Standards Profile for Image Distribution

1.0 General.

This Standards Profile for Image Distribution is one of a series of standards profiles defined for key points of interoperability within the United States Imagery System physical architecture. The profile provides definitions of applicable terminology, references, rationale, concept of operations, and identification of the specific industry and government standards necessary to allow connectivity of distributors and users' information systems for transfer of image files.

1.1 Scope.

This profile identifies the standards applicable to the electronic and low-cost media exchange of images between provider, distributor, and user within the USIS. To achieve the goal of a common exchange mechanism, image providers and distributors such as IDEX II and System III, and imagery user systems, whether COTS, GOTS or custom, shall comply with standards identified in this profile regarding connectivity (TCP / IP, FDDI), file transfer mechanisms (FTP), and electronic and low-cost media file formats (NITFS 2.0). Existing systems currently undergoing upgrades or enhancements, or new systems planned or currently in development shall be brought into compliance with this profile when and as directed by CIO.

1.2 References.

The following documents are cited in this Profile. They are delineated here to provide a consolidated listing for easy reference.

1.2.1 System Documents.

TCS-037-028/94	10 June 1994	Support Data Extensions, v1.0 for the NITF 2.0

1.2.2 ANSI and International Standards.

IEEE 802.2 (ISO 8802-2)	28 Dec 1984	Logical Link Control
X3.139 (ISO 9314-2)	5 Nov 1986	FDDI-Token Ring Media Access Control (MAC)
X3.148 (ISO 9314-1)	30 Jun 1988	FDDI-Physical Layer Protocol (PHY)
X3.166 (ISO 9314-3)	28 Sep 1989	FDDI-Physical Layer Medium Dependent (PMD)

1.2.3 DoD Standards.

MIL-STD-1777	12 Aug 1983	Internet Protocol
MIL-STD-1778	26 Aug 1983	Transmission Control Protocol
MIL-STD-1780	10 May 1984	File Transfer Protocol
MIL-STD-2500-NITF	18 June 1993	National Imagery Transmission Format (Version 2.0) for the National Imagery Transmission Format Standard

1.2.4 Internet Requests for Comments.

RFC 768	Aug 1980	User Datagram Protocol
RFC 791	Sept 1981	Internet Protocol
RFC 792	Sept 1981	Internet Control Message Protocol
RFC 793	Sept 1981	Transmission Control Protocol
RFC 854	May 1983	Telnet Protocol Specification
RFC 959	Oct 1985	File Transfer Protocol
RFC 1034	Nov 1987	Domain Names -- Concepts and Facilities

RFC 1035	Nov 1987	Domain Names -- Implementation and Specification
RFC 1042	Feb 1988	A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
RFC 1101	Apr 1989	DNS Encoding of Network Names and Other Types
RFC 1122	Oct 1989	Requirements for Internet Hosts--Communication Layers
RFC 1123	Oct 1989	Requirements for Internet Hosts---Application and Support
RFC 1155	May 1990	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157	May 1990	A Simple Network Management Protocol (SNMP)
RFC 1213	Mar 1991	Management of Information Base for Network Management of TCP/IP-Based Internets: MIB-II
RFC 1390	Jan 1993	Transmission of IP and ARP over FDDI Networks

1.2.5 NIST Implementation Agreements

NIST 500-162	Feb 1989	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 2, Edition 1, December 1988

1.3 Conformance. (TBD 001)

1.4 Test Methods. (TBD 002)

2.0 General Requirements.

2.1 Overview and Rationale.

The Image Distribution Standards Profile defines a standard interface between Image Distributors and commercial image file servers and workstations. Definition of this standards profile opens the architecture of the image distributor and allows standards-based connectivity to commercial information systems to be effected.

Section 3 defines the Image Distribution Standards Profile. The definition includes the format of the data, the methods of transporting the data to the user, and the methods of causing that data to be formatted and transferred.

The file format to be used is NITF 2.0. This format will be used across all of the image distributors. The format itself has changed to accommodate new data variations. These changes are described in NITF documentation and referenced in the Profile.

The standards defined for network connection described should be viewed as the first of a series of network-based access profiles. No single standard can support all users all the time. The standards described in the Profile (FDDI, TCP/IP, and FTP) provide the connectivity required to access an image.

It is important to recognize where in the overall architecture these standards are applied. Other standards such as NFS or Ethernet, may also play a role in the end-to-end architecture.

The underlying technology base is evolving rapidly, almost as fast as the standards selection process. The efficiency of available implementations has improved and will continue to improve over the effective lifetime of the standard. Emerging standards, such as ATM, are currently under consideration to determine the appropriate point at which to adopt the new standard as part of a Profile.

2.2 Concept.

In general, once a request for an image is received by an image distributor or provider, the image will be formatted as an NITF 2.0 file and sent either electronically via FTP, or copied to low-cost media and shipped to the recipient, as directed by the intial request. Specific examples for IDEX II and System III follow.

For IDEX, data ordering will be accomplished via the existing Host Data Base System (HDBS) attached to the IDEX facility. Images to be sent to low-cost media, to an IFS, or to a directly attached workstation will be directed to a queue dedicated to each of these. As the image is staged in IDEX, it will be converted to standard file format and distributed to the low-cost media, IFS, or workstation. IDEX-generated reference images and reduced resolution data sets can also be sent to workstations.

For System III RE-based workstations, data ordering will be done through a combination of the existing Host Data Base System channels and the System III API. The existing subimage ordering capability will be used.

An X-Window application will be used to interact with the site dissemination manager. This interaction will be done on either a HDBS terminal or workstation, or in an HDBS-controlled window visible on the workstation.

Standing and ad-hoc distributions can be defined, and images within the System III archive can also be ordered through the HDBS.

Centrally produced and distributed low-cost media-based image data can be used to support groups of workstations, or IFS/workstation combinations. For media, the data ordering mechanisms used in the near term for this concept rely on the existing nomination mechanism. A collection management terminal will be used to request that low-cost media be generated, using the existing customer and facility code mechanisms. Standing and ad-hoc distributions can be defined.

3.0 Image Distribution Standards Profile.

3.1 Basis for Definition.

This standards profile definition is driven by the goal of providing maximum interoperability between information provider systems and information user systems. In keeping with this objective, the profile definition makes data from various image distributors available to work groups and workstations of differing capabilities. It supports

a modular approach to hardware and software to allow changes to be made and to ease transition. It attempts to isolate image sources from user equipment so that changes can be made with minimal impact. The profile defines widely implemented, standard, open protocols so that commercial products from multiple vendors can be used and so that the products can easily migrate as standards and technology change. The definition of the elements which follow is based on these principles.

The data to be transferred across the image distribution interface include image pixel data, image support data, and any status and protocol messages to and from the Host Data Base System needed to support the image transfer.

3.2 Standard Interface Definition.

The image distribution standards profile definition is based on an open architecture. The image data distribution architecture is depicted in Figure 3.2-1. Image distributors will send the data across the interface to user information systems. Near-term electronically networked image distributors include IDEX II and System III. Media distribution will also be implemented. Future distributors will be added as they become available. This section describes the standard interface through which image data from both networked and media distributors will be made available.

3.2.1 Network Access Interface.

The standard network access interface provides access to data coming from the IDEX II and the System III Receive Element (RE) distributors in the near term. It is intended that future distributors in Figure 3.2-1 will also adhere to the network access standard interface as they are implemented. The standards profile is discussed in three parts: the connection element, the image transfer element, and the file format element. The connection element includes the communications aspects of the interface. The image transfer element includes the application used to send the image and its support data across the interface. The file format element includes the format of the file being transmitted, the format of the actual pixel data, and encoding.

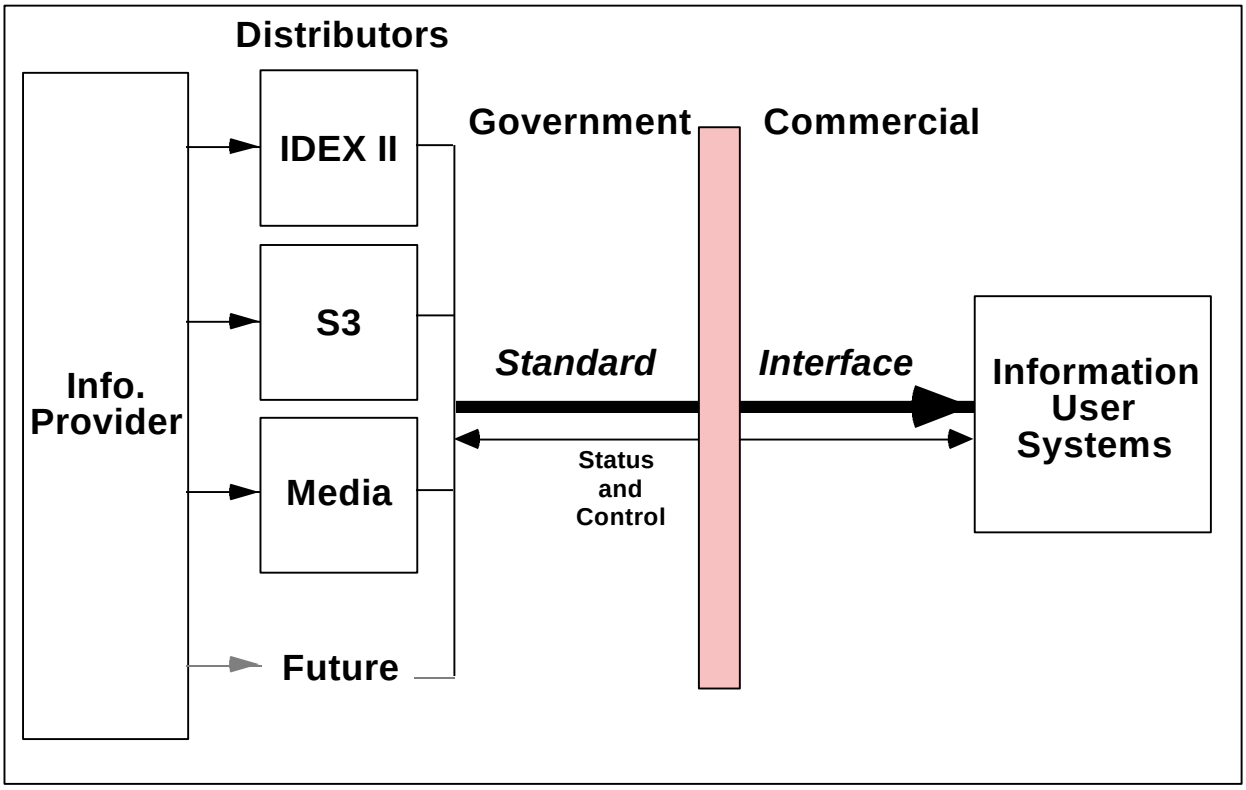

Figure 3.2-1. Image Data Distribution Architecture

3.2.1.1 Connection Element.
The connection element of the interface will provide the following services:

- Reliable stream transport to send the data defined in paragraph 3.1 across the interface.
- Routing to multiple, heterogeneous workstations and/or file servers.
- Name and address resolution for objects involved in transfer across the interface.
- Media-independent link level control.
- Multiple physical and medium access control options.

3.2.1.1.1 Transport.
The transport function will be implemented in accordance with the Transmission Control Protocol (TCP) as specified in MIL-STD-1778 and Internet Requests for Comments (RFCs) 793 and 1122. This implementation will be conditionally compliant with the applicable

portions of RFC 1122 as defined in that document. In the event of conflict among these documents, the order of precedence for resolving the conflict will be RFC 1122, first; RFC 793, second; and MIL-STD-1778, third.

3.2.1.1.2 Network.

3.2.1.1.2.1 Network and Routing Functions.

The network and routing functions will be implemented in accordance with the Internet Protocol (IP) as specified in MIL-STD-1777 and Internet RFCs 791 and 1122. This implementation will be conditionally compliant with the applicable portions of RFC 1122 as defined in that document. In the event of conflict among these documents, the order of precedence for resolving the conflict will be RFC 1122, first; RFC 791, second; and MIL-STD 1777, third.

3.2.1.1.2.2 Network Error and Control.

Network error and control functions will be implemented in accordance with the Internet Control Message Protocol (ICMP) as specified in Internet RFCs 792 and 1122. This implementation will be conditionally compliant with the applicable portions of RFC 1122 as defined in that document. In the event of conflict between these documents, RFC 1122 will take precedence over RFC 792.

3.2.1.1.2.3 Name and Address Resolution.

Resolution of names and addresses for objects on the network will conform to the Domain Name Service as specified in Internet RFCs 1034, 1035 and 1101.

3.2.1.1.3 Link Level Control.

Link level control functions will be implemented in accordance with ISO 8802-2 (ANSI/IEEE 802.2).

3.2.1.1.4 Medium Access Control.

Medium access control procedures will conform to the *Fiber Distributed Data Interface (FDDI) - Token Ring Media Access Control* Protocol (ANSI X3.139).

3.2.1.1.5 Physical.

The Physical layer of the interface will conform to the *Fiber Distributed Data Interface (FDDI) — Token Ring Physical Layer Protocol* (ANSI X3.148) and the *Fiber Distributed Data Interface (FDDI—Token Ring Physical Layer Medium Dependent* (ANSI X3.166) protocol.

3.2.1.1.6 Network Management.

Network management capabilities will be implemented by the Simple Network Management Protocol (SNMP) as defined in Internet RFCs 1157, 1155, 1213, and 768.

3.2.1.1.7 Implementation.

3.2.1.1.7.1 Implementation Agreements.

Connection element implementation will also abide by the agreements documented in the *Stable Implementation Agreements for Open Systems Interconnection Protocols* (NIST 500-162) for the standards referenced in this section.

3.2.1.1.7.2 Migration to Future Standards.

The implementation of the current standards outlined in this section will allow for a growth path to future standards, so that the higher efficiencies and performance capabilities of emerging standards can be integrated with minimal impact.

3.2.1.2 Image Transfer Element.

3.2.1.2.1 Functional Requirement.

The image transfer mechanism will provide for the transfer of the image data and image support data across the standard interface. The image data and support data may be requested by the user or prompted to be sent by another entity as described in paragraph 2.2.

3.2.1.2.2. Image Transfer Mechanism.

The mechanism to transfer imagery data across the interface will be implemented by the File Transfer Protocol (FTP) as specified in MIL-STD-1780 and Internet RFCs 959 and 1123. This implementation will be conditionally compliant with the applicable portions of RFC 1123 as defined in that document. In the event of conflict among these documents, the order of precedence for resolving the conflict will be RFC 1123, first; RFC 959, second; and MIL-STD-1780, third.

3.2.1.3 File Format Element.

The image file will contain image data, support data to assist in interpreting the image data, and other data as specified below. The file format will conform to the National Imagery Transmission Format (NITF) as specified in MIL-STD-2500-NITF, Version 2.0.

3.2.1.3.1 Header Data.

Header data will be in accordance with the NITF message header format as indicated in MIL-STD-2500-NITF, Version 2.0, Tables I and II. NITF 2.0, Tables I and II will be implemented as shown in Appendix A, Table A-I for primary data distributors.

3.2.1.3.2 Image Data.

The image data will be preceded by the image sub-header data as specified in MIL-STD-2500-NITF, Version 2.0, Tables III and IV. Data will be sent across the interface in uncompressed form. NITF 2.0, Tables III and IV will be implemented as shown in Appendix A, Table A-II for primary data distributors.

3.2.1.3.3 Support Data.

Support data will be included in the Image Extended Sub-Header Data field (IXSHD) as indicated in MIL-STD-2500-NITF, Version 2.0, Tables III, IV, XV and XVI, and Section 5.9.1.2. NITF 2.0, Tables XV and XVI will be implemented as shown in Appendix A, Table A-III for primary data distributors. Support data details are contained in the Support Data Extension document, TCS-037-028/94.

3.2.2 Media Access Interface.

Magnetic tape will be used for media-based distribution. The medium will be 8 mm and/or Super-VHS tape cartridges.[1]

Data transferred via these media will conform to the file format described in Section 3.2.1.3. Directory information will be placed on the tape as described below.

---

[1] Candidate models for the low-cost media device are the EXABYTE EXB-8500 and the Metrum RSP-2150. The Metrum RSP-2150 recorder uses "professional-grade, camera-quality, T-120 cartridges specially conditioned for digital use. The media is 900 Oe, the same energy level as that of SVHS tape media."
[—Metrum brochure]

The tape for media-based distribution will contain a number of files. The last file on the tape will be an ASCII file that contains directory information in the format described below in Table 3.2.2-1 It will consist of a line for the Tape Cassette ID Record and a line for each data file for the Per File Record. A line is a string of ASCII characters terminated by 'CR-LF' [0D-0A (hex)]. The files will be listed in the directory file in the same order that they are stored on the tape. Files are separated by file marks. Two file marks will be used to indicate the end of the tape.

FIELD	**SIZE (BYTES)**	**FORMAT**
TAPE CASSETTE ID RECORD:		
ORIGINATING STATION ID	10	ASCII CHARACTERS
DATE OF CREATION	6	YYMMDD
TIME OF CREATION	4	HHMM
NUMBER OF FILES	6	ASCII CHARACTERS
PER FILE RECORD		
IMAGE ID	64	FILE NAME
SECURITY CLASSIFICATION	1	T, S, C, R or U
CODE WORD	40	ASCII CHARACTERS
SIZE OF FILE	12	0-999999999999 (BYTES)
PHYSICAL LOCATION START	40	MEDIUM-SPECIFIC CODE (TRACK #, BLOCK #, ETC.)
PHYSICAL LOCATION END	40	MEDIUM-SPECIFIC CODE (TRACK #, BLOCK #, ETC.)

TABLE 3.2.2-1 TAPE DIRECTORY FORMAT

4.0 Security Implications.

The implications of security on an evolving work group architecture need to be determined based on the changes made to the existing information processing environment and the existing requirements documentation.

4.1 Basic Image Handling Security Perspectives.

The image handling functionality can be viewed as a suite of hardware and software to be added to an existing environment. The addition of image handling functionality to an

exploitation facility does not alter the global sense of activities or operational missions that are performed—only the tools used to execute the intelligence analysis process will change.

The existing imagery user environment includes security policies and directives that discretely govern how the analysis procedures must be executed when handling sensitive and classified material. The operational environment consists of equipment, procedures, and work flow processes. Each operational environment such as an operational location or facility is likely to have different security policies and directives. The security policies strive to achieve similar goals, however, differences in site characteristics drive the various security policies away from consistency. Tools, such as image handling capability, used as part of imagery analysis procedures, are executed within the environment governed by the security policies and directives.

Image handling capability is therefore subject to the constraints of the security policies but only through the operational environment in which image handling is to be deployed. In most cases, the security constraints applied to the process of imagery exploitation already exist for each candidate image handling installation. Therefore, softcopy image handling applications need not have additional requirements for upholding security policy, but image handling applications are responsible for not violating that existing set of governing security policies.

4.2 Typical Sources of Security Constraints.

Further insight to the basis of many security policies likely to be found at image handling candidate locations can be found in documents such as DCID 1/16, NACSIM 5100, DoD 5200.28-STD, and DoD Manuals 50-3 and 50-4. Most operational facilities will also have supplemental security policies documentation that further refines the security policy based on the aforementioned reference documents. The supplemental site-specific security policies may levy additional constraints or call for waivers to the standard security concepts.

System design and architectural guidelines for a specific site or organization may also drive supplemental security policies. System architects often address the cost trade-offs between strict security implementations and risk minimization through system design and architecture. An image handling implementation may therefore be constrained by

organizations' architectural preferences (mandates) for the purpose of compliance with security policy.

Other security guidelines, e.g., publications such as NSA's "Orange Book," permit flexibility in security policy based on levels of certification and perceived risk of information disclosure. The "perceived risk evaluation" for the compromise of data within a specific site is frequently rated with a zone of control. The security mechanisms that govern the zone of control rating for a facility include forced entry protection, perimeter control, physical structure, armed guards, electronics emissions, EMI evaluation of the facility, location and type of equipment and electronic surveillance. These elements are just a few security mechanisms that may be considered as part of an overall security plan and policy to protect sensitive information. An image handling installation must operate within the established security policies and boundaries that describe the security operations for a given site.

Along with zoned control, security organizations also typically rate data processing systems and networks at two levels of automated data handling integrity. The two levels, "system high" and "compartmented" implemented at a specific site, are driven by the complexity and National security sensitivity of the data that is processed and by the technology available. Compartmented modes of automated information systems management significantly raise the cost of system implementation due to present technology limitations. Although compartmented modes of system operation permit the management of a variety of dissimilar information classifications, many security organizations select a system high mode of security operation for their information processing systems. The system high mode dictates only one level of security classification be maintained for a given system and associated users and considers all data to be handled as if they were classified at the highest level of any single data item. The single security classification level is easier to manage with the present technology and hence is less costly. Not all security organizations treat their classified data handling systems congruently and are willing to invest resources to treat sensitive data in a compartmented mode of operation. Therefore, the image handling functionality will likely be deployed in both system high and compartmented security environments.

Glossary

Application Program Interface. An Application Program Interface is the interface between the application software and the application platform, across which all services are provided. The application program interface is primarily in support of application portablility, but system and application interoperability are also supported by a communication API.

Archive. An Archive is a data storage system that maintains a large volume of historical data for access by information users. Archive sites are typically established on a distributed basis so that many users can access the stored data. An imagery archive consists of imagery and imagery support data, including standard directory elements, that allow users to retrieve imagery responsive to their queries.

Commercial Off-The-Shelf. Commercial Off-The Shelf characterizes a commercial, available, supported product that is offered for sale, by a vendor. Commercial products are developed to meet perceived or actual market requirements. Product development and evolution are typically funded through the company's research and development budget and revenues derived from selling and supporting the product, respectively.

Commercial Workstation. A Commercial Workstation is a general-purpose, high-performance, desk-top computer that can be configured with application software (and hardware add-in boards) to meet the needs of a class of end-users, such as imagery analysts. Commercial and government off-the-shelf products are selected to provide the required functionality. However, custom-developed software may be necessary to fill gaps in functionality. A commercial workstation (as a multi-application platform) is differentiated from an application-specific workstation which can only be used as a part of the system to which it is connected.

Cooperating Application Software. Cooperating Application Software is application software which, through application program interfaces, can transparently exchange data and services. Cooperating software reduces the need for monolithic applications that perform all necessary functions internal to themselves.

Data Storage System. A Data Storage System identifies any system that can store data and provide users access to the data. Data storage systems may be large or small, central, distributed, or local. Hard disks in workstations, work group file servers, and image provider archives are all examples of data storage systems. For the data storage system to be useful to a large community of users, standard data formats, query mechanisms and responses to queries must be provided.

Dissemination. Dissemination is a process by which digital data is electrically or physically delivered to a specific group of users against a standing profile of the users'

information requirements or users' ad hoc requests. Electrical dissemination systems also serve as image data distributors. The dissemination system is neither the provider nor the end-user of the image data, yet in addition to dissemination, it may provide on-line storage, some image processing, archives, and access to the information provider (whether physical or logical). The existing primary dissemination system provides near-original quality imagery in near-real-time, for both hardcopy and softcopy exploitation. In the future, the system architecture will evolve to provide for modular Receive Elements with image file server functionality. The next-generation Receive Elements will offer a standard interface for connectivity and file format standards defined in this Profile.

Distributed Architecture. A Distributed Architecture characterizes a computer architecture that uses processing and data storage systems that are not exclusively centralized. The degree to which the elements are distributed depends on the needs of the users that the information system supports. Elements of a distributed architecture may be distributed throughout a building or on a world-wide, geographic basis.

Government Off-The-Shelf. A description which characterizes a government-funded, available, supported, product which is offered for use within the government, typically to address horizontal aspects of a particular discipline. Government off-the-shelf products are developed to meet the specific requirements of a class of users, e.g. imagery analysts. Government-developed products typically require functionality which cannot be obtained in commercial off-the-shelf products because the market is too small to justify the development, the functionality is too government-specific, or the application and/or data is classified. Product development and evolution are typically funded through the government's research and development budget.

High Performance Media (TBD 003)

High Performance Media Device. A High Performance Media Device is a magnetic media reproducer/recorder that can be used to distribute large volumes of data, e.g. image data, to imagery information systems. Typically, a High-Performance Media Device would be an input to a data storage system, such as a file server or archive. Its performance would be such that large files could be rapidly retrieved from the media. High-Performance Media Devices are necessary when high-bandwidth networks are not available for direct distribution of data to data storage systems.

IDEX II. IDEX II (Image Data Exploitation) is a softcopy exploitation system, developed by a joint program office, to meet community needs for a high-performance, digital image processing and display system for National imagery. IDEX II consists of mostly custom-developed hardware and software. Because of its capabilities, and geographically distributed sites it supports, IDEX II is a defacto component of a distributed imagery architecture which makes use of second-tier image data distributors. An image data interface is the gateway through which workstations will gain access to image data stored in IDEX II archives. The interface consists of the hardware and software necessary to

convert IDEX-specific (non-standard) protocols and formats to those which adhere to the standards identified in this Profile. The interface provides the capability for a commercial workstation to request and receive image data directly from IDEX or through an image server that receives its data from IDEX. Once the image data has been received, the workstation is free to access and manipulate it without intervention by IDEX**.**

Image Data Distributor. An Image Data Distributor is an element of a distributed architecture which provides image distribution services to network-connected and standalone commercial workstations and other devices. An Image Data Distributor is an imagery information system that, though it did not create the data, appears to be the source of image data to the end-user of a workstation. The IDEX II softcopy exploitation system, and System III Receive Elements are examples of image data distributors.

Image Distribution. Image distribution is a subset of the dissemination process whereby imagery that is maintained by image information providers or distributors is transferred from government-specific systems to commercial image file servers (or workstations with file server functionality) in compliance with the standards defined in the Standards Profile for Image Distribution.

Image File Server. An image file server (IFS) is a device that can accept image data from an image distributor or media device for eventual access by any or all workstations in a given work group.

Image Support Data. Image Support Data is data necessary to make image data useful to an imagery user or imagery information system. Image Support Data characterizes the image data against a standard set of parameters.

Imagery Information System. An Imagery Information System is any computer or set of computers that have the capability to store, process, display, and output imagery and imagery-derived products.

Information Provider. An Information Provider is an organization that creates or produces and maintains information for use by those who need the information to perform their task (information users). Information providers create and maintain new information on a timely basis, retain and provide access mechanisms to historical information, provide ordering and order status mechanisms to users, and provide delivery of the required information either electrically or via media. In the context of Standards Profile for Image Distribution, the central image data processing facility is considered the image information provider. All other systems are considered second-tier image data distributors.

Information User. An information user is any organization, system, or individual that requires information from a provider ~~(~~or distributor~~)~~ to perform their required tasks or mission.

Interconnectivity. The ability of two or more information systems to establish communications via point-to-point links or internetworking. Interconnectivity provides the capability for access to one system by another, but does not guarantee interoperability.

Interoperability. The ability of two or more systems to exchange information and to mutually use the information that has been exchanged.

Key Point of Interoperability. Specific points in the United States Imagery System architecture where access to data and services is provided between systems by establishing profiles which define a standard interface.

Local Area Network. A Local Area Network is the lowest level in a set of hierarchical networks. A Local Area Network is one which supports a single work group or several work groups within an organization or facility. Local Area Networks are typically based on commercial products that adhere to industry communications standards.

Low-Cost Media. Low-Cost Media is magnetic media used to store and distribute large image files (or portions thereof) directly to standalone commercial workstations or work group image file servers that support a small number of users. Though the media supports relatively high data storage capacities, and is relatively affordable, i.e. 8 mm or 1/2" cassettes, these media do not support high read/write performance.

Low-Cost Media Device. A Low-Cost Media Device is a commercial tape recorder/reproducer which handles Low-Cost Media.

Metropolitan Area Network. A Metropolitan Area Network is the middle level in a set of hierarchical networks. It generally services multiple organizations or facilities within a given geographic area, and may even service subscribers in an entire city or county. This level of network provides gateways to other distant networks.

National Exploitation Laboratory. The National Exploitation Laboratory, or the NEL, is an organization within the National Photographic Interpretation Center, that studies, analyzes, and evaluates the imagery exploitation process and its associated tools such as workstations, applications, and other commercial products. The NEL serves as a clearinghouse for Community requirements associated with softcopy exploitation.

National Image Transmission Format. The National Image Transmission Format, or NITF, is a standardized format for the transmission of National imagery. Originally applied only to the transmission of small images by Secondary Dissemination Systems, NITF now accommodates large images, and all associated support data for transfers of imagery from image distributors to user information systems.

Network-Connected Workstation. A Network-Connected Workstation is one that is electrically connected to a Local Area Network, thus being capable of sharing resources

with other workstations on the network. A Network-Connected Workstation can receive imagery from an image file server on the network.

Profile. A set of one or more base standards and, where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards necessary for accomplishing a particular function.

Receive Element. A Receive Element performs image dissemination functions to network-connected and standalone workstations by providing image file services and low-cost media generation, respectively.

Softcopy Exploitation. Softcopy Exploitation involves imagery display, processing, data extraction, and reporting that makes use of workstations for display of digital imagery.

Stand-alone Workstation. A Stand-alone workstation is a workstation that is not connected to a network. It receives data, such as digital imagery, on magnetic media. Correspondingly, any products generated by the workstation would be media-based. The media are read and written directly by the workstation.

United States Imagery System. The name given to the set of interoperable, existing and planned imagery collection, processing, distribution, and exploitation assets that support National, Strategic, and Tactical missions as part of a unified architecture. The United States Imagery System will be an open system environment to allow data and service sharing among its participating information providers and information users.

User Information System. A User Information System is any computer system that is owned and operated by the user or their parent organization. The System supports the mission and tasks of the individual or organization. User Information Systems connect to Metropolitan Area or Wide Area Networks to receive data from Information Providers or Distributors.

Wide Area Network. A Wide Area or Global Network allows connection of a diverse set of world-wide users for the purpose of information interchange. The Wide Area Network is the highest level in a set of hierarchical networks. Wide Area Networks connect to Metropolitan Area Networks—both of which are typically provided by common carriers (commercial network service providers).