Space Communications Protocol Standards

(SCPS) Project

Joint NASA/DOD

Space Mission Requirements Study

OCTOBER 1993

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

The use of standards provides a means to achieve benefits in the life cycle cost of space programs. These benefits include cost and schedule reductions in the areas of systems development, testing, integration, operation, maintenance and upgrade. Several functions, traditionally performed with heavy reliance on human intervention, may be able to be both automated and standardized across civil and military space systems. In addition, standards will facilitate interoperability between systems that are required to communicate with each other. As a pilot project to formally explore the potential of this common standardization, USSPACECOM and NASA have undertaken a joint effort in the area of space data communications. This effort attempts to (1) determine the feasibility of establishing common standards across civil and military space systems, (2) define specific standards that will meet the requirements and constraints of space systems in both communities, (3) have such standards adopted by national and international standards bodies, and (4) deploy implementations of such standards in civil and military space systems.

This technical report documents the requirements identification and assessment work performed to date in support of this task. The remainder of this document is structured as follows. Section 2 presents an overview of the task as well as the technical approach undertaken to accomplish the entire task. The next section describes the requirements assessment process. Section 4 briefly summarizes work based on the common requirements. Finally, section 5 provides conclusions and recommendations.

THIS PAGE IS INTENTIONALLY BLANK

SECTION 2

TASK OVERVIEW

2.1 PURPOSE AND SCOPE

The purpose of this task is to establish data communications standardswhich are common to U.S. civil and military space systems. This standardization is expected to be a means to achieve benefits in the life cycle cost of space programs. These benefits include cost and schedule reductions in the areas of systems development, testing, integration, operation, maintenance and upgrade. Also, several functions, traditionally performed with heavy reliance on human intervention, may be able to be both automated and standardized across civil and military space systems. In addition, standards will facilitate interoperability between systems that are required to communicate with each other. This will provide, in turn, flexibility to the U.S. government in the deployment of space systems.

As a pilot project to formally explore the potential of this common standardization, United States Space Command (USSPACECOM) and National Aeronautics and Space Administration (NASA) have undertaken a joint effort in the area of space data communications. From a technical perspective, this task addresses asynchronous data communications where the data is in digital form, including the digital representation of voice and video; however, voice and video communications requiring isochrony (constant time between data samples) are outside its scope at this time. Furthermore, this task addresses end-to-end communications of space-based systems, involving the entire space segment and that portion of the ground segment involved with data communications to/from space vehicles. Issues such as physical channel/data link techniques and protocols are outside the scope of this task. The above end-to-end communications will support both mission independent (platform) and mission dependent (payload) space applications. Examples of mission independent applications are space vehicle telemetry, space vehicle commanding, and the transfer of program and data tables between the ground and space vehicles. Examples of mission dependent applications are remote sensing and weapons control.

From a programmatic perspective, the standards produced through this task are intended to apply to both new systems and those systems undergoing a major upgrade. Systems will be expected to incorporate such standards only if they are not yet past the System Requirements Review (SRR) milestone in the acquisition cycle at the time that the standards are initially approved by the respective space communities.

2.2 APPROACH

A three phase technical approach has been adopted to accomplish this task. Phase I is exploratory in nature and consists of initial work to determine the degree to which it is operationally and technically feasible to standardize data communications across civil and military space systems. Phase II involves the development and validation of space data communications standards that can be applied to both civil and military systems. Phase III consists of protocol deployment into these space systems.

Two groups have been established as the means to perform the task. The first group, the Space Communications Protocol Standards Technical Oversight Group (SCPS TOG), provides community oversight. It has the authority to approve the degree to which common standardization should be pursued as well as the specific standards and profiles to be developed. All U.S. civil and military space organizations are eligible to be represented in the SCPS TOG. The second group, the SCPS Technical Working Group (TWG), is a technical arm of the SCPS TOG and, as such, defines and implement the technical approach outlined above. This group consists of technical experts selected by USSPACECOM and NASA. The technical progress achieved by this group is periodically presented to the SCPS TOG for review and approval. Several organizations have participated in the SCPS TWG. The participating military organizations have been USSPACECOM including the Air Force and Navy components, Defense Information Systems Agency (DISA), National Security Agency (NSA), Rome AF Labs, Space & Missile Center (SMC), United Kingdom Defense Research Agency (DRA), MITRE, and space contractors. The participating civil organizations have been NASA, Jet Propulsion Laboratory (JPL), MITRE, a university, and space contractors.

The exploratory phase, phase I, was completed during FY93. Two teams were formed to carry out this phase: the Requirements Gathering/Assessment Team (RGAT) and the Capabilities Survey/Analysis Team (CSAT). The RGAT collected pertinent system requirements and determined the functional protocol requirements common to civil and military systems. The CSAT investigated the protocol capabilities of current standards as potential candidates to fulfill the common requirements. The RGAT identified 30 protocol functional requirements for space systems and found that, based on the analysis of four civil and three military missions, 28 (93%) are common to both civil and military systems. These requirements can be categorized as follows: (a) file handling, including the loading/upgrade of software programs/data-tables into space vehicles; (b) end-to-end reliable delivery across many transmission paths; (c) end-to-end data protection, providing the security and integrity of messages; and (d) networking, the routing and addressing of messages on an end-to-end basis through the space/ground network. In addition, a conceptual protocol stack was derived to support the common protocol requirements. The CSAT proposed standards to meet the protocol requirements established by the RGAT. Based on results of the work of these two teams, the SCPS TOG approved the continuation of this task beyond FY93.

Phase II of the technical approach was started in FY94. The requirements work has been expanded to include the collection of detailed operational scenarios (including work loads), system parameters and user performance requirements for each of the systems surveyed during Phase I. From this data, performance-oriented protocol requirements will be generated. Also, additional systems are planned to be surveyed and analyzed. Concurrent with the requirements effort, the development/validation of the standards proposed in Phase I was started. This is being accomplished by the specification, simulation, and implementation (hardware and software) of the proposed standards.

A systems engineering approach was developed and is being used to guide and evaluate the development/validation work. The objective of this approach is to ensure that the resulting standards meet both the functional and performance requirements of both military

and civil space systems. As a means to assess the standards, a testing program, technical reviews and user demonstrations will be conducted. The test program includes the following: (a) validating the protocol specifications according to DISA procedures, (b) verifying that the simulations and prototype implementations properly represent the protocols and the space environment, and (c) determining if the resulting implementations meet the functional and performance system requirements. These requirements will be verified in laboratory, ground environment (emulating the space environment), and space environment test beds in an incremental way. The latter test beds include a bent-pipe satellite configuration as well as a configuration where the protocol implementations reside onboard a satellite. This building block approach to testing minimizes both cost and technical risk because it allows problems to be discovered and corrected prior to committing to the operational deployment of the standards.

During this phase government/industry workshops will be held where the government formally introduces this task to the commercial community for the purpose of technology disclosure and the solicitation of comments. The products of this phase will be both DOD and NASA standards which will be submitted to US/international standards bodies for their approval.

During Phase III the US/international standards bodies are expected to finalize the formal approval of the standards. Concurrent with this approval process the following is planned: (a) the implementation (software code) generated in Phase II will be made available to contractors/vendors that wish to start building implementations of the standards, (b) support will be provided toward the development of conformance and interoperability tests which will be used to evaluate the contractor/vendor implementations, and (c) assistance will be provided to specific programs toward the incorporation of these standards in their hardware/software environments.

THIS PAGE IS INTENTIONALLY BLANK

SECTION 3

REQUIREMENTS ASSESSMENT

3.1 INTRODUCTION

The purpose of the requirements assessment is to determine (1) protocol functional requirements and (2) a conceptual protocol stack common to civil and military space systems.

This section presents the process involved in identifying both the protocol functional requirements and the conceptual protocol stack as well as the results to date.

3.2 PROCESS DESCRIPTION

The process followed to identify common protocol functional requirements and a conceptual protocol stack is shown in Figure 1. The process steps are as follows: (1) conduct a survey of both civilian and military space missions, (2) for each mission identify the system functional requirements that affect end-to-end data communications, (3) determine the required data communications services (DCSs), (4) analyze the DCSs to identify those that can be implemented via protocols (i.e., the protocol functional requirements), (5) determine the set of these protocol requirements which are common to both civil and military systems (these are the common protocol functional requirements), and (6) generate a generic protocol stack that best supports these common requirements.

3.2.1 Missions Surveyed

The missions surveyed were selected based on consultation with both USSPACECOM and NASA personnel. The NASA missions are (1) the Goddard Space Flight Center (GSFC) missions, including the Small Explorer, the X-ray Timing Explorer (XTE), and the Earth Observing System (EOS), and (2) the Space Station Freedom (SSF). The SSF has been recently renamed SpaceStation Alpha; however, the term SSF will be used throughout the rest of this document. The DoD missions are (1) the Ballistic Missile Defense/Brilliant Eyes (BMD/BE) system, (2) the Global Positioning System (GPS), and (3) the Defense Meteorological Satellite Program (DMSP). These DoD missions are briefly described below.

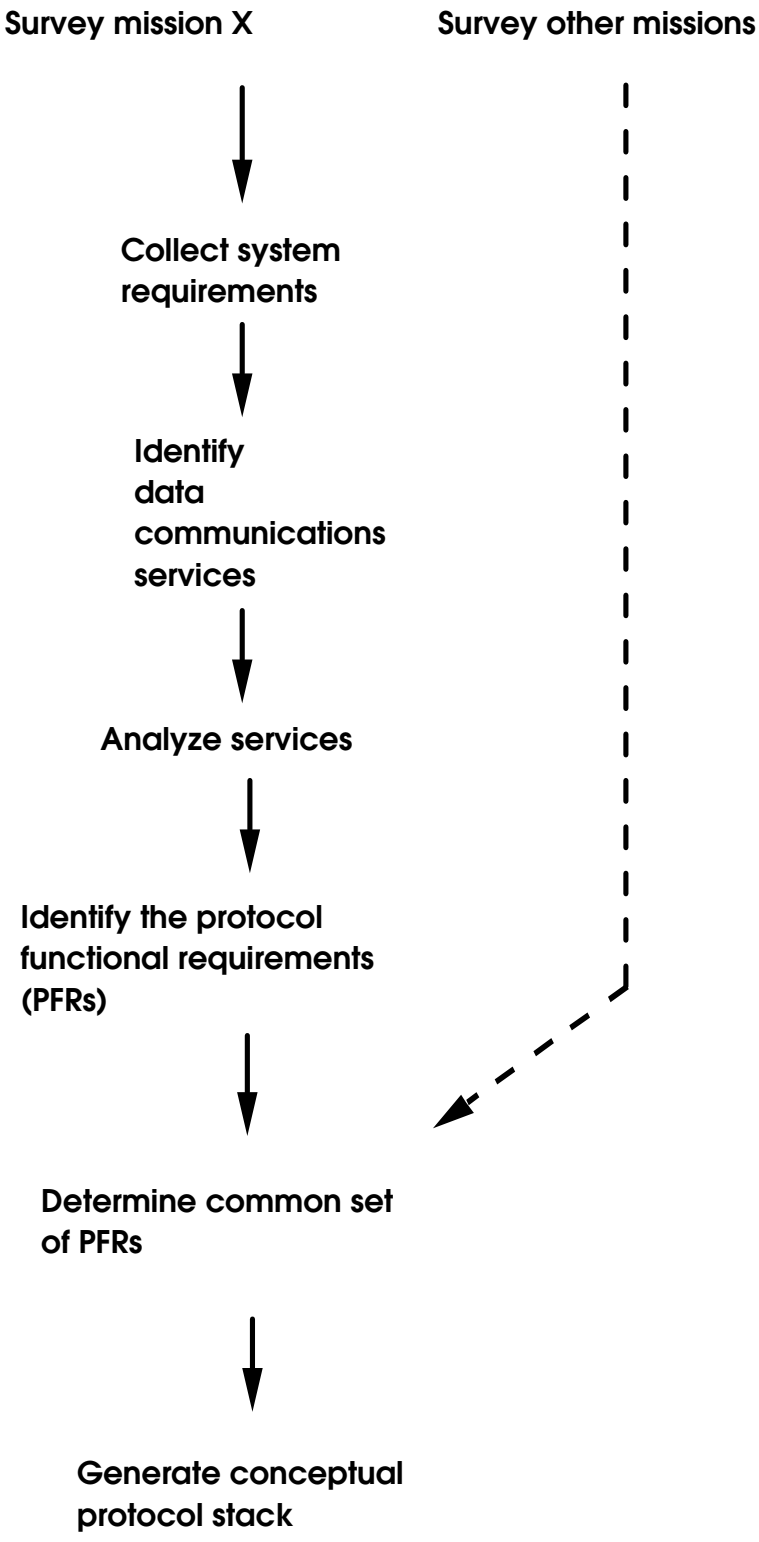

Figure 1 – Process Flow

3.2.1.1 Ballistic Missile Defense/Brilliant Eyes

BMD/BE is a space based surveillance element which provides global surveillance access to boosters, post-boost vehicles (PBVs) and deployed midcourse objects in response to directed tasking. BE provides a capability to monitor missile launch locations within designated regions for early launch notification; it may also be used as a launch confirmation source during the boost phase on a global basis. BE surveillance data is provided to the command and control element throughout the boost, post-boost and midcourse phases for engagement planning, to support kill assessment and midcourse object discrimination. BE will provide, on a noninterference basis, surveillance to support collateral mission areas.

BE consists of four segments: space, ground, launch and support. The space segment consists of a distributed constellation of low altitude satellites with taskable infrared and visible sensors to collect surveillance data against boosters, PBVs, and deployed midcourse objects. The ground segment contains the element command and control function. The launch segment includes launch vehicles, facilities, and hardware/software to place the satellites in orbit. The support segment provides all integrated logistics support.

3.2.1.2 Global Positioning System

The Navstar GPS is a space-based radiopositioning, velocity, and time-transfer system that has three major segments: space, control and user. The GPS concept is predicated upon accurate and continuous knowledge of the spatial position of each satellite in the system with respect to time and distance from a transmitting satellite to the user. Each satellite transmits unique ephemeris (positioning) data. This data is periodically updated by the master control station via four remote ground antennas based upon information obtained from five widely dispersed monitor stations. The GPS receiver makes time-of-arrival measurements of the satellite signals to determine the distance from the user to the satellites. These distance calculations, along with range rate information, are combined to yield system time and the user's three dimensional position and velocity with respect to the satellite system. A time coordination factor then relates the satellite system to Earth coordinates.

3.2.1.3 Defense Meteorological Satellite Program

DMSP is a space-and-ground-based system used for collection and timely dissemination of global environmental data to DoD and other government agencies. This data consists of visible and infrared cloud cover and other specialized meteorological, oceanographic, and solar geophysical information required to support DoD worldwide operations. DMSP is composed of (1) the space segment, (2) the Command, Control, and Communications Segment (C^3S), and (3) the user segment.

The principal function of the space segment is to continually acquire environmental data through its satellite sensors. This data is stored onboard the satellites for delayed transmission to the C^3S. Subsequently the data is relayed to strategic elements of the user segment for processing and analysis. Real-time environmental data can also be transmitted directly from the space segment to tactical elements of the user segment. The DMSP space

vehicles are placed into a near-circular sun-synchronous polar orbit at a nominal altitude of 450 miles.

The C^3S conducts all mission planning, generates real-time and stored program commands, provides computer memory uploads to the space segment, and handles telemetry acquisition, processing and postpass analysis.

The user segment consists of Air Force Global Weather Central (AFGWC), the Navy Fleet Numerical Oceanography Center (FNOC), and the tactical terminals. These terminals receive DMSP mission data in real time. The AFGWC is the primary strategic user and distributor of DMSP satellite data destined for the Air force and Army. The FNOC distributes DMSP data to the Navy and Marine Corps.

3.2.2 System Requirements

System requirements pertinent to end-to-end space data communications were collected for each of the above missions. Requirements were collected in the following categories: (a) space applications that need to be supported, (b) data exchange scenarios and (c) data communications services. The following space applications were addressed: (1) space vehicle telemetry, (2) space vehicle commanding, (3) program and data tables transfer, (4) mission (payload) data collection and reporting, and (5) mission control commanding. Three data exchange scenarios were included: ground source to space destination(s), space source to ground destination(s) and space source to space destination(s). A total of 30 data communications services within the following four service categories were addressed: (1) file handling, (2) end-to-end data transfer (transport), (3) end-to-end data protection, and (4) networking. The system requirements collected for each DoD mission appear in the first section of Appendixes A, B and C, respectively.

3.2.3 Analysis of Data Communications Services

The 30 data communications services were analyzed for each surveyed mission to determine those that can be implemented via standardized data communications protocols. See Figure 2 for the analysis method. The are three levels of analysis for each service. The first level determines whether or not the service is currently performed at all by a mission. The second analysis level is as follows. For a performed service, determine whether or not the service is implemented via data communications protocols. For a service not performed, determine whether or not the service would be performed if the means were provided. The third analysis level determines whether or not it is practical to implement the service via protocols. As a result of the above analysis, a decision is made as to whether or not protocol standardization is applicable to the service. See 3.3.1 for the analysis results.

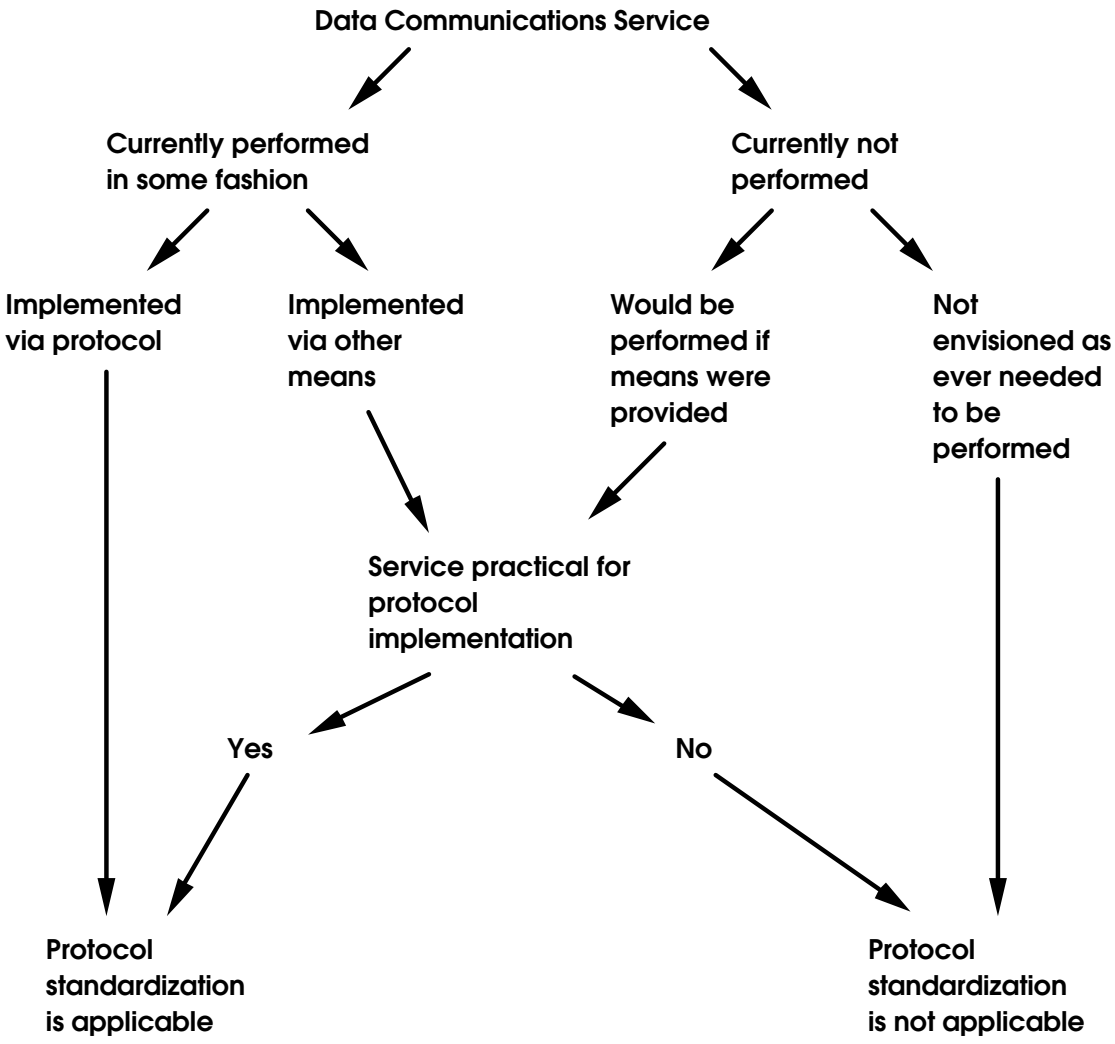

Figure 2 – DCS Assess Flow

3.3 RESULTS TO DATE

This section documents (1) protocol functional requirements common to civil and military systems, and (2) the conceptual stack that supports these requirements.

3.3.1 Identification of Protocol Functional Requirements

The results of the detailed DCSs analysis for each DOD mission surveyed appear in Appendixes A.2, B.2 and C.2. Figures 3-5 show a summary of the analysis results for these missions. This shows that all the DCSs can be implemented via protocols. Therefore, there are 30 protocol functional requirements. In addition, it further shows that at least 97% of the 30 DCSs can be standardized via data communications protocols in each individual mission.

Table 1 shows those data communications services common to both civil and military missions. This is the set of common protocol requirements. The criteria for categorizing a

service as common is that such service is applicable for protocol standardization in at least 3 of 4 civil and 2 of 3 military missions. Of the 30 services, 28 fulfill (and all exceed) this criteria. Therefore, common protocol functional requirements exist in 93% (28 out of 30) of the cases. A set of standard protocols, common to civil and military systems, can be developed to implement these common requirements.

Based on the DCSs analysis, there are 30 DOD protocol functional requirements (PFR) identified in four categories are as follows: (a) file handling, including the loading/upgrade of software programs/data-tables into space vehicles; (b) end-to-end reliable delivery across many transmission paths; (c) end-to-end data protection, providing the security and integrity of messages; and (d) networking, the routing and addressing of messages on an end-to-end basis through the space/ground network. Of those 30, 28 are common requirements with NASA. The functional requirements under each of the above categories are listed below. Each of the 30 requirements is uniquely identified by a letter and a number. A definition of each functional requirement is provided in the next paragraph.

A. File handling

- F.1: Operations on entire files
- F.2: Operations on file records (portion of a file)
- F.3: Two-party file transfer
- F.4: Proxy file transfer
- F.5: User-initiated interrupt and abort
- F.6: System-detected interrupt notification
- F.7: Resumption after interrupt
- F.8: Integrity over operations on entire files
- F.9: Integrity over operations on file records
- F.10: File handling security

B. Transport

- Delivery reliability
  - T.1: Full
  - T.2: Best-effort
  - T.3: Minimal
- T.4: Multicasting (with minimal reliability)
- T.5: Precedence handling
- T.6: Segmentation
- T.7: Operation over wide range of constraints
- T.8: Graceful closing of connections
- T.9: Different response to congestion and to corruption

C. Data protection

- P.1: Access control
- P.2: Source authentication
- P.3: Command authentication
- P.4: Integrity
- P.5: Confidentiality

D. Networking

- N.1: Support for multicasting
- N.2: Support for multiple routing options
- N.3: Packet lifetime support with automatic duplicate discard
- N.4: Separate reporting of congestion and corruption
- N.5: Support for precedence handling
- N.6: Differentiation between real and exercise data

3.3.2 Definition of Protocol Functional Requirements

A. File Handling

The functional requirements for the transfer of data files between end points within a space data communications system are stated below. Requirement F.4 is a DOD-requirement; it is not a NASA requirement. The remaining requirements are both DOD and NASA requirements.

Requirement F.1: Operations on entire files

The SCPS file handling protocol:

F.1.1: Shall provide the capability to rename files.

F.1.2: Shall provide the capability to delete files.

If a file directory structure is present in the file system, then the SCPS file handling protocol:

F.1.3: Shall provide the capability to create a directory.

F.1.4: Shall provide the capability to delete a directory.

F.1.5: Shall provide the capability to change the current working directory.

F.1.6: Shall provide the capability to list the names of files in a directory.

Requirement F.2: Operations on file records

The SCPS file handling protocol:

F.2.1: Shall provide the capability to read and extract any record or set of records within a file.

F.2.2: Shall provide the capability to insert a record or set of records into any location within a file, where location means at the beginning of a file, at the end of a file, or between other records of a file.

F.2.3: Shall provide the capability to replace (overwrite) any record or set of records within a file.

F.2.4: Shall provide the capability to delete any record or set of records within a file.

Requirement F.3: Two party file transfer

The SCPS file handling protocol shall provide the capability for either of two end systems to send and receive a complete file.

Requirement F.4: Proxy file transfer

The SCPS file handling protocol shall provide the capability for either of two end systems to send and receive a complete file under the control of a third end system.

Requirement F.5: User-initiated interrupt and abort

The SCPS file handling protocol:

F.5.1 (Manual Interrupt): Shall provide the capability for the user to cause an interrupt of a file transfer after the start but before the completion of the transfer.

F.5.2 (Manual Abort): Shall provide the ability for a user to terminate a file transfer after the start but before the completion of the transfer. An aborted file transfer cannot be resumed.

Requirement F.6: System-detected interrupt notification

The SCPS file handling protocol:

F.6.1 Shall recognize a notification which identifies that the communications supporting a file transfer has been interrupted. This notification is sent by a lower layer (e.g., the transport layer).

F.6.2 Shall act upon this notification (see F.7.2)

Requirement F.7: Resumption after interrupt

The SCPS file handling protocol:

F.7.1 (Manual Resume): Shall provide the capability to manually resume a file transfer from the point of interruption for manual interrupts and automatically detected interrupts.

F.7.2 (Automatic Resume): Shall provide the capability to automatically resume a file transfer from the point of interruption for automatically detected interrupts.

Requirement F.8: Integrity over operations on entire files

The SCPS file handling protocol shall have the capability to preserve the integrity of operations on entire files. Integrity of operations is defined to mean that the operation performed is the same as the operation requested, and that an operation is not performed upon detection of an error by the file handling protocol.

Requirement F.9: Integrity over operations on file records

The SCPS file handling protocol shall have the capability to preserve the integrity of operations on file records. Integrity of operations is defined to mean that the operation performed is the same as the operation requested, and that an operation is not performed upon detection of an error by the file handling protocol.

Requirement F.10: File handling security

The SCPS file handling protocol:

F.10.1 (User Access): Shall provide the capability to restrict user access to the functions of the (file handling) protocol.

F.10.2 (File Access): Shall provide the capability to prevent unauthorized access to files.

B. Transport

The functional requirements for providing reliable transfer of data between end systems within a space data communications system are stated below. All requirements are both DOD and NASA requirements.

Requirement T.1: Full reliability

Provided that there is end-to-end link availability and sufficient link capacity for retransmissions, the SCPS transport protocol:

T.1.1: Shall provide the capability to deliver *all* data segments to the correct destination(s), as addressed at the source.

T.1.2: Shall provide the capability to deliver *all* data segments in the same order as originated at the source, with no duplicate or extraneous data.

T.1.3: Shall provide the capability to deliver *all* data segments for which there are *no* detected errors.

T.1.4: Shall provide the capability to recover from detected data transmission errors.

The full reliability requirement appliesto the unicast communications mode only (it does not apply to multicast).

Requirement T.2: Best effort reliability

Provided that there is end-to-end link availability, the SCPS transport protocol:

T.2.1: Shall provide the capability to deliver data segments to the correct destination(s), as addressed at the source.

T.2.2: Shall provide the capability to continue to deliver data segments to the correct destination(s), irrespective of the loss of a subset of the data segments.

T.2.3: Shall provide the capability to deliver data segments in the same order as originated at the source, with *no* duplicate or extraneous data.

T.2.4: Shall provide the capability to deliver data segments for which there are *no* detected errors.

The best effort reliability requirement applies to the unicast communications mode only (it does not apply to multicast).

Requirement T.3: Minimal Reliability

The SCPS transport protocol:

T.3.1: Shall provide the capability to deliver transmitted data segments to the correct destination(s), as addressed at the source, with no guarantee of (a) order, (b) completeness, or (c) elimination of duplicates.

T.3.2: Shall provide the capability to deliver data segments for which there are *no* detected errors.

The requirement for minimal reliability applies to both the unicast and multicast communications modes.

Requirement T.4: Multicasting

The SCPS transport protocol:

Shall provide the capability to deliver data segments to any subset of all possible destinations, as addressed at the source, under the minimal reliability transmission criteria.

Requirement T.5: Precedence handling

The SCPS transport protocol:

T.5.1: Shall provide the capability to recognize the precedence level specified by the user for a connection (in full reliability and best effort reliability operation) or for a data segment (in minimal reliability operation).

T.5.2: Shall provide a default precedence level that can be set by system configuration personnel.

T.5.3: Shall provide the capability to deliver data segments in accordance with their assigned precedence level.

Requirement T.6: Segmentation

The SCPS transport protocol:

T.6.1: Shall provide the capability for specification of the maximum segment size, by the system administrator, in accordance with system performance characteristics.

T.6.2: Shall provide the capability for peer transport entities to negotiate a maximum segment size.

T.6.3: Shall provide the capability to reassemble the finite-sized data segments back into their original form as a unitary message.

T.6.2 and T.6.3 only apply when employing full reliability and best-effort reliability (they do not apply under minimal releiability).

Requirement T.7: Operation over wide range of conditions

The SCPS transport protocol:

T.7.1: Shall be able to be configured to operate in processing environments typical of those available on space-based platforms.

T.7.2: Shall be able to support workloads typical of those anticipated for space-based platforms.

T.7.3: Shall be able to operate reliably under the delay, bandwidth, and error conditions typical of space-based communication environments.

Requirement T.8: Graceful closing of connections

The SCPS transport protocol:

T.8.1: Shall provide the capability to recognize requests for termination of a logical connection originating from the user of that connection.

T.8.2: Shall provide the capability to recognize termination requests of a logical connection originating from its peer transport entity.

T.8.3: Shall provide the capability for peer transport entities to mutually agree upon the closure of a logical connection.

T.8.4: Shall provide the capability to ensure successful delivery of any data segments in transit to a destination prior to the mutually-agreed termination of any logical connection required for that data segment, subject to the caveats expressed in T.1.

Requirement T.9: Response to congestion and corruption

The SCPS transport protocol:

T.9.1: Shall provide the capability to differentiate between network congestion and network data corruption, as identified by the network level protocol.

T.9.2: Shall provide the capability to counteract the identified network congestion anomalies.

T.9.3: Shall provide the capability to compensate for the identified network data corruption anomalies.

C. Data Protection

The functional requirements for the protection of data between end points within a space data communications system are stated below. Requirement P.5 is a DOD-only requirement; it is not a NASA requirement. The remaining requirements are both DOD and NASA requirements.

Requirement P.1: Access control

The SCPS data protection protocol shall provide the capability to control access to network resources. Only those users (or processes acting on behalf of users) with authorization shall be granted access to network resources. Examples of network resources are end systems, transport protocols within an end system, and routers.

Requirement P.2: Source authentication

The SCPS data protection protocol shall provide the capabilty to verify the identity of the end system that originated network communications.

Requirement P.3: Command authentication

The SCPS data protection protocol shall provide a capability to digitally *sign* a message to indicate that the message was actually sent by the user (or process acting on behalf of the user) claiming to send it.

Requirement P.4: Integrity

The SCPS data protection protocol shall provide the capability to ensure that the data sent is *exactly* the data received. It will provide the assurance that any unauthorized modification of the data will be detected while the data is in transit across the network.

Requirement P.5: Confidentiality

The SCPS data protection protocol shall provide the capability to ensure that the data transmitted across the network can be properly interpreted only by authorized users (or processes acting on behalf of users).

D. Networking

The functional requirements for providing network services for the transfer of data between end points within a space data communications system are stated below. All requirements are both DOD and NASA requirements.

Requirement N.1: Support for multicasting

The SCPS network protocol:

N.1.1: Shall be able to recognize the group destination specified by the user application, provided that such destination is a valid one

N.1.2: Shall be able to select the group address that correctly corresponds to the destination referred to in N.1.1.

N.1.3 Shall be able to assign proper group addresses to each outgoing packet that requires one

N.1.4: Shall be able to recognize valid group addresses and properly interpret them. Proper interpretation is defined as accurately determining how to route/relay the packets containing such group addresses.

Requirement N.2: Support for multiple routing options

The SCPS network protocol:

N.2.1: Shall be able to request the address of its neighboring node(s) from a routing module(s)

N.2.2: Shall be able to select the proper neighboring node for a packet and transmit the packet to that node.

N.2.3: Shall be able to route a packet to a unicast destination.

N.2.4: Shall be able to route a packet to a multicast destination consisting of one or more end systems.

N.2.5: Shall be able to flood route a packet to all space-based end systems.

N.2.6: Shall ensure that a flood routed packet that has been forwarded by a node is not subsequently forwarded by that same node.

Requirement N.3: Packet lifetime support with auto discard

The SCPS network protocol:

N.3.1 Shall be able to assign a maximum-age indication (e.g., hop count or time value) to each outgoing packet that requires one

N.3.2: Shall be able to determine the age of an incoming packet and properly interpret it. Proper interpretation is defined as accurately determining whether or not the incoming packet should be discarded due to having reached (or exceeded) its allowed lifetime.

N.3.3 Shall be able to automatically discard a packet which lifetime has been reached (or exceeded)

N.3.4: Shall, when a hop count is in use, be able to properly increment the age of each outgoing packet that requires it (adjusting or recomputing any network layer checksum or forward error correction as necessary).

Requirement N.4: Separate reporting of congestion & corruption

The SCPS network protocol:

N.4.1 Shall be able to detect and differentiate between network congestion and network data corruption.

N.4.2: Shall be able to report each of these two conditions to the transport protocol in a way that differentiates between them

N.4.3: Shall be able to manage and possible discard data in response to congestion.

N.4.4: In the event that it is necessary to discard data, data shall be discarded in order from lowest precedence to highest precedence.

Requirement N.5: Support for precedence handling

The SCPS network protocol:

N.5.1: Shall be able to recognize the precedence level specified by the application

N.5.2: Shall be able to provide a default precedence level for those packets that require one

N.5.3 Shall be able to assign the proper precedence level to each outgoing packet that requires one

N.5.4: Shall be able to recognize the precedence level associated with an incoming packet.

N.5.5: Shall be able to process incoming packets in accordance with their assigned precedence level.

N.5.6: Shall provide the ability for system configuration personnel to set the default precedence level for a system.

N.5.7: Shall provide for sixteen levels of precedence

Requirement N.6: Differentiation between real & exercise data

The SCPS network protocol:

N.6.1: Shall be able to recognize the data type (real vs. nonreal) specified by the application

N.6.2: Shall be able to provide a default data type to each outgoing packet.

N.6.3 Shall be able to assign the proper data type to each outgoing packet

N.6.4: Shall be able to recognize the data type associated with an incoming packet.

N.6.5: Shall be able to process incoming packets in accordance with their assigned data type.

N.6.6: Shall provide the ability for system configuration personnel to set the default data type for a system

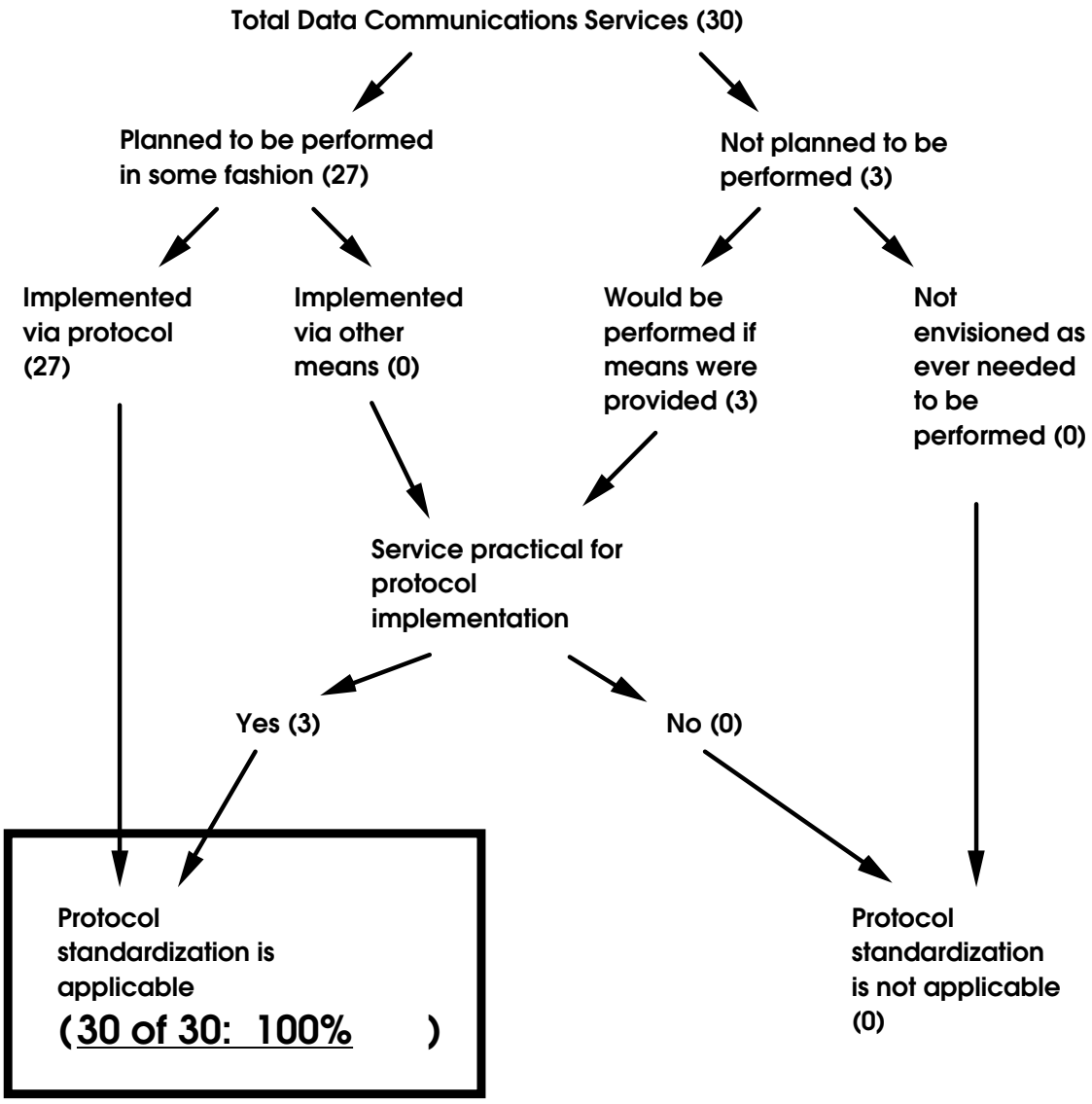

Figure 3 – BE Mission Assess Total

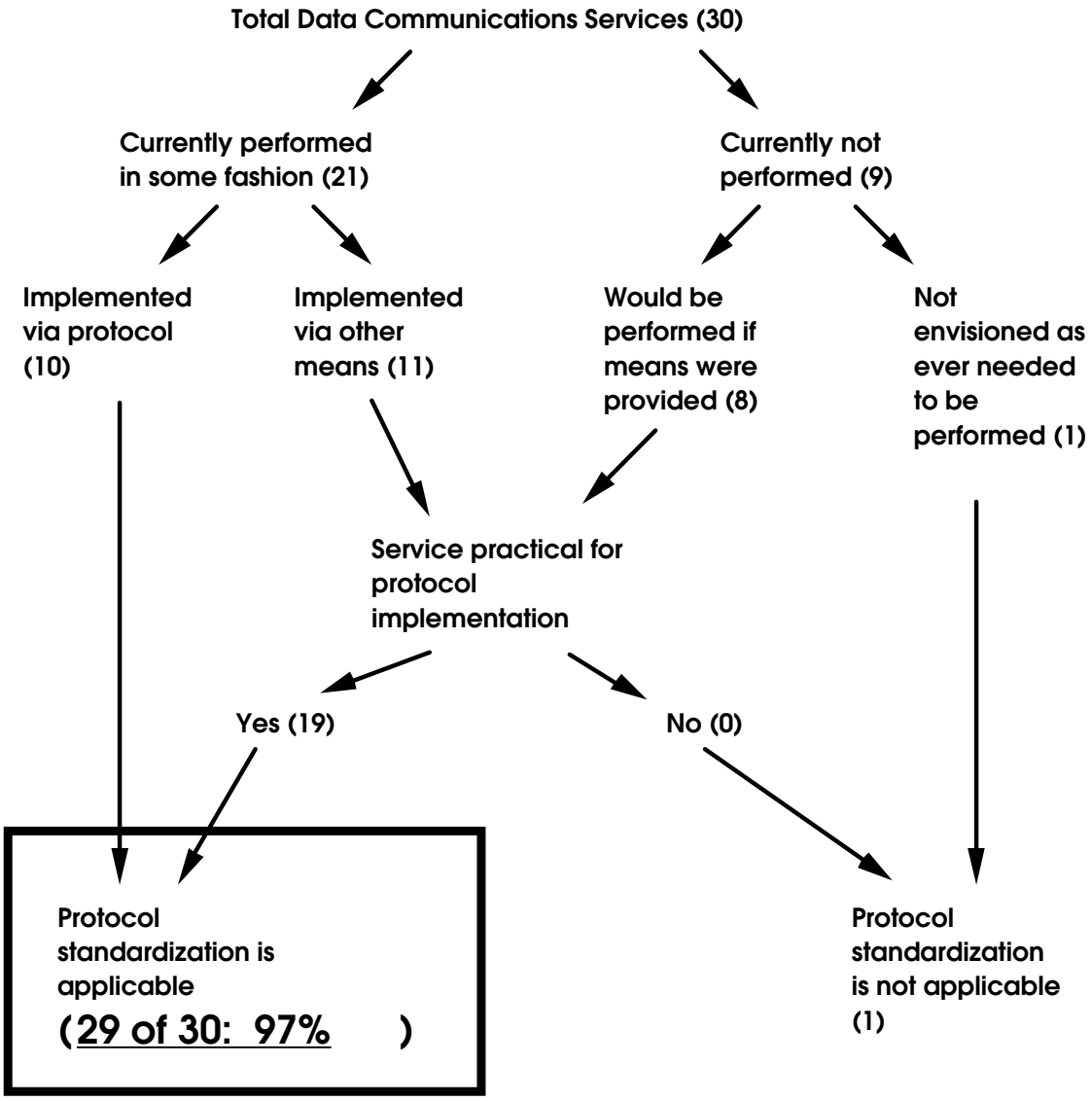

Figure 4 – GPS Mission Assess Total

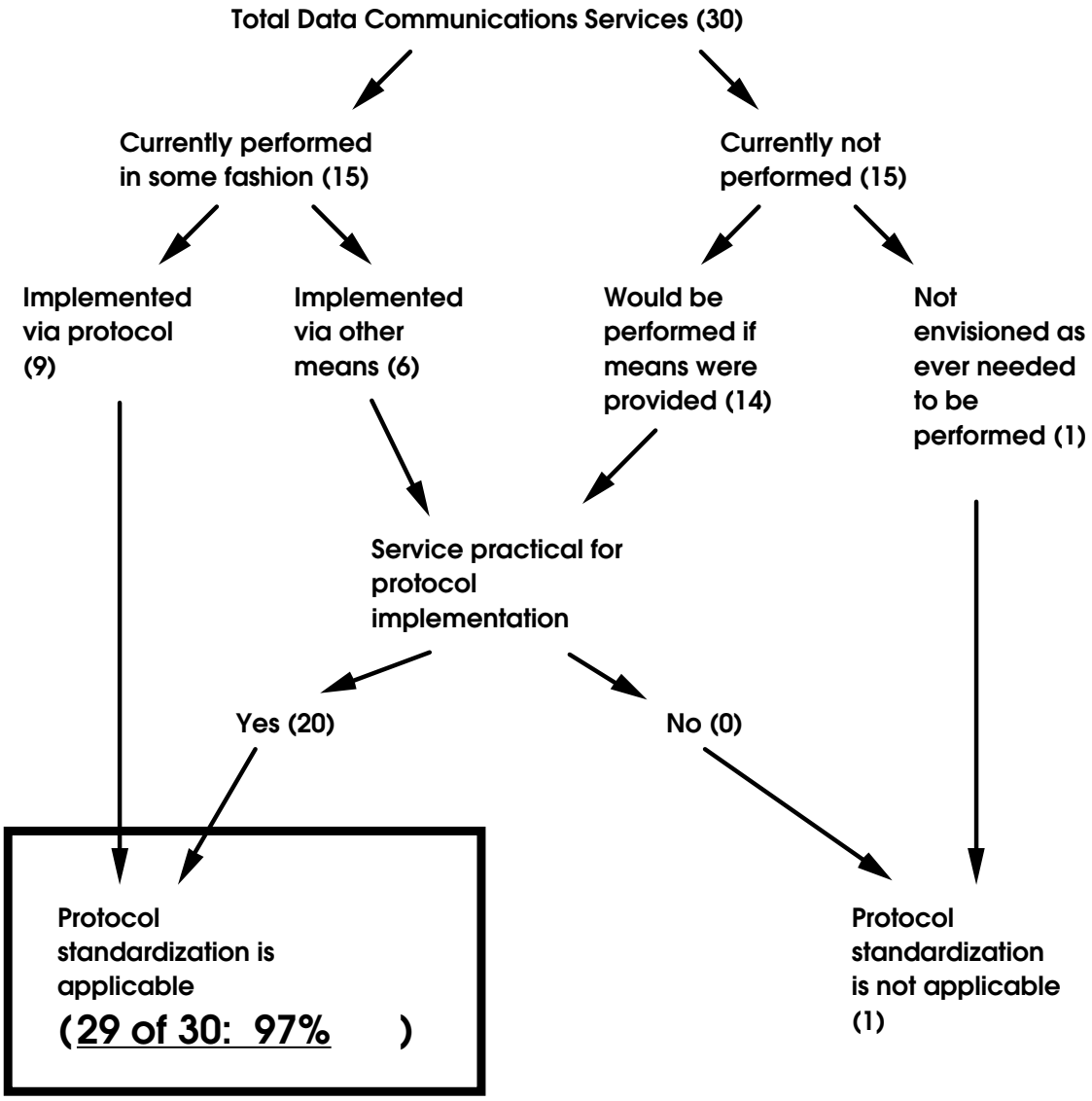

Figure 5 – DMSP Mission Assess Total

Table 1. Functions Common to Civil and Military Missions

	Communications Function	Civil Missions where Standardization is Applicable	Military Missions where Standardization is Applicable	Common Function
A. File Handling				
(1)	Operations on entire files	All	All	Yes
(2)	Operations on file records	All	All	Yes
(3)	Two party file transfer	All	All	Yes
(4)	Three party (proxy) file transfer	None	1 out of 3 (BMD/BE)	NO
(5)	User initiated file transfer features: interrupt/resumption & abort	All	All	Yes
Automatic file transfer features				
(6)	Progress monitoring	All	All	Yes
(7)	Interrupt detection	All	All	Yes
(8)	Resumption after interrupt	All	All	Yes
Preservation of integrity				
(9)	Over entire file	All	All	Yes
(10)	Over file record(s)	All	All	Yes
B. Transport				
(1)	Full reliability	All	All	Yes
(2)	Best effort reliability	All	All	Yes
(3)	Minimal reliability	All	All	Yes
(4)	Multicast with minimal reliability	All	All	Yes

Table 1. Concluded

Communications Function			Civil Missions where Standardization is Applicable	Military Missions where Standardization is Applicable	Common Function
B. Transport (concluded)					
	(5)	**Precedence handling**	**All**	**All**	**Yes**
	(6)	**Segmentation**	**All**	**All**	**Yes**
	(7)	**Operation over wide constraints**	**All**	**All**	**Yes**
	(8)	**Graceful close of connections**	**All**	**All**	**Yes**
	(9)	**Response to congestion & corruption**	**All**	**All**	**Yes**
C. Data Protection					
	(1)	**Access control**	**All**	**All**	**Yes**
	(2)	**Source authentication**	**All**	**All**	**Yes**
	(3)	**Command authentication**	**All**	**All**	**Yes**
	(4)	**Integrity**	**All**	**All**	**Yes**
	(5)	**Confidentiality**	**None**	**All**	**NO**
D. Networking					
	(1)	**Support for multicasting**	**All**	**All**	**Yes**
	(2)	**Support for multiple routing options**	**All**	**All**	**Yes**
	(3)	**Packet lifetime/auto discard**	**All**	**All**	**Yes**
	(4)	**Report congestion & corruption**	**All**	**All**	**Yes**
	(5)	**Support for precedence handling**	**All**	**All**	**Yes**
	(6)	**Differentiate real from exercise data**	**All**	**All**	**Yes**

3.3.3 Generation of Conceptual Protocol Stack

A protocol stack was then derived, which consists of conceptual protocols that support the common protocol requirements. These protocols were assigned to layers of the Open systems Interconnection (OSI) reference model. See figure 6. The shaded area constitutes the space protocols that support the common protocol requirements established in 3.3.1. The rest of the diagram is provided for context, i.e., to show how these protocols fit with the rest of the elements involved in data communications.

The space applications on top of the diagram use the services provided by the protocols to fulfill their data communications requirements. They access such services via Application Programming Interfaces (APIs) of which there are three. The one labeled MIN TS - API provides access to the minimal reliability transport service. The F&BE TS - API allows access to the full and best-effort reliability transport service whereas the FHS - API provides access to the file handling service. Notice that the data protection and networking services are not directly accessible to the space applications. The shaded networking service provides dynamic routing of packets throughout the space/space and space/ground subnetworks. The other two (non shaded) networking services already exist. The protocols shown under the three networking services also already exist and are shown to complete the protocol stack.

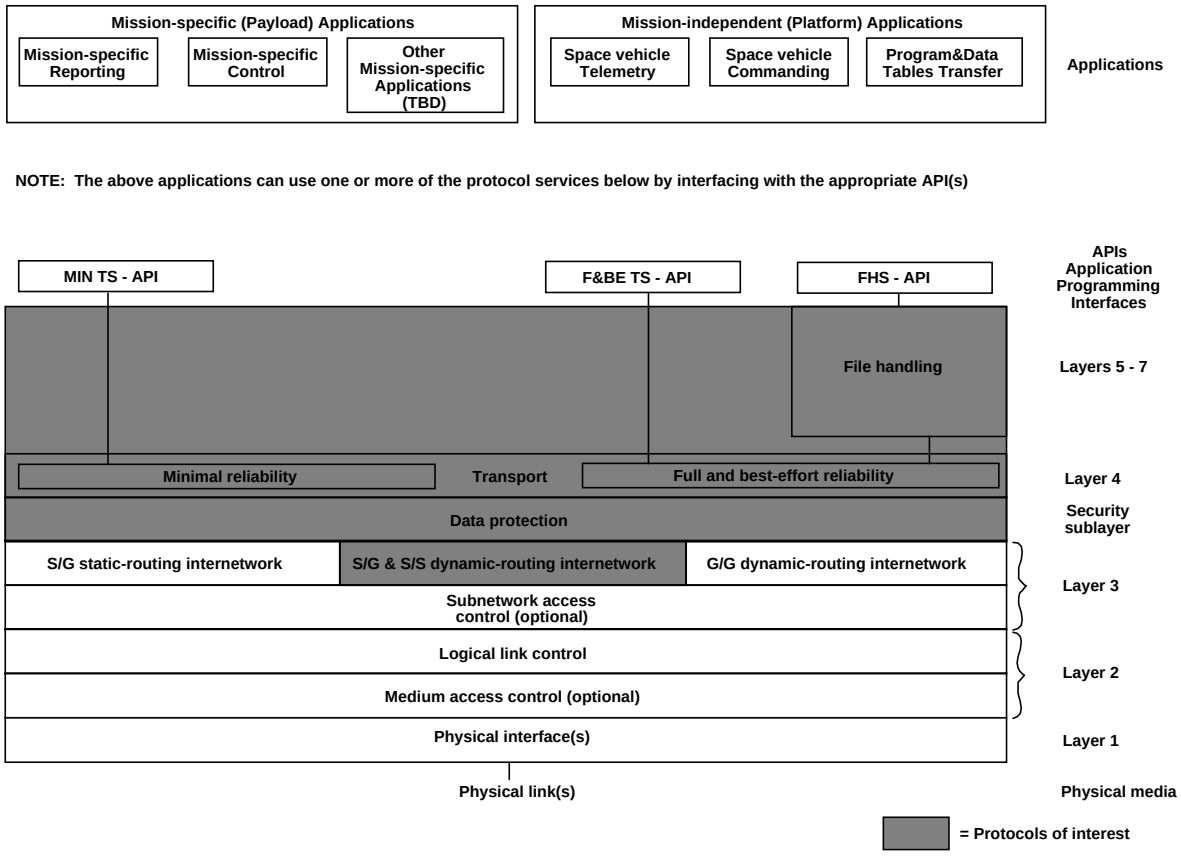

Figure 6 – Protocol Stack –9/30

THIS PAGE IS INTENTIONALLY BLANK

SECTION 4

SUMMARY OF WORK BASED ON THE REQUIREMENTS ASSESSMENT RESULTS

The second SCPS TWG team, the CSAT, defined mechanisms to meet the protocol requirements established by the RGAT, and considered ISO protocols as the initial candidates for providing such mechanisms. The primary protocols considered and their disposition are given in table 2 below.

Table 2. Candidate Space Communications Protocol Standards

Protocol	Disposition	Comments
File Transfer, Access, and Management (FTAM)	Discarded	Implementation size exceeds the memory limitations of space vehicles
DOD File Transfer Protocol (FTP)	Selected as a possibility	With functional enhancements, in competition with the Space Station FTP
Space Station (FTP)	Selected as a possibility	With functional enhancements, in competition with the DOD FTP
Connection-oriented Class 4 Transport Protocol (TP4)	Discarded	Implementation size approx 3 times that of TCP
Connectionless Transport Protocol (CLTP)	Discarded	Because TP4 was discarded
Connection-oriented Transmission Control Protocol (TCP)	Modified and selected	Functional enhancements and adaptation to space environment
Connectionless User Datagram Protocol (UDP)	Modified and selected	Functional enhancements
Network Layer Security Protocol (NLSP)	Discarded	Not yet approved by ISO; unnecessarily complex
DOD Security Protocol for Layer 3 (SP3)	Selected in two versions	Provides end-to-end data protection; full version and a modified, less overhead version
Connectionless Network Protocol (CLNP)	Discarded	Too much bit overhead, not enough functionality for space configurations
Internet Protocol (IP)	Discarded	Too much bit overhead, not enough functionality for space configurations
SCPS Network Protocol (SCPS NP)	New	Less overhead and increased functionality

THIS PAGE IS INTENTIONALLY BLANK

SECTION 5

CONCLUSIONS AND RECOMMENDATIONS

A requirements assessment was performed based on data collected for four civil and three military space missions. The four civil missions are SE, XTE, EOS, and SSF. The three military missions are BMD/BE, GPS, and DMSP. Thirty data communications services were analyzed for each of these missions to determine those that both (1) are common to civil and military systems (this is the set of common protocol functional requirements), and (2) can be implemented via standard space data communications protocols. Based on results to date, there are 28 out of 30 cases (93 percent) where protocol functional requirements are common and the standardization of space protocols applies.

A conceptual protocol stack was derived to support these common requirements. The derived protocol requirements and associated conceptual stack provided sufficient information to define protocol mechanisms that make up space data communications standards. Thus, based on the results of the requirements assessment work done by the RGAT, the CSAT defined some specific protocol mechanisms and identified candidate standards.

The requirements work has been expanded to include the collection of detailed operational scenarios (including work loads), system parameters and user performance requirements for each of the systems surveyed during Phase I. From this data, performance-oriented protocol requirements will be generated. Also, additional systems are planned to be surveyed and analyzed.

It is recommended that DOD programs provide this expanded requirements information to USSPACECOM so that the SCPS protocols can support a broadbase of military space programs. Specific templates have been designed and are available to collect these requirements.

THIS PAGE IS INTENTIONALLY BLANK

DEFINITIONS

The following terms and phrases have the indicated definitions when associated with the SCPS protocols.

- **Broadcast**: The transmission of a message from a source end system to all possible end systems (within the address space of the source end system).

- **Data segment**: An arbitrary grouping of contiguous data bits in multiples of eight bits.

- **Deep space**: For purposes of the SCPS project, any distance greater than 37,000 miles (62,000 kilometers) above the surface of the earth.

- **End system**: The true source and destination points involved in a data communication transaction. SCPS communications may occur between end systems on ground and space, between space end systems, and between ground end systems.

- **File**: Any data set presented to the file handling protocol that is designated as a file by the user of the protocol.

- **Flood Routing**: A process by which a packet is replicated and forwarded on all data links except the one on which it was received. With SCPS flood routing, packets that have been forwarded before by a node are not forwarded again.

- **Logical connection**: A logical connection is established when two peer protocols (i.e., protocols at the same level in the OSI reference model) agree to communicate and then agree on the conditions and parameters under which the communication will be conducted (frequently referred to as hand shaking).

- **Message**: For purposes of the SCPS project, a message is anything presented to the file handling or transport protocols by a user for transmission to another end system. This includes files, file records, text messages, binary messages, etc. A message may be divided into data segments and eventually into packets for transmission.

- **Multicast:** The transmission of a message from a source end system to more than one but not all possible end systems (within the address space of the source end system).

- **Node**: Any point in the transmission path between end systems that operates upon the communication signal. A node can be a switch, a repeater, a bridge, a router, another end system acting as a router, etc.

- **Packet**: For purposes of the SCPS project, a packet is the data-unit of the network layer sent to/received from the data link layer.

- **Precedence**: The hierarchical scheme for establishing the priority of a message. The higher the precedence level, the greater the priority of the message.

- **Record**: Any data set presented to the file handling protocol as a logical subset or portion of a file.

- **Super GEO**: Satellite orbits above 22,500 miles (37,500 kilometers) above the surface of the earth but less than 37,000 miles (62,000 kilometers).

- **Unicast**: The transmission of a message from a source end system to one other end system (within the address space of the source end system).

- **User**: The person at an end system (or a software application process acting as a proxy for such a person) that is the source or ultimate destination of a message

ACRONYMS

AF	Air Force
AFGWC	Air Force Global Weather Central
AFSPACECOM	Air Force Space Command
API	Application Programming Interface
APPLIC	Applicable
BMD/BE	Ballistic Missile Defense/Brilliant Eyes
CSAT	Capabilities Survey/Analysis Team
C^3S	Command, Control and Communications Segment
DCS	Data Communications Services
DISA	Defense Information Systems Agency
DMSP	Defense Meteorological Satellite Program
EOS	Earth Observing System
F&BE	Full and Best Effort (delivery reliability)
FHS ????	File Handling Service
FNOC	Fleet Numerical Oceanography Center
FY `	Fiscal Year
GPS	Global Positioning System
GSFC	Goddard Space Flight Center
IMPL	Implemented
JPL	Jet Propulsion Laboratory
MIN	Minimal (reliability)
NASA	National Aeronautics and Space Administration
NSA	National Security Agency
OSI	Open Systems Interconnection
PBV	Post Boost Vehicles
PERF	Performed
PROT	Protocol
RGAT	Requirements Gathering/Assessment Team
SCPS	Space Communications Protocol Standards

S/G	Space/Ground
S/S	Space/Space
SSF	Space Station Freedom
SRR	System Requirements Review
STAND	Standard
TBD	To be Determined
TDRS ????	Tracking Data Relay Satellite
TOG	Technical Oversight Group
TS	Transport Service
TWG	Technical Working Group
U.S.	United States
USSPACECOM	United States Space Command
XTE	X-ray Timing Explorer

APPENDIX A

BMD/BE

This appendix documents the collected system requirements and constraints as well as the assessment of the data communications services for the BMD/BE mission.

A.1 SYSTEM REQUIREMENTS

Table A-1. BMD/BE System Requirements

	System Requirement	Currently performed in this mission	Comments
1	**Space Applications**		
1a	**Space vehicle commanding**	**Yes**	
1b	**Space vehicle telemetry**	**Yes**	
1c	**Program & data table transfer**	**Yes**	
1d	**Mission control commanding**	**Yes**	
1e	**Mission data collection**	**Yes**	

Table A-1. Continued

2	**Data Exchange Scenarios**		
2a	**Ground source to space destination**	**Yes**	
2b	**Space source to ground destination**	**Yes**	
2c	**Space source to space destination**	**Yes**	

3	**Data Communications Services: File Handling**		
3a	**Operation on entire files**	**Yes**	
3b	**Operation on individual file records**	**Yes**	
3c	**Preservation of integrity during operations**	**Yes**	
3d	**Two party file transfer**	**Yes**	
3e	**Three party (proxy) file transfer**	**Yes**	
3f	**Interrupt/resumption and abort of file transfer**	**Yes**	**Interrupt, resumption and abort are both manually and automatically managed**

Table A-1. Continued

4	**Data Communications Services: E-E Data Transfer**		
4a	**Delivery reliability**		
4a1	**Full**	**Yes**	
4a2	**Best effort**	**Yes**	
4a3	**Minimal**	**Yes**	
4b	**Multicasting**	**Yes**	**Only with minimal reliability**
4c	**Precedence handling**	**Yes**	

Table A-1. Continued

5	**Data Communications Services: E-E Data Protection**		
5a	**Access control**	**Yes**	
5b	**Source authentication**	**Yes**	**Combined with command authentication**
5c	**Command authentication**	**Yes**	**Combined with source authentication**
5d	**Integrity**	**Yes**	
5e	**Confidentiality**	**Yes**	

6	**Data Communications Services: Networking**		
6a	**Support for multicasting**	**Yes**	
6b	**Support for multiple routing services**	**Yes**	
6c	**Precedence handling**	**Yes**	
6d	**Differentiation of real from exercise data**	**Yes**	

A.2 ASSESSMENT OF DATA COMMUNICATIONS SERVICES

The following table shows the results of assessing each data communications service for the BMD/BE mission. The table is structured as follows. The leftmost column lists specific services under four categories: (a) file handling, (b) transport, (c) data protection, and (d) networking. The headings of the next four columns correspond to four of the categories presented in the DCS analysis flow (See Figure 2 in the main body of this document). The headings labels are as follows:

- **PERF: IMPL by PROT** - Currently performed in some fashion: implemented via protocol
- **PERF: IMPL by OTHER MEANS** - Currently performed in some fashion: implemented via other means
- **NOT PERF: TO BE PERF if MEANS PROV** - Currently not performed: would be performed if means were provided
- **NOT PERF: NOT TO EVER BE PERF** - Currently not performed: not envisioned as ever needed to be performed

For each service, an "X" is marked under one of these four columns.

The rightmost column is used to indicate the disposition of the service. A "Yes"/"No" indicates that protocol standardization is applicable (**PROT STAND is APPLIC**)/not applicable for the service.

Table A-2. BMD/BE: DCSs Assessment

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
A	**File Handling**					
(1)	**Operations on entire files**	**X**				**Yes**
(2)	**Operations on file records**	**X**				**Yes**
(3)	**Two party file transfer**	**X**				**Yes**
(4)	**Three party (proxy) file transfer**	**X**				**Yes**

Table A-2. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
(5)	**User-initiated file transfer features: interrupt/resumption and abort**	**X**				**Yes**
	Automatic file transfer features					
(6)	**Progress monitoring**	**X**				**Yes**
(7)	**Interrupt detection**	**X**				**Yes**
(8)	**Resumption after interrupt detection**	**X**				**Yes**
	Preservation of integrity during operations					
(9)	**Over entire file**	**X**				**Yes**
(10)	**Over file record(s)**	**X**				**Yes**

Table A-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
B	**Transport**					
	Delivery reliability					
(1)	**Full**	**X**				**Yes**
(2)	**Best effort**	**X**				**Yes**
(3)	**Minimal**	**X**				**Yes**
(4)	**Multicasting (with minimal reliability provided by protocols)**	**X**				**Yes**
(5)	**Precedence handling**	**X**				**Yes**
(6)	**Segmentation**	**X**				**Yes**

Table A-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
(7)	Efficient operation over a wide range of constraints			X		Yes
(8)	Graceful closing of connections	X				Yes
(9)	Separate response to congestion and to corruption			X		Yes

Table A-2. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
C	**Data Protection**					
(1)	**Access control**	**X**				**Yes**
(2)	**Source authentication**	**X**				**Yes**
(3)	**Command authentication**	**X**				**Yes**
(4)	**Integrity**	**X**				**Yes**
(5)	**Confidentiality**	**X**				**Yes**

Table A-2. Concluded

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
D	**Network**					
(1)	**Support for multicasting**	**X**				**Yes**
(2)	**Support for multiple routing services**	**X**				**Yes**
(3)	**Packet lifetime support with automatic discard**	**X**				**Yes**
(4)	**Separate reporting of congestion and corruption**			**X**		**Yes**
(5)	**Precedence handling**	**X**				**Yes**
(6)	**Differentiation of real from exercise data**	**X**				**Yes**

THIS PAGE IS INTENTIONALLY BLANK

APPENDIX B

GPS

This appendix documents the collected system requirements and constraints as well as the assessment of the data communications services for the GPS mission.

E.1 SYSTEM REQUIREMENTS

Table B-1. GPS System Requirements

	System Requirement	Currently performed in this mission	Comments
1	**Space Applications**		
1a	**Space vehicle commanding**	**Yes**	
1b	**Space vehicle telemetry**	**Yes**	
1c	**Program & data table transfer**	**Yes**	
1d	**Mission control commanding**	**Yes**	
1e	**Mission data collection**	**Yes**	

Table B-1. Continued

2	**Data Exchange Scenarios**		
2a	**Ground source to space destination**	**Yes**	
2b	**Space source to ground destination**	**Yes**	
2c	**Space source to space destination**	**No**	

3	**Data Communications Services: File Handling**		
3a	**Operation on entire files**	**Yes**	
3b	**Operation on individual file records (pages)**	**Yes**	
3c	**Preservation of integrity during operations**	**Yes**	
3d	**Two party file transfer**	**Yes**	
3e	**Three party (proxy) file transfer**	**No**	
3f	**Interrupt/resumption and abort of file transfer**	**Yes**	**Interrupt, resumption and abort are both manually and automatically managed**

Table B-1. Continued

4	**Data Communications Services: E-E Data Transfer**		
4a	**Delivery reliability**		
4a1	**Full**	**Yes**	
4a2	**Best effort**	**Yes**	
4a3	**Minimal**	**No**	
4b	**Multicasting**	**No**	
4c	**Precedence handling**	**Yes**	

Table B-1. Concluded

5	**Data Communications Services: E-E Data Protection**		
5a	**Access control**	**Yes**	
5b	**Source authentication**	**Yes**	
5c	**Command authentication**	**Yes**	
5d	**Integrity**	**Yes**	
5e	**Confidentiality**	**Yes**	

6	**Data Communications Services: Networking**		
6a	**Support for multicasting**	**No**	
6b	**Support for multiple routing services**	**No**	
6c	**Precedence handling**	**Yes**	
6d	**Differentiation of real from exercise data**	**Yes**	

B.2 ASSESSMENT OF DATA COMMUNICATIONS SERVICES

The following table shows the results of assessing each data communications service for the GPS mission. The table is structured as follows. The leftmost column lists specific services under four categories: (a) file handling, (b) transport, (c) data protection, and (d) networking. The headings of the next four columns correspond to four of the categories presented in the DCS analysis flow (See Figure 2 in the main body of this document).. The headings labels are as follows:

- **PERF: IMPL by PROT** - Currently performed in some fashion: implemented via protocol
- **PERF: IMPL by OTHER MEANS** - Currently performed in some fashion: implemented via other means
- **NOT PERF: TO BE PERF if MEANS PROV** - Currently not performed: would be performed if means were provided
- **NOT PERF: NOT TO EVER BE PERF** - Currently not performed: not envisioned as ever needed to be performed

For each service, an "X" is marked under one of these four columns.

The rightmost column is used to indicate the disposition of the service. A "Yes"/"No" indicates that protocol standardization is applicable (**PROT STAND is APPLIC**)/not applicable for the service.

Table B-2. GPS: DCSs Assessment

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
A	**File Handling**					
(1)	**Operations on entire files**	**X**				**Yes**
(2)	**Operations on file records**	**X**				**Yes**
(3)	**Two party file transfer**	**X**				**Yes**
(4)	**Three party (proxy) file transfer**				**X**	**No**

Table B-2. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
(5)	**User-initiated file transfer features: interrupt/resumption and abort**	**X**				**Yes**
	Automatic file transfer features					
(6)	**Progress monitoring**		**X**			**Yes**
(7)	**Interrupt detection**		**X**			**Yes**
(8)	**Resumption after interrupt detection**		**X**			**Yes**
	Preservation of integrity during operations					
(9)	**Over entire file**	**X**				**Yes**
(10)	**Over file record(s)**		**X**			**Yes**

Table B-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
B	**Transport**					
	Delivery reliability					
(1)	**Full**	**X**				**Yes**
(2)	**Best effort**	**X**				**Yes**
(3)	**Minimal**			**X**		**Yes**
(4)	**Multicasting (with minimal reliability provided by protocols)**			**X**		**Yes**
(5)	**Precedence handling**		**X**			**Yes**
(6)	**Segmentation**		**X**			**Yes**

Table B-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
(7)	Efficient operation over a wide range of constraints			X		Yes
(8)	Graceful closing of connections		X			Yes
(9)	Separate response to congestion and to corruption			X		Yes

Table B-2. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
C	**Data Protection**					
(1)	**Access control**	**X**				**Yes**
(2)	**Source authentication**		**X**			**Yes**
(3)	**Command authentication**		**X**			**Yes**
(4)	**Integrity**	**X**				**Yes**
(5)	**Confidentiality**	**X**				**Yes**

Table B-2. Concluded

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
D	Network					
(1)	Support for multicasting			X		Yes
(2)	Support for multiple routing services			X		Yes
(3)	Packet lifetime support with automatic discard			X		Yes
(4)	Separate reporting of congestion and corruption			X		Yes
(5)	Precedence handling		X			Yes
(6)	Differentiation of real from exercise data		X			Yes

THIS PAGE IS INTENTIONALLY BLANK

APPENDIX C

DMSP

This appendix documents the collected system requirements and constraints as well as the assessment of the data communications services for the DMSP mission.

C.1 SYSTEM REQUIREMENTS

Table C-1. DMSP System Requirements

	System Requirement	Currently performed in this mission	Comments
1	**Space Applications**		
1a	**Space vehicle commanding**	**Yes**	
1b	**Space vehicle telemetry**	**Yes**	
1c	**Program & data table transfer**	**Yes**	
1d	**Mission control commanding**	**Yes**	
1e	**Mission data collection**	**Yes**	

Table C-1. Continued

2	**Data Exchange Scenarios**		
2a	**Ground source to space destination**	**Yes**	
2b	**Space source to ground destination**	**Yes**	
2c	**Space source to space destination**	**No**	

3	**Data Communications Services: File Handling**		
3a	**Operation on entire files**	**Yes**	
3b	**Operation on individual file records (pages)**	**No**	
3c	**Preservation of integrity during operations**	**Yes**	
3d	**Two party file transfer**	**Yes**	
3e	**Three party (proxy) file transfer**	**No**	
3f	**Interrupt/resumption and abort of file transfer**	**No**	

Table C-1. Continued

4	**Data Communications Services: E-E Data Transfer**		
4a	**Delivery reliability**		
4a1	**Full**	**Yes**	
4a2	**Best effort**	**Yes**	
4a3	**Minimal**	**No**	
4b	**Multicasting**	**No**	
4c	**Precedence handling**	**No**	

Table C-1. Concluded

5	**Data Communications Services: E-E Data Protection**		
5a	**Access control**	**Yes**	
5b	**Source authentication**	**Yes**	
5c	**Command authentication**	**Yes**	
5d	**Integrity**	**Yes**	
5e	**Confidentiality**	**Yes**	

6	**Data Communications Services: Networking**		
6a	**Support for multicasting**	**No**	
6b	**Support for multiple routing services**	**No**	
6c	**Precedence handling**	**No**	
6d	**Differentiation of real from exercise data**	**Yes**	

C.2 ASSESSMENT OF DATA COMMUNICATIONS SERVICES

The following table shows the results of assessing each data communications service for the DMSP mission. The table is structured as follows. The leftmost column lists specific services under four categories: (a) file handling, (b) transport, (c) data protection, and (d) networking. The headings of the next four columns correspond to four of the categories presented in the DCS analysis flow (See Figure 2 in the main body of this document). The headings labels are as follows:

- **PERF: IMPL by PROT** - Currently performed in some fashion: implemented via protocol
- **PERF: IMPL by OTHER MEANS** - Currently performed in some fashion: implemented via other means
- **NOT PERF: TO BE PERF if MEANS PROV** - Currently not performed: would be performed if means were provided
- **NOT PERF: NOT TO EVER BE PERF** - Currently not performed: not envisioned as ever needed to be performed

For each service, an "X" is marked under one of these four columns.

The rightmost column is used to indicate the disposition of the service. A "Yes"/"No" indicates that protocol standardization is applicable (**PROT STAND is APPLIC**)/not applicable for the service.

Table C-2. DMSP: DCSs Assessment

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
A	**File Handling**					
(1)	**Operations on entire files**	**X**				**Yes**
(2)	**Operations on file records**			**X**		**Yes**
(3)	**Two party file transfer**	**X**				**Yes**
(4)	**Three party (proxy) file transfer**				**X**	**No**

Table C-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
(5)	User-initiated file transfer features: interrupt/resumption and abort			X		Yes
	Automatic file transfer features					
(6)	Progress monitoring			X		Yes
(7)	Interrupt detection			X		Yes
(8)	Resumption after interrupt detection			X		Yes
	Preservation of integrity during operations					
(9)	Over entire file	X				Yes
(10)	Over file record(s)			X		Yes

Table C-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
B	**Transport**					
	Delivery reliability					
(1)	**Full**	**X**				**Yes**
(2)	**Best effort**	**X**				**Yes**
(3)	**Minimal**			**X**		**Yes**
(4)	**Multicasting (with minimal reliability provided by protocols)**			**X**		**Yes**
(5)	**Precedence handling**		**X**			**Yes**
(6)	**Segmentation**		**X**			**Yes**

Table C-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
(7)	**Efficient operation over a wide range of constraints**			**X**		**Yes**
(8)	**Graceful closing of connections**	**X**				**Yes**
(9)	**Separate response to congestion and to corruption**			**X**		**Yes**

Table C-2. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
C	Data Protection					
(1)	Access control	X				Yes
(2)	Source authentication		X			Yes
(3)	Command authentication		X			Yes
(4)	Integrity	X				Yes
(5)	Confidentiality	X				Yes

Table C-2. Concluded

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
D	**Network**					
(1)	**Support for multicasting**			**X**		**Yes**
(2)	**Support for multiple routing services**			**X**		**Yes**
(3)	**Packet lifetime support with automatic discard**			**X**		**Yes**
(4)	**Separate reporting of congestion and corruption**			**X**		**Yes**
(5)	**Precedence handling**		**X**			**Yes**
(6)	**Differentiation of real from exercise data**		**X**			**Yes**

THIS PAGE IS INTENTIONALLY BLANK

A.2 ASSESSMENT OF DATA COMMUNICATIONS SERVICES

The following table shows the results of assessing each data communications service for the BMD/BE mission. The table is structured as follows. The leftmost column lists specific services under four categories: (a) file handling, (b) transport, (c) data protection, and (d) networking. The headings of the next four columns correspond to four of the categories presented in the DCS analysis flow (See Figure 2 in the main body of this document). The headings labels are as follows:

- **PERF: IMPL by PROT** - Currently performed in some fashion: implemented via protocol
- **PERF: IMPL by OTHER MEANS** - Currently performed in some fashion: implemented via other means
- **NOT PERF: TO BE PERF if MEANS PROV** - Currently not performed: would be performed if means were provided
- **NOT PERF: NOT TO EVER BE PERF** - Currently not performed: not envisioned as ever needed to be performed

For each service, an "X" is marked under one of these four columns.

The rightmost column is used to indicate the disposition of the service. A "Yes"/"No" indicates that protocol standardization is applicable (**PROT STAND is APPLIC**)/not applicable for the service.

Table X. Composite DCSs Assessment across DoD Missions

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
A	**File Handling**					
(1)	**Operations on entire files**	**BE GPS DMSP**				**Yes**
(2)	**Operations on file records**	**BE GPS**		**DMSP**		**Yes**
(3)	**Two party file transfer**	**BE GPS DMSP**				**Yes**
(4)	**Three party (proxy) file transfer**	**BE**			**GPS DMSP**	**No**

Table X. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
(5)	**User-initiated file transfer features: interrupt/resumption and abort**	**BE GPS**		**DMSP**		**Yes**
	Automatic file transfer features					
(6)	**Progress monitoring**	**BE**	**GPS**	**DMSP**		**Yes**
(7)	**Interrupt detection**	**BE**	**GPS**	**DMSP**		**Yes**
(8)	**Resumption after interrupt detection**	**BE**	**GPS**	**DMSP**		**Yes**
	Preservation of integrity during operations					
(9)	**Over entire file**	**BE GPS DMSP**				**Yes**
(10)	**Over file record(s)**	**BE**	**GPS**	**DMSP**		**Yes**

Table X. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
B	**Transport**					
	Delivery reliability					
(1)	**Full**	**BE GPS DMSP**				**Yes**
(2)	**Best effort**	**BE GPS DMSP**				**Yes**
(3)	**Minimal**	**BE**		**GPS DMSP**		**Yes**
(4)	**Multicasting (with minimal reliability provided by protocols)**	**BE**		**GPS DMSP**		**Yes**
(5)	**Precedence handling**	**BE**	**GPS DMSP**			**Yes**
(6)	**Segmentation**	**BE**	**GPS DMSP**			**Yes**

Table X. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
(7)	Efficient operation over a wide range of constraints			BE GPS DMSP		Yes
(8)	Graceful closing of connections	BE DMSP	GPS			Yes
(9)	Separate response to congestion and to corruption			BE GPS DMSP		Yes

Table X. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
C	**Data Protection**					
(1)	**Access control**	**BE GPS DMSP**				**Yes**
(2)	**Source authentication**	**BE**	**GPS DMSP**			**Yes**
(3)	**Command authentication**	**BE**	**GPS DMSP**			**Yes**
(4)	**Integrity**	**BE GPS DMSP**				**Yes**
(5)	**Confidentiality**	**BE GPS DMSP**				**Yes**

Table X. Concluded

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF:** IMPL by OTHER MEANS	**NOT PERF:** TO BE PERF if MEANS PROV	**NOT PERF:** NOT TO EVER BE PERF	PROT STAND is APPLIC
D	Network					
(1)	Support for multicasting	BE		GPS DMSP		Yes
(2)	Support for multiple routing services	BE		GPS DMSP		Yes
(3)	Packet lifetime support with automatic discard	BE		GPS DMSP		Yes
(4)	Separate reporting of congestion and corruption			BE GPS DMSP		Yes
(5)	Precedence handling	BE	GPS DMSP			Yes
(6)	Differentiation of real from exercise data	BE	GPS DMSP			Yes

Table Y. Composite DCSs Assessment across NASA Missions

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
A	**File Handling**					
(1)	**Operations on entire files**	**GSFC SSF**				**Yes**
(2)	**Operations on file records**	**SSF**		**GSFC**		**Yes**
(3)	**Two party file transfer**	**GSFC SSF**				**Yes**
(4)	**Three party (proxy) file transfer**				**GSFC SSF**	**No**

Table Y. Continued

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
(5)	**User-initiated file transfer features: interrupt/resumption and abort**	**GSFC SSF**				**Yes**
	Automatic file transfer features					
(6)	**Progress monitoring**	**GSFC SSF**				**Yes**
(7)	**Interrupt detection**	**GSFC SSF**				**Yes**
(8)	**Resumption after interrupt detection**			**GSFC**	**SSF**	**Yes**
	Preservation of integrity during operations					
(9)	**Over entire file**	**GSFC SSF**				**Yes**
(10)	**Over file record(s)**			**GSFC SSF**		**Yes**

Table Y. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
B	**Transport**					
	Delivery reliability					
(1)	**Full**	**GSFC SSF**				**Yes**
(2)	**Best effort**	**GSFC SSF**				**Yes**
(3)	**Minimal**	**SSF**		**GSFC**		**Yes**
(4)	**Multicasting (with minimal reliability provided by protocols)**		**SSF**	**GSFC**		**Yes**
(5)	**Precedence handling**	**SSF**	**GSFC**			**Yes**
(6)	**Segmentation**	**SSF**	**GSFC**			**Yes**

Table Y. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
(7)	**Efficient operation over a wide range of constraints**			**GSFC SSF**		**Yes**
(8)	**Graceful closing of connections**	**SSF**	**GSFC**			**Yes**
(9)	**Separate response to congestion and to corruption**			**GSFC SSF**		**Yes**

Table Y. Continued

		Service Status/Disposition				
	Data Communications Service (DCS)	**PERF: IMPL by PROT**	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
C	**Data Protection**					
(1)	**Access control**		**SSF**	**GSFC**		**Yes**
(2)	**Source authentication**		**SSF**	**GSFC**		**Yes**
(3)	**Command authentication**		**SSF**	**GSFC**		**Yes**
(4)	**Integrity**	**GSFC SSF**				**Yes**
(5)	**Confidentiality**				**GSFC SSF**	**No**

Table Y. Concluded

	Data Communications Service (DCS)	Service Status/Disposition				
		PERF: IMPL by PROT	**PERF: IMPL by OTHER MEANS**	**NOT PERF: TO BE PERF if MEANS PROV**	**NOT PERF: NOT TO EVER BE PERF**	**PROT STAND is APPLIC**
D	**Network**					
(1)	**Support for multicasting**		**SSF**	**GSFC**		**Yes**
(2)	**Support for multiple routing services**			**GSFC SSF**		**Yes**
(3)	**Packet lifetime support with automatic discard**			**GSFC SSF**		**Yes**
(4)	**Separate reporting of congestion and corruption**			**GSFC SSF**		**Yes**
(5)	**Precedence handling**	**SSF**	**GSFC**			**Yes**
(6)	**Differentiation of real from exercise data**		**GSFC SSF**			**Yes**

THIS PAGE IS INTENTIONALLY BLANK