Real Time
NSAWC	Naval Strike and Air Warfare Center
ONI	Office of Naval Intelligence
OpsCon	Operations Concept
PCO	Primary Concentrator
PEO(CU)	Program Executive Office Cruise Missiles and Unmanned Aerial Vehicles
PGM	Precision Guided Missile / Munitions

PMA281	Project Management Authority 281
PR / DR	Problem / Discrepancy Report
PRM	Product Request Message
PSM	Product Status Message
PTW	Precision Targeting Workstation
RAID	Redundant Array of Inexpensive / Independent Disks
RAM	Random Access Memory
RDS	Rapid Deployment Suite
RIC	Requirement to Image Correlation
RRDS	Reduced Resolution Data Set
SCIF	Sensitive Compartmented Information Facility
SGI	Silicon Graphics, Inc.
SIMM	Server Image Manifest Message
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedure
SPA	Strike Planning Archive
SPAWAR	Space and Naval Warfare
SSCSDD	SPAWAR Systems Center San Diego Detachment
S-VHS	Super-Vertical Helix Scan (video cassette technology)
TB	Terabyte (1,024 Gigabyte)
TBD	To Be Determined
TBR	To Be Resolved
TCF	Technical Control Facility
TCP / IP	Transmission Control Protocol / Internet Protocol
TFRD	Tape Format Requirements Document

TIC	Target to Image Correlation
USIGS	US Imagery and Geospatial Information System
VPN	Virtual Private Network
WPC	Washington Planning Center
Y2K	Year 2000

Table 7-1 List of Acronyms