

ANNEX K TO JTF-SFA OPORD DEEP FREEZE

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS

OPR: JTF-SFA/J6

1. Situation.

a. Enemy. Refer to Basic Order.

b. Friendly. Refer to Basic Order.

c. Assumptions.

1) Overall communications planning responsibility resides with National Science Foundation (NSF).

2) USPACOM and its components, as described in this annex, provide communications services to support Operation DEEP FREEZE (ODF) operations IAW negotiated agreements with NSF. See Appendix 1 for copy of the Communications SLA between NSF and JTF SFA.

3) Communications support is required for all aspects of Antarctic operations: Air and ship traffic control, mission and unit command and control, scientific data collection and management, logistics and supply support, safety and rescue, weather, and in-transit visibility (ITV) of people, equipment and supplies.

4) Since Antarctica is a vast area with little terrestrial cable connectivity, ODF relies heavily on radio and satellite communications systems for connectivity. Unique operational considerations include: (1) high latitudes operations make communications vulnerable to solar and geomagnetic disturbances and (2) high latitude stations require very shallow look angles to satellites in geosynchronous or slightly inclined, near equatorial orbits, making continuous viewing nearly impossible.

5) The DOD makes military satellite communications resources available to the NSF on a non-interference basis. Reimbursement for operational costs will be IAW negotiated agreements between DOD and NSF agents.

6) Using precedent established by JCS in 1997 for aircraft flights supporting ODF, waiver has been granted to the mandate to use Demand Assigned Multiple Access (DAMA) protocols and encryption methods over DOD UHF SATCOM resources. Waiver for AMC aircraft operation is maintained and managed by AMC/A58 through USTRANSCOM/J6-OP.

2. Mission. Plan and report status of communications services supporting ODF operations designated in this OPOD to ensure sufficient connectivity for the safe and effective execution of all missions. This annex identifies methods, sources, and responsibilities necessary for meeting this requirement.

3. Execution.

a. Guiding Principles.

1) CDR JTF-SFA through the Director, Command, Control, Communications and Computer Systems Directorate (J6), is ultimately responsible for providing C2 of USPACOM forces and In-Transit Visibility (ITV) of en route assets.

2) JTF-SFA/J6 will coordinate with supporting commands' J6 or A6 regarding interoperability of communications systems as they support ODF operations.

b. Operational Concept.

1) The US Navy Space and Warfare Systems Center, Charleston, SC (SPAWARSYSCEN CHS), under interagency agreement with NSF, is assigned by NSF as the US Antarctic Program Spectrum Manager. SPAWAR is also responsible for Air Traffic Control and Landing Systems Operations, Support, and Maintenance; weather forecasting and weather observation equipment maintenance; and is responsible for coordinating commercial SATCOM support.

2) The Prime Contractor for NSF Antarctica operations is responsible for ground communications services, land mobile radio support, antenna maintenance and computer system maintenance supporting the entire USAP.

3) TRANSCOM/J6-OP is responsible for submitting requests for UHF SATCOM support for aircraft transiting between Christchurch and Antarctic Continent and for all Antarctic intra-continental UHF SATCOM support. TRANSCOM/J6-OP is also responsible for submitting waivers to DoD for not utilizing DAMA channels for UHF SATCOM.

4) JTF-SFA components and gained forces will provide planning and execution support for communications services as assigned by USPACOM.

5) JTF-SFA components and gained forces will provide COMSEC as required.

c. Tasks and Responsibilities.

1) 13 AEG/CC.

a) Inform JTF-SFA/613 Air Operations Center (613 AOC) of mission plans, schedules and changes.

b) Refer to Appendix 1 for communications outage reporting guidelines. NOTE: SPAWAR reports and seeks service restoration for commercial SATCOM outages via their own channels.

c) Provide overall command authority of deployed JTF-SFA forces and act as a focal point for issues relating to military personnel behavior on the USAP.gov network and military workstations.

2) JTF-SFA/J3 Operations & Plans.

Support JTF-SFA operations IAW Communications SLA in Appendix 1.

3) JTF-SFA/J6.

a) Provide or coordinate for required communications to support JTF-SFA in consonance with supported CDR USPACOM priorities.

b) Coordinate to ensure JTF-SFA SATCOM requirements are provided to USPACOM for access to DoD SATCOM assets.

c) Coordinate and advise JTF-SFA Commander on the operational direction and management of USAF communications forces supporting ODF.

d) Submit to NSF all JTF-SFA Information Technology (IT) requirements in format to be specified by NSF NLT the Annual Planning Conference.

e) Identify and report to USPACOM/J63 those communications requirements which cannot be satisfied with available resources.

f) Coordinate support with 747 CS to resolve any VPN problems for JTF-SFA staff deployed from Hickam.

g) Provide COMSEC materials for 13 AEG/CC and JTF-SFA staff IAW applicable instructions. GSA-approved safes for storing SECRET COMSEC materials are available at Christchurch.

h) Coordinate COMSEC requirements for deploying forces IAW applicable instructions.

i) Provide mid-season GPS codes and end-of season COMSEC for returning 109 AW crews.

j) Coordinate access to restricted .mil websites and databases, to include but not limited to G081, ARMS, ABSS, and Discoverer for all JTF-SFA personnel.

k) Manage tactical communications assets if deployed.

- l) Coordinate deployment, employment, and redeployment of mobile communications forces from in-theater and CONUS-based units in support of this OPORD if required.
 - m) Submit requests to USPACOM for JCS-controlled mobile/transportable communications assets, if required.
 - n) If required to support tactical deployments, request additional satellite channel allocations from RSSC-PAC and provide information copies to DISA-PAC and USPACOM/J6.
 - o) Ensure USTRANSCOM validates and submits UHF satellite access requests (SARs) to GSSC IAW JCS procedural, precedence, and apportionment guidelines in CJCSI 6250.01.
- 4) 747 CS.
- a) Provide access to .mil network from Christchurch, NZ and McMurdo Station, Antarctica for JTF-SFA staff deployed from Hickam AFB via VPN.
 - b) Support JTF-SFA CSA or NSF Prime Contractor requests for assistance to resolve any VPN problems for JTF-SFA staff deployed from Hickam.
- 5) 109 AW.
- a) Provide ADVON and REDEPLOYMENT computer support for all JTF-SFA forces.
 - b) Provide JTF-SFA/J6 with Information Technology (IT) planning support for 109 AW requirements.
 - c) Gather all 109 AW IT requirements and submit to JTF-SFA/J6 NLT 1 July.
 - d) Provide JTF-SFA/J6 a list of required COMSEC for the season NLT 1 September.
- 6) 62 AW.
- a) Provide JTF-SFA/J6 with all IT requirements for upcoming season NLT 1 April.
 - b) Provide COMSEC transportation, protection, storage, and issuance for 304 EAS forces IAW applicable instructions. GSA-approved safes for storing SECRET COMSEC materials are available at Christchurch.
- 7) SPAWARSYSCEN CHS
- a) Notify USPACOM, through JTF-SFA/J6, when there are changes to communications requirements that necessitate changing current SATCOM requirements.

- b) Provide frequency spectrum management for the USAP.
 - c) Provide Air Traffic Control and Landing Systems Operations, Support, and Maintenance.
 - d) Provide weather observation equipment operations, maintenance and support.
 - e) Coordinate commercial SATCOM requirements and support.
- 8) NSF Prime Contractor.
- a) Provide antenna maintenance, computer and phone maintenance and support, land mobile radio support and HF radio maintenance at McMurdo Station.
 - b) Provide communications support in Christchurch, New Zealand as outlined in Appendix 1.
- 9) US Coast Guard Station, Alameda.
- Submit SARs to USPACOM and coordinate with JTF-SFA/J6 for UHF SATCOM access for the USCG icebreaker supporting Antarctic operations, specifying either their own ICDB or USPACOM ICDB for dedicated or DAMA service as justified by traffic load.
- d. Intelligence and Reconnaissance. Not used.
 - e. Special Measures. Not Used.
4. Administration, Logistics, Maintenance and Supply.
- a. Logistics.
 - 1) If military IT Unit Type Codes (UTCs) are deployed, they will be deployed with sufficient spare parts (i.e. bench stock or Readiness Spares Packages) to provide self-support for at least 30 days. If military communications units are deployed in support of ODF, they must satisfy this spares requirement.
 - 2) On-site assets may be used to meet spares requirements. If deploying unit(s) can not meet this requirement, they will coordinate shortfalls/requirements through JTF-SFA/J6.
 - b. Administration.
 - 1) Reports. Appendices are utilized for this annex.
 - 2) Errors or omissions in this plan should be brought to the attention of JTF-SFA/J6.
 - c. Maintenance.

- 1) RPSC-NZ will provide communications maintenance support to JTF-SFA in New Zealand and RPSC will provide communications maintenance support to JTF-SFA in Antarctica.
- 2) IT equipment maintenance at Christchurch will be conducted in accordance with Appendix 1. All communications equipment maintenance at McMurdo will be conducted by RPSC-NZ.
- 3) Maintenance of deployed tactical equipment will be conducted by the deployed unit. If additional support is required it will be coordinated through JTF-SFA/J6.

d. Supply.

NSF, RPSC, and SPAWAR provide supplies IAW their contract responsibilities. Units deploying with their own IT equipment are responsible for their own re-supply. JTF-SFA/J3 provides supplies for IT equipment as outlined in Appendix 1.

5. Command and Control.

a. Command Relationships. Refer to Annex J.

b. Command, Control, Communications, and Computer Systems. The following Minimum Essential Communications and Control Data and Network Systems are required to effectively perform C2 functions:

- 1) Global Command and Control System (GCCS) access. GCCS is a comprehensive, global C2 system fully implementing the C4I for the warrior vision by providing distributive collaborative planning, Time Phased Force Deployment Data (TPFDD) manipulation, and communications capability among the Joint Staff, Unified Commands, Component Commands, and the JFC. GCCS access is provided via SIPRNET webpage access. SIPRNET is not accessible in Christchurch, NZ or McMurdo Antarctica. GCCS inputs are made via secure fax to home-station support elements for processing.
- 2) Defense Switched Network (DSN). DSN is an inter-base telecommunications system providing end-to-end common user and dedicated telephone service for the Department of Defense (DOD). DSN is not accessible in Christchurch, NZ or McMurdo Antarctica. All deploying personnel will use commercial telephones provided by the NSF Prime Contractor.
- 3) Non-secure Internet Protocol Router Network (NIPRNET). A worldwide network of unclassified IP routers that will support various applications to include Internet access and unclassified e-mail. IAW Appendix 1, NSF provides deploying military personnel with network access, printing capabilities and office automation software via the 'usap.gov' network. JTF-SFA personnel can access military sites via this '.gov' network.
- 4) Global Decision Support System (GDSS) (NIPR & SIPR) is a USTRANSCOM-funded system providing Mobility Air Forces (MAF) Command and Control (C2) information for the Defense Transportation System (DTS) to combatant commanders

throughout the full spectrum of military operations. As the MAF's **principal C2 system**, the operational imperative is to deliver robust capabilities to command and control MAF forces using a net-centric environment, allowing access and information sharing across classified and unclassified domains. Direction given by the SECDEF assigning USTRANSCOM responsibility for Distribution Process Ownership increases the need for greater theater and strategic mobility operations and control. GDSS will interoperate with Air Force/Army/Joint C2 systems, and is an integral part of USTRANSCOM's Defense Transportation System (DTS). As the USTRANSCOM, Joint, and Air Force C2 architectures mature, GDSS will be consistent with the USTRANSCOM, Joint, and USAF C2 Communities of Interest (COI). With interfaces to over 40 systems, GDSS is the hub of information flow within the Mobility Air Forces for C2 operations. It is a replicated, distributed C2 system composed of nodes located at Scott AFB IL, Travis AFB CA, Yokota AB JA, Hickam AFB HI, RAF Mildenhall, UK, and Ramstein AB GE.

5) USTRANSCOM Single Mobility System (NIPR&SIPR). Web based capability that provides world-wide users single point access to the Defense Transportation System, GDSS, and quick visibility of air mobility data.

///signed///

STANLEY T. KRESGE
Lieutenant General, USAF
Commander, JTF-Support Forces Antarctica

Appendices

- 1- Draft Communications SLA
- 3- Satellite Communications Planning

OFFICIAL

///signed///

RONALD C. COURNOYER, Col, USAF
Director, Communications and Information
JTF-Support Forces Antarctica

UNITED STATES ANTARCTIC PROGRAM

PROGRAM SERVICE LEVEL AGREEMENT



TITLE		OPERATING YEAR AGREEMENT	
INFORMATION TECHNOLOGY SUPPORT		<input type="checkbox"/>	Preliminary Agreement
		<input checked="" type="checkbox"/>	Final Agreement
PERIOD OF PERFORMANCE			
Fiscal Year	Begin - 2009 End - 2014		
CUSTOMER		SUPPLIER	
Joint Task Force – Support Forces Antarctica		National Science Foundation Office of Polar Programs	
PROGRAM MANAGEMENT APPROVAL			
SUPPLIER			
Project/Mission Manager			
(ON FILE)			
		Brian Stone Date	
		National Science Foundation Office of Polar Programs, Division of Antarctic Infrastructure and Logistics 4201 Wilson Blvd, Rm 755, Arlington, VA 22230 Telephone: (703)292-7458; E-mail: bstone@nsf.gov	
CUSTOMER			
Project/Mission Manager			
(ON FILE)			
		Col Paul Sheppard, USAF Date	
		Joint Task Force Support Forces Antarctica Deputy Commander, JTF-SFA 25 E. Street, Suite C-111 Hickam AFB, HI 96853 Telephone: (808)449-4744; E-mail: Ronald.Smith@hickam.af.mil	

SLA CHANGE HISTORY LOG

ISSUE	EFFECTIVE DATE	EXPIRATION DATE	DESCRIPTION OF CHANGES
Original	12/10/2008	09/30/2014	Initial Service Level Agreement

Table of Contents

1.	<u>CONTEXT</u>	1
1.1	<u>SUMMARY</u>	1
1.2	<u>PARTIES TO THE AGREEMENT</u>	1
1.3	<u>PURPOSE OF THE SLA</u>	2
1.4	<u>SCOPE OF THE SLA</u>	2
2.	<u>SERVICE INFORMATION</u>	2
2.1	<u>DESCRIPTION OF SERVICES</u>	2
2.2	<u>SERVICES COVERED</u>	3
2.3	<u>OPERATIONAL CONSIDERATIONS</u>	4
2.3.1	<u>COORDINATION POINTS OF CONTACT</u>	4
2.3.2	<u>USE OF GOVERNMENT CONTRACTORS IN THE PERFORMANCE OF WORK</u>	5
2.3.3	<u>CUSTOMER SERVICE DELIVERY OPERATING LOCATIONS</u>	6
2.4	<u>SERVICE REQUEST PROTOCOL</u>	6
2.5	<u>PREREQUISITES FOR SERVICE</u>	8
2.5.1	<u>Transfer of Customer Equipment (CE) to Supplier Custody</u>	8
2.5.2	<u>Supplier Commitments</u>	8
2.5.3	<u>Customer Commitments</u>	9
2.6	<u>COSTS, BILLING, AND PAYMENTS</u>	9
2.7	<u>REFERENCES</u>	9
2.8	<u>EXCLUSIONS</u>	9
2.9	<u>SERVICE STANDARDS</u>	10
2.9.1	<u>Availability</u>	10
2.9.2	<u>Responsiveness</u>	10
2.9.3	<u>Timeliness</u>	10
2.9.4	<u>Quality</u>	11
2.10	<u>CUSTOMER AND SUPPLIER RESPONSIBILITIES</u>	11
2.10.1	<u>OPERATIONS COMPLIANCE</u>	11
2.10.2	<u>TROUBLE REPORTING</u>	12
2.10.3	<u>DEMARCATIION OF RESPONSIBILITIES</u>	12
2.10.4	<u>FAULT RESOLUTION</u>	12
2.10.5	<u>OUTAGE COORDINATION AND NOTIFICATIONS</u>	13
2.10.6	<u>ACCESS TO CUSTOMER FACILITIES</u>	13
2.11	<u>SERVICE TRACKING</u>	14
2.11.1	<u>SUPPLIER</u>	14
2.11.2	<u>CUSTOMER</u>	14
2.12	<u>SERVICE REPORTING</u>	14
2.12.1	<u>SUPPLIER</u>	14
2.12.2	<u>CUSTOMER</u>	15
3.	<u>MANAGEMENT INFORMATION</u>	15
3.1	<u>SERVICE REVIEWS</u>	15
3.2	<u>CHANGE PROCESS</u>	16
3.3	<u>PROBLEM MANAGEMENT AND RESOLUTION</u>	16
4.	<u>APPENDICES</u>	ERROR! BOOKMARK NOT DEFINED.
4.1	<u>APPENDIX A – CONTACT INFORMATION</u>	ERROR! BOOKMARK NOT DEFINED.
4.2	<u>APPENDIX B – CUSTOMER EQUIPMENT INVENTORY TRANSFERRED TO SUPPLIER</u> ..	ERROR! BOOKMARK NOT DEFINED.
	BOOKMARK NOT DEFINED.	
4.3	<u>APPENDIX C – PROBLEM ESCALATION</u>	ERROR! BOOKMARK NOT DEFINED.
4.4	<u>APPENDIX D – GLOSSARY OF KEY TERMS</u>	ERROR! BOOKMARK NOT DEFINED.
4.5	<u>APPENDIX E – NSF INTER-AGENCY SERVICE REQUEST PROTOCOL</u> ..	ERROR! BOOKMARK NOT DEFINED.
	DEFINED.	

List of Figures

FIGURE 1 – SUPPLIER-CUSTOMER SERVICE MANAGEMENT RESPONSIBILITY ASSIGNMENTS	5
--	---

List of Tables

TABLE 1 - CUSTOMER AND SUPPLIER IDENTIFICATION	2
TABLE 2 - LIST OF COVERED SERVICES	3
TABLE 3 - CLASS OF SERVICE DEFINITIONS	6
TABLE 4 - CUSTOMER ORDER ENTRY PROCESS	7
TABLE 5 - CUSTOMER REQUEST SERVICE PROCESSING PRIORITY	8
TABLE 6 - SERVICE DESK HOURS OF OPERATION	10
TABLE 7 - AFTER-HOURS CALL-OUT RESPONSE	10
TABLE 8 – SERVICE PERFORMANCE MEASURES	14
TABLE 9 – SEASONAL REPORTING REQUIREMENTS	15
TABLE 10 - SUPPLIER CONTACT INFORMATION	ERROR! BOOKMARK NOT DEFINED.
TABLE 11 - SUPPLIER ANTARCTIC SUPPORT CONTRACTOR CONTACT INFORMATION	ERROR! BOOKMARK NOT DEFINED.
DEFINED.	
TABLE 12 – CUSTOMER CONTACT INFORMATION	ERROR! BOOKMARK NOT DEFINED.
TABLE 13 - NON-URGENT SERVICE REQUEST ESCALATION PROTOCOL	ERROR! BOOKMARK NOT DEFINED.
TABLE 14 - URGENT, IMMEDIATE SERVICE REQUEST ESCALATION PROTOCOL	ERROR! BOOKMARK NOT DEFINED.
TABLE 15 - GLOSSARY OF KEY TERMS	ERROR! BOOKMARK NOT DEFINED.

CONTEXT

SUMMARY

The National Science Foundation (NSF, herein designated as “Supplier”) and the Joint Task Force, Support Forces Antarctica (JTF-SFA, herein designated as “Customer”) of the United States Air Force Pacific Air Forces (USAF PACAF) have an established relationship for the provisioning of Department of Defense (DoD) logistics and operational support for the United States Antarctic Program, as established by an executive Memorandum of Agreement between NSF and the Secretary of the Air Force.

This Service Level Agreement (SLA), hereinafter “the SLA”, establishes areas of responsibilities, operational parameters and exceptions between the NSF Office of Polar Programs and the JTF-SFA, hereinafter the “Trading Partners”.

As required and mutually negotiated, NSF provides resources to facilitate the execution of services provided by JTF-SFA. Per other agreements and arrangements, NSF provides administrative and operational facilities and support services to JTF-SFA personnel stationed at the USAP logistical operations center in Christchurch, New Zealand, adjacent to the Christchurch International Airport and within USAP McMurdo Station, Ross Island, Antarctica.

JTF-SFA must utilize digital data communications and data processing/computing as a component of its support to NSF.

Prior agreements for digital data communications and data processing/computing supporting JTF-SFA activities in Christchurch, NZ called for JTF-SFA to provide and technically support its own computing hardware for attachment to NSF provisioned Christchurch local area networking (LAN) services and provide routine Tier 1 support. JTF-SFA can no longer sustain technical support and has requested NSF to assume the provisioning of all hardware. NSF and JTF-SFA have agreed that each agency benefits from changing the hardware provisioning relationship to this new status. Revised provisioning entails the transfer of current JTF-SFA assets supporting the Christchurch and/or McMurdo mission requirements to NSF for NSF custodial responsibility and ownership. This SLA addresses services delivered and managed by NSF to JTF-SFA.

This SLA supersedes the previous SLA of 2006 for the delivery of IT and communications services.

PARTIES TO THE AGREEMENT

The agencies involved in this Agreement have established Offices of Primary Responsibility (OPRs) for administrative and technical management of the terms contained herein, as follows:

Table 1 - Customer and Supplier Identification

SUPPLIER	CUSTOMER
<u>National Science Foundation</u> Office of Polar Programs Division of Antarctic Infrastructure and Logistics National Science Foundation 4201 Wilson Boulevard, Room 755S Arlington, VA 22230 http://www.nsf.gov/	<u>Joint Task Force – Support Forces Antarctica</u> Pacific Air Forces 13 th Air Force 13AF/A6 25 E. Street Hickam AFB, HI 96853

PURPOSE OF THE SLA

The purpose of the SLA is to define the specific services provided, identify requisite terms and conditions affecting the Supplier and the Customer, and document the cost of service, if any. The SLA manages expectations for availability, performance, security, and response to problems.

SCOPE OF THE SLA

This SLA pertains to Supplier provided information technology (IT) and communications services to the Customer in support of the Customer's fulfillment of USAP mission operations services provided to NSF via separate agreements. Services are delivered within Antarctica and the country of New Zealand.

This is not a cost-reimbursable service. NSF, as Supplier, provides services to JTF-SFA, as Customer, in concert with other in-kind logistical support resources provided in accord with the executive MOA.

Commitment to the terms of the agreement is based on best effort and intent.

SERVICE INFORMATION

DESCRIPTION OF SERVICES

The Service is defined as follows:

Desktop computing and commodity Internet data communications; electronic mail; local area network services for file storage, printing, removable media; use of USAP standard office automation applications; Tier 1/2/3 service desk support; and hosting of select Customer supplied applications and/or computing appliances.

SERVICES COVERED

Table 2 - List of Covered Services

SERVICE	SERVICE ELEMENTS
Desktop Computing	<ol style="list-style-type: none"> 1. USAP configuration standard 2. USAP standard life-cycle replenishment, subject to USAP program priorities as determined by the Supplier 3. IBM/PC compatible 4. Microsoft Windows based operating system 5. Support for Customer specified PKI authentication hardware necessary for Customer access to remote applications (e.g., CAC reader)
Commodity Internet	<ol style="list-style-type: none"> 1. New Zealand: <ol style="list-style-type: none"> a. Tunneled routing of Customer traffic into the commodity Internet in New Zealand. Source IP address representing Customer traffic originating from the USAP Christchurch network is identified as a U.S. Government network. Address registration information provided in Appendix F. b. Tunneled routing of Customer traffic into the USAP internal network for all traffic destinations involving USAP IP address space. 2. McMurdo: <ol style="list-style-type: none"> a. Direct routing of customer traffic onto CONUS national Internet backbone, Domain Name presented as <i>host.usap.gov</i> 3. Firewall port management for authorized Customer network traffic, subject to appropriate information security analysis and risk reviews. 4. Traffic packet prioritization and shaping at the discretion of the Supplier to manage WAN bandwidth utilization in the best interests of the USAP mission requirements for the affected operating location
Local Area Network Services	<ol style="list-style-type: none"> 1. USAP LAN network account 2. Network file storage – access to common shares and user dedicated shares, per USAP standard resource allocation conventions 3. Network attached printer access – common use, access printers
Office Automation Applications	<ol style="list-style-type: none"> 1. USAP standard electronic mail service, to include user account assignments within the USAP enterprise mail system (e.g., user email address presented as <i>user.name@usap.gov</i>) 2. USAP standard Microsoft Office software suite 3. USAP standard WWW browser configuration 4. USAP specific administrative or mission support applications, as required on a case-by-case basis 5. HTTP access to local USAP Intranet 6. Hosting of Customer operational information content on the

SERVICE	SERVICE ELEMENTS
Service Desk	<p>local USAP Intranet</p> <ol style="list-style-type: none"> 1. USAP supplied hardware and software applications are fully covered 2. Customer supplied hardware and software applications are covered only to the extent that the Supplier's operating location capability can support, to be negotiated on a case-by-case basis 3. Tier 1 walk-up and remote desk call support, as Supplier resources allow 4. Tier 2 technical support for resolution of technical support difficulties un-resolvable at Tier 1 or for the introduction of Customer supplied hardware/software. 5. Tier 3 support is transparent to the Customer and is implemented at the discretion of the Supplier's Tier 2 support level.
Hosting of Customer Equipment (CE)	<ol style="list-style-type: none"> 1. Customer-unique software applications, on case-by-case, best level of effort basis 2. Limited to desktop applications and printers unless separately cleared by the Supplier program management office 3. Mandatory pre-screening for and remediation of information security vulnerabilities before authorized to interconnect with Supplier information systems (e.g., screening and security conformance of transient laptop computers, etc.)
Information Security Compliance	<ol style="list-style-type: none"> 1. USAP configuration standard, compliant with USAP standard configurations and patch management of Customer Equipment (CE) and Customer utilized Supplier Equipment (SE), e.g. desktop computers 2. Annual information security awareness training validation 3. Augmentation of Supplier information security awareness training with USAP-specific training 4. CE incorporated into appropriate Supplier accreditation boundary for certification and accreditation purposes and subject to Supplier's certification and accreditation process

OPERATIONAL CONSIDERATIONS

COORDINATION POINTS OF CONTACT

Individuals and their roles identified as key Points of Contact (POC) are specified in Attachment A. These individuals are the principal Supplier and Customer POCs in the performance of this SLA. POC information includes Supplier and Customer support contractors.

Either the Supplier or the Customer may unilaterally change its POC or support contractor POC by written notice by a duly authorized (Supplier; Customer) Government official. Changes shall be carried via updates to Attachment A.

USE OF GOVERNMENT CONTRACTORS IN THE PERFORMANCE OF WORK

The Supplier utilizes a large support contractor to implement the terms and conditions of this agreement. The basic responsibility relationships are depicted in **Figure 1**. For the Supplier, the NSF/OPP Antarctic Support Contractor (ASC) further utilizes the services of teaming sub-contractors and outsourced sources of telecommunications services as part of its Supplier role. This requires effective lines of Supplier-Customer communications among all parties. Effective service management for order entry, daily operations, trouble reporting, and fault resolution require direct communications between the Customer site representative and the local NSF Antarctic Support Contractor (ASC) IT Service Desk at the affected operating location.

Service Management Responsibilities			
Task Description	NSF Antarctic Support Contractor	NSF USAP Program Office	JTF-SFA 13-AEG
Service Request	A	C, I	R
Service Delivery	R	A	C, I
Trouble Notification	A	C, I	R
Trouble Management	R	A	C, I
Policy Formulation	C, I	R, A	I
Policy Enforcement	R	A, C, I	C, I
Policy Conformance	A	C, I	R
Legend			
Responsible - Those who do work to achieve the task. There can be multiple resources responsible.			
Accountable - The resource ultimately answerable for the correct and thorough completion of the task. Only one A for each task.			
Consulted - Those whose opinions are sought. Two-way communication.			
Informed - Those who are kept up-to-date on progress. One-way communication.			

Figure 1 – Supplier-Customer Service Management Responsibility Assignments

Appendix A defines the specific organization identified under the generic title of ASC. This information is provided as part of the specific contact information needed for service management communications.

CUSTOMER SERVICE DELIVERY OPERATING LOCATIONS

Service delivery occurs at two primary locations: (1) the USAP operating location situated at the International Antarctic Center, Christchurch, NZ and (2) within McMurdo Station, Antarctica. Multiple physical service delivery points exist at these two operating locations.

The continental U.S. (CONUS) termination of the Internet service element occurs at the location of the NSF's USAP WAN network operations center/data center. At the present time, this function is hosted by the NSF ASC at the ASC headquarters facility. This termination may be subject to change in future years as a consequence of ASC contract termination and subsequent competitive re-acquisition. Should such a condition occur, the anticipated transition time frame would be during October, 2009 – March, 2010. This information is provided for future reference for subsequent SLA modifications, if required.

SERVICE REQUEST PROTOCOL

Table 3 describes the various types of user service requests supported. These definitions are used to further describe the Customer service support and escalation processes.

Table 3 - Class of Service Definitions

CLASS OF SERVICE DEFINITIONS		
CLASS	PRECEDENCE TYPE	DEFINITION
Routine	Non-urgent	Character of service is consistent with established baseline of Customer support. Minor deviations or changes. Utilizes existing hardware/software. No budgetary impacts of significance - support falls within existing Supplier funding guidelines. No exceptions to standard information security practices and policy. Timeline to implement service is flexible and not time sensitive.
Non-Routine	Non-urgent	Character of service may deviate significantly from the established baseline of Customer support. The introduction of a new service is required. New or different hardware/software is required. Significant budgetary impacts or additional funding augmentation to existing Supplier funding guidelines is required. Exceptions to standard information security practices and policy required. Timeline to implement service may be constrained or inflexible.
Work Stoppage	Non-urgent	Routine or non-routine class of service addressing a disruption and/or Customer work stoppage. Customer work stoppage is tolerable and results in no Customer mission impacts of significance.
Work Stoppage	Urgent	Routine or non-routine class of service addressing a disruption and/or Customer work stoppage for which delays in timely processing the request result in unacceptable impacts to Customer work functions.
Mission Impact	Immediate	Any class of service for which there is a clear and significant impact to the Customer mission which requires immediate attention to prevent loss of life, loss of property, major disruptions in the Customer's commitments to other organizations, significant financial impact/loss, and similar impacts.

Table 4 provides a summary explanation of the Customer service request protocol for submitting and processing, described as order entry. Distinctions are invoked between the service classes defined in **Table 3**.

Table 4 - Customer Order Entry Process

ORDER ENTRY PROCESS		
CLASS	PRECEDENCE TYPE	ORDER ENTRY DESCRIPTION
Routine	Non-urgent	Customer submits service request directly to the Supplier's Service Desk at the affected operating location.
Non-Routine	Non-urgent	Customer submits service request via the Supplier's organizational Inter-Agency Service Request protocol
Work Stoppage	Non-urgent	Customer submits service request directly to the Supplier's Service Desk at the affected operating location if the request otherwise fits the routine service definition. Non-routine nature requests must be coordinated with the Supplier program office where a determination is made if the Inter-Agency Service Request protocol must be followed.
Work Stoppage	Urgent	Customer submits service request directly to the Supplier's Service Desk at the affected operating location.
Mission Impact	Immediate	Customer submits service request directly to the Supplier's Service Desk at the affected operating location.

Examples of Routine service requests may include, but are not restricted to: office automation application trouble resolution, email account set-up, email archiving, LAN account set-up, password reset, telephone number assignment, moves/adds/changes for LAN and/or telephone outlet locations, etc.

A copy of the NSF Inter-Agency Service Request protocol cited in **Table 5** is included in Appendix E.

Table 5 describes the processing protocol applied to the various classes of service requests defined in **Table 3**.

(Remainder of page intentionally blank)

Table 5 - Customer Request Service Processing Priority

SERVICE PROCESSING PRIORITY		
CLASS	PRECEDENCE TYPE	PRIORITY MANAGEMENT
Routine	Non-urgent	First in - First Out (FIFO) - Orders are processed in time sequence as they are received, merged with service requests from other customers.
Non-Routine	Non-urgent	First in - First Out (FIFO) - Orders are processed in time sequence as they are received, merged with service requests from other customers.
Work Stoppage	Non-urgent	First in - First Out (FIFO) - Orders are processed in time sequence as they are received, merged with service requests from other customers. As resources allow and/or as other Customers with work in progress may permit, best efforts would be exercised to see if servicing priority can be elevated to shorten the processing delay.
Work Stoppage	Urgent	Last in - First Out (LIFO) - Orders are processed upon receipt, with all other service processing for requests with lower customer impact consequences are suspended until satisfactory progress is made for processing the urgent request.
Mission Impact	Immediate	Last in - First Out (LIFO) - Orders are processed immediately upon receipt with an immediate preemption of all other customer service request processing. Dedicated efforts are expended to process or resolve. Extended hour service management coverage may be invoked, as needed.

The Supplier does not warrant that guaranteed response times can be provided when servicing any Customer request. Customer service requests are processed on a best level of effort basis. Where practicable, the Supplier will attempt to place priority emphasis on Customer requests in the urgent/immediate class.

PREREQUISITES FOR SERVICE

Transfer of Customer Equipment (CE) to Supplier Custody

For the inaugural year of service, the Customer agrees to transfer the itemized inventory of CE as defined in Appendix B as a requirement for the Christchurch, NZ operating location.

Supplier Commitments

The Supplier agrees to:

- a) Provide service to the Customer utilizing CE assets and supplies transferred to the Supplier to become Supplier Equipment (SE)
- b) Support Customer inventory verification and hand-off for CE currently pre-positioned at the operating locations
- c) Assume full custodial responsibility for the CE, to include compliance with Federal property management and reporting

- d) Assume full operations, maintenance, and life cycle replenishment of the CE

Customer Commitments

The Customer agrees to:

- a) Transfer CE computing assets utilized by the Customer for Christchurch, NZ operations to the Supplier. The equipment to be transferred will include five (5) new desktop machines and one laser printer to replace Customer equipment deemed by the Supplier as non-supportable.
- b) Verify inventory in-place and exercise best effort to provide necessary documentation to the Supplier
- c) Exercise best efforts to ensure all assets transferred are fully functional and in proper working order
- d) Transfer assets in accord with Supplier protocols for inventory management of excess personal property, to include needed coordination with the Supplier's ASC Contractor
- e) Abide by Supplier priorities for hardware/software lifecycle replacement/refresh

COSTS, BILLING, AND PAYMENTS

The cost of the Service is provided at no direct cost to the Customer.

Service scope and performance levels are subject to unilateral adjustment by the Supplier as Supplier budgetary requirements may dictate.

Service is provided by the Supplier on a best level of effort with no explicit or implicit guarantees of specific service levels or quality.

REFERENCES

- a) Service Level Agreement Between Joint Task Force Support Forces Antarctica 500 Air Expeditionary Group (AEG) and the National Science Foundation Office of Polar Programs, June 2006.

EXCLUSIONS

Supplier services shall exclude the following without prior coordination and approval by the Supplier SLA Administrator:

- a) Expansion of Customer seat-count beyond pre-established FY2008 operating season levels
- b) Support for unauthorized Customer equipment (hardware, software)
- c) Deviations from USAP standard office automation applications and versions
- d) Introduction of non-standard computing systems and/or peripherals, relative to established USAP conventions

- e) Customer support requests for operating locations other than those explicitly described within this SLA

SERVICE STANDARDS

Availability

Services will be nominally available 24x7x365, exclusive of regularly scheduled maintenance outages and holidays.

Table 6 - Service Desk Hours of Operation

LOCAL SERVICE DESK - HOURS OF OPERATION			
OPERATING LOCATION	SEASON	Day of Week	HOURS
Christchurch	Austral Summer	M - F	0800 - 1700 NZT
	Austral Winter	"	"
McMurdo	Austral Summer	M - Sa	0730 - 1700 NZT
	Austral Winter	M - F Sa	0800 - 1700 NZT 0800 - 1200 NZT

Responsiveness

These responsiveness standards apply to after-hours call-out required Supplier response to Customer urgent/immediate service requests.

Table 7 - After-Hours Call-Out Response

LOCAL SERVICE DESK - AFTER HOURS CALL-OUT RESPONSE			
OPERATING LOCATION	SEASON	RESPONSE TO CALL OR PAGE	TECHNICIAN ROLL-OUT
Christchurch	Austral Summer	90 Minutes	4 Hours
	Austral Winter	"	"
McMurdo	Austral Summer	30 Minutes	2 Hours
	Austral Winter	"	"

Timeliness

Supplier will exercise best efforts to resolve Customer technical support requests in a timely manner.

Supplier shall be sensitive to Customer mission impacts imparted by Service disruptions and anomalies and shall exercise due diligence when responding.

Quality

Supplier does not guarantee performance of Customer applications transiting the commodity Internet or site-to-site secure tunnels via the commodity Internet, as traffic management is beyond the ability of the Supplier to affect.

Supplier can apply packet shaping to Customer network traffic flowing via the USAP WAN links servicing the operating locations to provide relative Quality of Service as applied to all USAP traffic. Specific Customer requirements must be managed on a case-by-case basis.

CUSTOMER AND SUPPLIER RESPONSIBILITIES

OPERATIONS COMPLIANCE

Customer	<p>The Customer shall be responsible for operating in conformance with the Supplier's standard operating procedures and information security compliance protocols, to include awareness training and conformance to Rules of Behavior.</p> <p>The Customer shall submit all transient computing equipment (e.g., laptop computers) to a full Supplier information security compliance scan and shall allow the Supplier to apply needed software patches and/or anti-viral files necessary to comply with acceptable risk levels as determined by the local Supplier site operator.</p> <p>The Customer shall ensure that all transient computing equipment (e.g., laptop computers) requiring information security compliance scanning/remediation shall be configured with appropriate administrative password control supplied to allow Supplier site operators to perform necessary security functions.</p> <p>The Customer shall ensure that all Customer-unique software applications introduced into the USAP computing environment are submitted to the Supplier for an information security risk analysis and determination prior to implementation. The Customer shall abide by Supplier risk determinations regarding risk acceptance, required remediation, and/or rejection.</p> <p>The Customer shall self-coordinate all access to specific DoD NIPRNET websites (*.mil) if the Customer's personnel cannot obtain access via the Supplier's network. The Customer shall provide operating instructions to Customer personnel for trouble reporting protocols and shall file a courtesy copy with the Supplier's local operating location Service Desk.</p>
Supplier	<p>The Supplier shall enforce USAP desktop configuration standards, restrictions on installation of non-USAP standard software, vulnerability scans, patch management, anti-virus scans, and vulnerability remediation.</p> <p>The Supplier shall grant reciprocity for Customer information security awareness training performed under DoD standards in cases where a responsible Customer official can provide verification for Customer personnel and the age of the training meets USAP timeliness requirements. This does not excuse the Customer from additional awareness training and acknowledgement requirements per USAP standard procedures.</p> <p>The Supplier shall maintain and replenish all desktop, file, and print hardware per USAP standard operation procedures and priorities.</p>

TROUBLE REPORTING

Customer	The Customer shall use standard Service Desk support requests for non-urgent trouble reports. The Customer shall use established site-specific protocols for reporting urgent/immediate response trouble notifications.
Supplier	The Supplier shall provide the Customer a trouble reporting hotline telephone number and/or pager number.

DEMARCATON OF RESPONSIBILITIES

Customer	<p>The Customer shall be responsible for configuration management of Customer-unique software applications that are granted permission for installation and operation. Exceptions shall be negotiated on a case-by-case basis.</p> <p>The Customer shall agree to operate under USAP standard desktop user privileges for operating system configuration management. The Customer shall submit a business case to the Supplier for Supplier evaluation for deviations on a case-by-case basis.</p> <p>The Customer shall supply all software and equipment required to support Department of Defense Public Key Infrastructure capabilities. This includes Common Access Card readers, software, and drivers.</p>
Supplier	<p>The Supplier shall manage all desktop configurations and settings in order to ensure compliance with Federally mandated configuration standards.</p> <p>The Supplier shall assign desktop user privileges for operating system configuration management per USAP standard desktop management procedures. Exceptions shall be granted on a case-by-case basis as determined by a Customer business case request.</p>

FAULT RESOLUTION

Customer	The Customer authorizes direct contact between the Supplier's ASC Operations and Maintenance staff and the Customer's individual staff stationed at the covered operating locations.
Supplier	<p>The Supplier's ASC contractor acts as the Operations and Maintenance (O&M) contractor for first line support within Antarctica and New Zealand.</p> <p>The Supplier's ASC contractor will use processes and procedures that have been established and are currently in use to provide support to trouble shooting any problems that might arise.</p>

OUTAGE COORDINATION AND NOTIFICATIONS

Customer	The Customer shall notify the Supplier of special mission operations that are highly sensitive to service disruptions such that the Supplier should take same into special consideration when planning service outages.
Supplier	<p>The Supplier shall coordinate with the Customer a minimum of one week in advance for scheduled Service outages.</p> <p>The Supplier shall notify the Customer SLA Operational Services Outage Notification contact for all planned outages of greater than 1 (one) hour in duration, or for all unplanned outages of 6 (six) hours or greater in duration. Customer contact information provided in Appendix A.</p> <p>The Supplier shall coordinate with Customer activities and shall modify schedules/plans as needed to accommodate Customer mission needs.</p> <p>The Supplier shall provide the Customer’s ASC contractor with timely outage notification information for both scheduled and unscheduled outages to support the Customer’s mission operations. This shall include adding Customer designated contacts to standard USAP outage notification e-mail listserv accounts for USAP Enterprise, McMurdo, and Christchurch operating locations.</p>

ACCESS TO CUSTOMER FACILITIES

Customer	The Customer shall facilitate Supplier ASC contractor and subcontractor access to Customer occupied facility locations at the affected operating locations.
Supplier	The Supplier shall ensure reasonable notification and coordination of any physical access to the Customer occupied spaces at the affected operating locations. Coordination shall occur with the ASC contractor designated point(s) of contact at the affected operating locations.

SERVICE TRACKING

SUPPLIER

The Supplier shall collect the performance information indicated in Table 8 on a best-efforts basis and shall maintain an historical archive to support annual trending analysis and inter-annual comparisons over the anticipated lifetime of this service agreement.

Table 8 – Service Performance Measures

INFORMATION ITEM	DATA	ADDITIONAL DATA
New Service Requests	Number of events per reporting interval	-
Trouble Reports	Number of events per reporting interval	-
Call-back response time performance to Customer after-hour support calls	Number of events per reporting interval	Max., Min., Average Time
Roll-out response time performance to respond to Customer after-hour trouble	Number of events per reporting interval	Max., Min., Average Time
Problem resolution time – time to resolve Customer urgent/immediate trouble	Number of events per reporting interval	Max., Min., Average Time

CUSTOMER

The Customer and the Supplier will negotiate additional performance data collection on a case-by-case basis. The Supplier does not guarantee that any/all requests can be honored, as requests shall be subject to personnel and equipment limitations incurred by the Supplier's ASC contractor.

SERVICE REPORTING

SUPPLIER

The Supplier will exercise best efforts to provide the Customer seasonal service summary reports. The reports shall contain, at a minimum, the following information listed in **Table 9**:

Table 9 – Seasonal Reporting Requirements

INFORMATION ITEM
Anomaly report summaries, to include all outages irrespective of origin (Supplier, Customer)
Summary explanation(s) regarding any network outage or degraded performance
Tabular presentation of reporting month Service Performance Measures
Graphical presentation of cumulative Service Performance Measures from beginning of Fiscal Year through conclusion of the reporting month, with depiction of service trend line and with depiction of nominal accepted performance limit

The Supplier is excused for incompleteness or inaccuracies in its reporting due to reporting items contingent upon Customer provided information or other conditions beyond the control of the Supplier.

The Supplier will provide the seasonal summary service reports on a nominal schedule of 30 calendar days following the end of the austral summer USAP operating season at the affected operating location. Specific report format and form will be defined by the Supplier.

Supplier seasonal summary service reports shall be delivered via the Supplier’s main Agency point of contact.

CUSTOMER

The Customer agrees to exercise best efforts to provide the Supplier with technical data that, in the determination of the Supplier, is needed in order to ensure quality of the Service and/or to comply with Federal policy and statutory requirements for information security and the protection of personally identifiable information.

The Customer and the Supplier will negotiate technical data requests on a case-by-case basis.

MANAGEMENT INFORMATION

SERVICE REVIEWS

Agency program representatives from the Supplier and the Customer may review Service performance and management issues as required, typically on a case-by-case basis, but no less frequently than annually. An annual review should occur on or before the conclusion of the 3rd quarter of the Fiscal Year. A request for a service review may be initiated by either party.

An updated SLA, if required, shall be published no later than the conclusion of the 3rd quarter of the Fiscal Year for the purpose of managing service in the upcoming Fiscal Year.

CHANGE PROCESS

Changes to this SLA may be proposed by either the Supplier or Customer Agency primary points of contact cited in Appendix A.

Changes to this SLA that do not increase the annual financial obligation by the Supplier may be managed directly with the designated primary Agency points of contact cited in Appendix A.

Changes to this SLA that result in an increase in the Supplier's annual financial obligations, impart a substantial increase in service, or other major change may be formulated by the designated primary Agency points of contact cited in Appendix A, however, formal clearance and approval processes will be required.

Changes that impact other pre-existing Customer-Supplier agreements shall require the participation and approval of the appropriate program official for both Customer and Supplier.

Where ever practicable, substantive changes to this SLA shall be limited to an annual basis, coincident with the annual Service Review.

Changes to this SLA shall be tracked in the SLA Change History Log, located in the front piece of this document.

PROBLEM MANAGEMENT AND RESOLUTION

The Supplier and the Customer will use Best Effort and Intent to resolve any problems, issues or communications at the local operating location level.

The Supplier and the Customer agree that daily operations issues management, to include service request/trouble report coordination, management, and closure/resolution, are best managed at the lowest responsible organizational level. The Supplier agrees that its supporting contractor (the Supplier's ASC) is authorized for direct interaction for this end.

In the event that the Supplier ASC contractor cannot resolve an issue, gain adequate support to resolve an outage on the needed time scale, or other similar operational management issue, the Customer and the Supplier ASC contractor are to escalate the issue as outlined in the problem escalation protocol defined in Appendix C.

APPENDIX 3 TO ANNEX K TO USPACOM OPORD DEEP FREEZE
SATELLITE COMMUNICATIONS PLANNING

1. Situation. See OPORD.

a. General.

b. Purpose. This appendix outlines satellite communications support planning.

c. Operational Concept. Air traffic control, command control, and weather information is exchanged between JTF-SFA aircraft and Christchurch, NZ and McMurdo Station via UHF channels aboard DOD MILSATCOM payloads on FleetSat and/or UHF Follow-On (UFO) satellites.

d. Resource Availability. Currently, USTRANSCOM SATCOM Database entry designated USTRANSCOM 000173 provides a dedicated 25 kHz channel for this purpose during the flying season. Alternatively, satellite terminal-telephones, such as Iridium, may be used in accordance with appropriate USAF, ICAO, and FAA certifications and USTRANSCOM SDB entry 188.

e. Execution.

(1) Command control and limited In-Transit Visibility information is exchanged among AMC TALCEs and TACC via AMC global C2 voice and data nets using various FleetSat and UFO packages. This support is not specific to ODF and TACC publishes communications plans notifying units of the channel and frequency assignments.

(2) Command, control and administrative traffic are exchanged between US Coast Guard (USCG) operational and administrative sites and USCG icebreakers. When operating in the Antarctic area under command of Commander, Support Forces Antarctica (CJTF-SFA), out of the ordinary SATCOM support is requested by the USCG, and validated by CDRUSPACOM for assignment of channels IAW USPACOM and JCS procedures.

(3) UHF SATCOM requirements include: air traffic control, command control, and weather information exchanges between JTF-SFA aircraft and Christchurch, NZ and/or McMurdo Station.

f. Resources.

(1) Commercial Satellite Resources. RPSC can provide IRIDIUM capability to aircrews for use as backups to the LST 5B.

(2) Military SATCOM Resources. MILSAT resources include LST 5B UHF SATCOM terminals at Christchurch and McMurdo and ARC-210s in C-17 aircraft.

(3) CJSC-Controlled Equipment. N/A.