BY ORDER OF THE COMMANDER
480 INTELLIGENCE SURVEILLANCE
AND RECONNAISSANCE WING (ACC)

480TH ISR WING INSTRUCTION
17-100

8 JUNE 2017

Cyberspace

MISSION SYSTEM INFORMATION
TECHNOLOGY (IT)
SERVICE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **http://www.e-publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 480 ISRW/SCX

Certified by: 480 ISRW/SC
(Lt Col Matthew D. Fisher)
Pages: 21

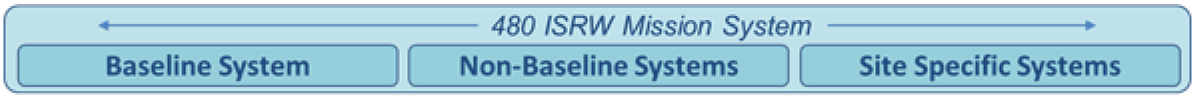
This publication implements Air Force Instruction (AFI) 17- 100, *Information Technology Service Management (ITSM)*. It provides guidance, direction and assigns responsibilities for 480 ISRW Mission System IT Service Management. It applies to all personnel within the 480 ISRW. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. See **Attachment 1** for a glossary of references and supporting information. This instruction reflects the substantial changes made in AFI 17-100 and describes how ITSM will be implemented in the 480 ISRW Mission System Operations.

1. Purpose . This instruction documents responsibilities for managing 480 ISRW Mission System Technology (IT) services. The 480 ISRW Mission System (hereafter interchangeably referred to as the “Mission System” or “System”) is composed of the Air Force provisioned portion of the Distributed Common Ground System (DCGS, i.e., “Baseline system”) as well as the enterprise and site specific non-baseline ISR systems required to support, enable or automate 480 ISRW operational capabilities. Mission System Operations are the actions taken to manage, configure, operate, maintain, defend, sustain or extend any portion, or support the operation of the Mission System. This guidance addresses Mission System operations and product support management performed by 480 ISRW personnel. It excludes Mission System strategy, programming, funding, portfolio planning, and engineering or acquisition activities performed by HQ ACC, 25 AF or the AF DCGS Program Management Office (PMO, i.e., Air Force Life Cycle Management Center Command and Control ISR (C2ISR) Division (AFLCMC/HBG)).

1.1. **Objectives** . The objective of this Instruction is to reduce mission risk and improve Mission System agility and its ability to meet requirements by adopting ITSM practices for Mission System operations, product support management and data center lifecycle management.

1.2. **Mission System** . The 480 ISRW Mission System (**see Figure 1**) is a National Security System (NSS) and Platform IT supporting AF unique IT Governance information capabilities in the Warfighting Mission Areas (WMA) and Defense Intelligence Mission Areas (DIMA). It includes the Air Force provisioned portion of the DCGS consisting of computer hardware and software connected together in a computer network devoted to Tasking, Processing, Exploitation and Dissemination of ISR information. The Mission System evolved from individually engineered and acquired non-baseline stove piped systems to a complex system of systems with over 28 programs managing as many as 60 infrastructure-impacting changes at any one point in time without standardized management responsibilities across all systems. It also includes enterprise site- specific and non-baseline and ISR systems which were developed and have evolved over time to meet operational requirements. This instruction documents product support management responsibilities to support improved management of operational requirements for the entire Mission System.

Figure 1. 480 ISRW Mission System.



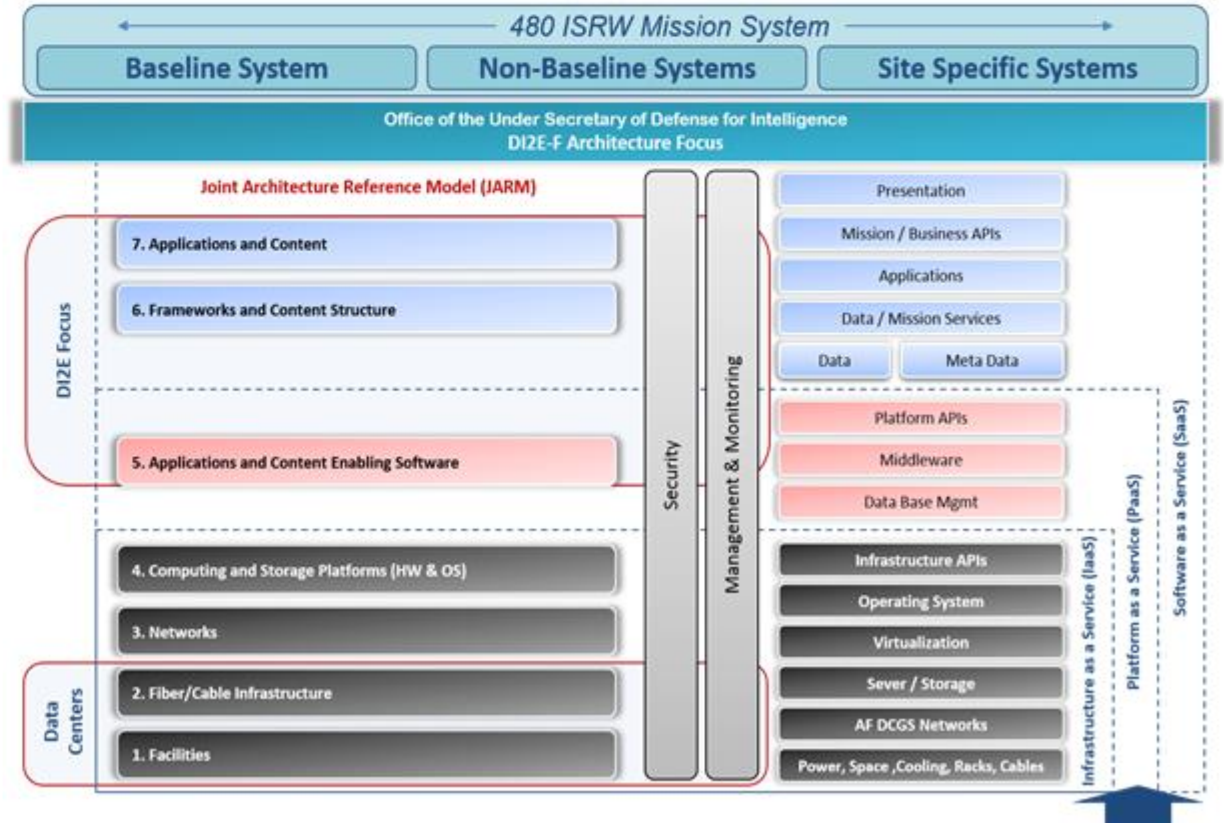
1.3. **Examples of Baseline Systems** : Geospatial Intelligence (GEOINT) Baseline 4.1, Deployable Ground Intercept Facility (DGIF), Deployable Shelterized Segment-Film (DSS-F), Cedallion, Ground Control Processor (GCP), etc.

1.4. **Examples of Non-Baseline Systems** : Combined Enterprise Regional Information Exchange System (CENTRIXS), Consolidated Operations and Information Center (COIC), Collaboration, Command and Control of Processing, Exploitation and Dissemination (C3PED), Communications and Maintenance Control Center (CMCC), DCGS Google Earth Thread Server (DGETS), Unified Collections Operations Reporting Network (UNICORN), United States Battlefield Information Collection and Exploitation System (USBICES), etc.

1.5. **Examples of Site Specific ISR Systems** . Broad Area Synoptic High Resolution Network (BASHRNet), European Command Partner Integration Environment (EPIE), Joint Airborne ISR Exploitation Experiment (JAISREE), Project Diamond, etc.

1.6. **Mission System ITSM Lifecycle**. The 480 ISRW employs the Joint Architecture Reference Model (JARM) to illustrate Mission System components relative to IT services (**see Figure 2).** The JARM was developed by the Defense Intelligence Information Enterprise (DI2E) to describe seven layers of an Intelligence Community (IC) weapon system and depicts the relationship of system layers to IT services. Further, IC Information Technology Enterprise (IC ITE) uses the JARM framework to standardize how IC systems are described and shows the relationship of the system layers to IT services.

Figure 2. The 480 ISRW Mission System and IT Services.

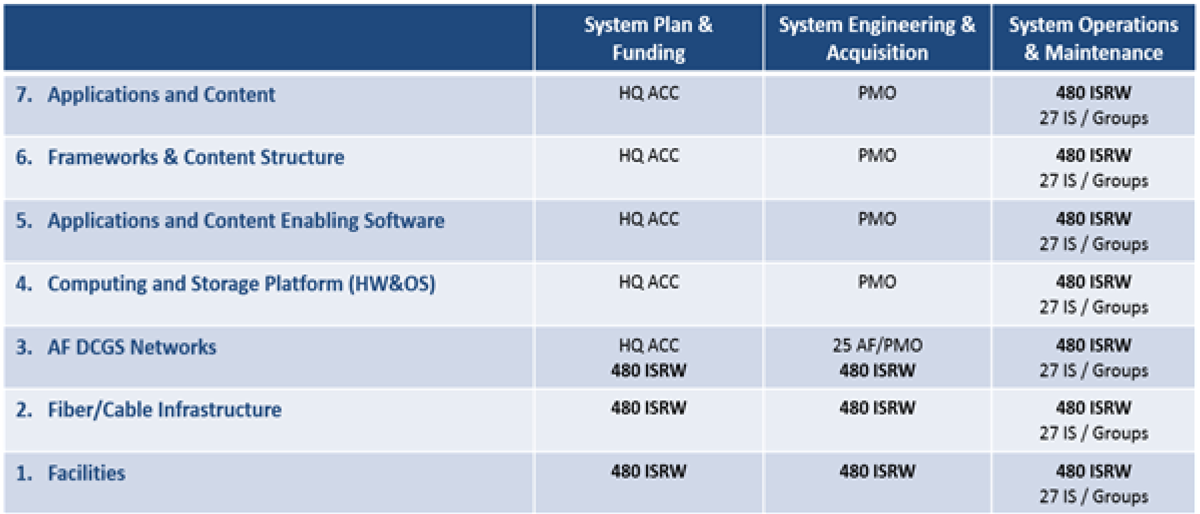

480 ISRW Mission System
Baseline System
Non-Baseline Systems
Site Specific Systems
Office of the Under Secretary of Defense for Intelligence
DI2E-F Architecture Focus
Joint Architecture Reference Model (JARM)
DI2E Focus
7. Applications and Content
6. Frameworks and Content Structure
5. Applications and Content Enabling Software
4. Computing and Storage Platforms (HW & OS)
3. Networks
2. Fiber/Cable Infrastructure
1. Facilities
Data Centers
Security
Management & Monitoring
Presentation
Mission / Business APIs
Applications
Data / Mission Services
Data
Meta Data
Platform APIs
Middleware
Data Base Mgmt
Infrastructure APIs
Operating System
Virtualization
Sever / Storage
AF DCGS Networks
Power, Space ,Cooling, Racks, Cables
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

1.7. **The 480 ISRW Mission System.** It supports three types of IT services: Infrastructure Services (IaaS), Platform Services (PaaS) and Software Services (SaaS).

1.8. **The 480 ISRW Infrastructure IT Service.** This includes data center facilities and fiber/cable infrastructure, power, space and cooling systems; rack infrastructure; networks; and computing and storage that must be collectively available as a whole to host the Mission System. The Infrastructure IT Service sets the maximum level of availability possible for the Mission System Platforms and Software. It is the foundation upon which all other Mission System IT services are built.

1.9. **Distribution of Lifecycle Management Responsibilities** . The responsibilities for the seven layers of the 480 ISRW Mission System and IT Services are illustrated in **Figure 3**. The 480 ISRW is responsible for Layers 1 through 2 and share responsibility for System Plan and Funding with HQ ACC, as well as for System Engineering and Acquisition with 25 AF and the PMO.

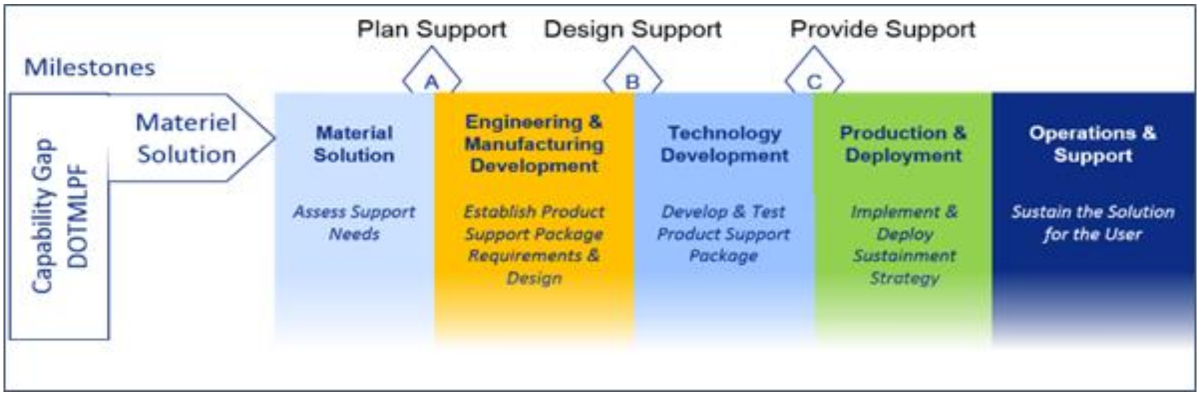
Figure 3. Mission System Lifecycle Management Responsibilities.



	System Plan & Funding	System Engineering & Acquisition	System Operations & Maintenance
7. Applications and Content	HQ ACC	PMO	480 ISRW 27 IS / Groups
6. Frameworks & Content Structure	HQ ACC	PMO	480 ISRW 27 IS / Groups
5. Applications and Content Enabling Software	HQ ACC	PMO	480 ISRW 27 IS / Groups
4. Computing and Storage Platform (HW&OS)	HQ ACC	PMO	480 ISRW 27 IS / Groups
3. AF DCGS Networks	HQ ACC 480 ISRW	25 AF/PMO 480 ISRW	480 ISRW 27 IS / Groups
2. Fiber/Cable Infrastructure	480 ISRW	480 ISRW	480 ISRW 27 IS / Groups
1. Facilities	480 ISRW	480 ISRW	480 ISRW 27 IS / Groups

1.10. **Demarcation between Acquisition and Operational Responsibilities** . The line of demarcation between System Acquisition and System Operation is Acquisition **Milestone C** as shown in **Figure 4**. System Operations processes become actively involved from a process standpoint once the Acquisition Milestone "C" is reached and an introduced system has been developed, produced, and baselined per acquisition process requirements. The 480 ISRW/SC participates in activities and provides input at Milestones B and C; however, prior to base-lining at Milestone C, emergent systems and services fall outside the span of control of 480 ISRW System ITSM operational processes. Mission and System Operations requirements are provided early in the system lifecycle. System Operations Processes become active at Milestone C.

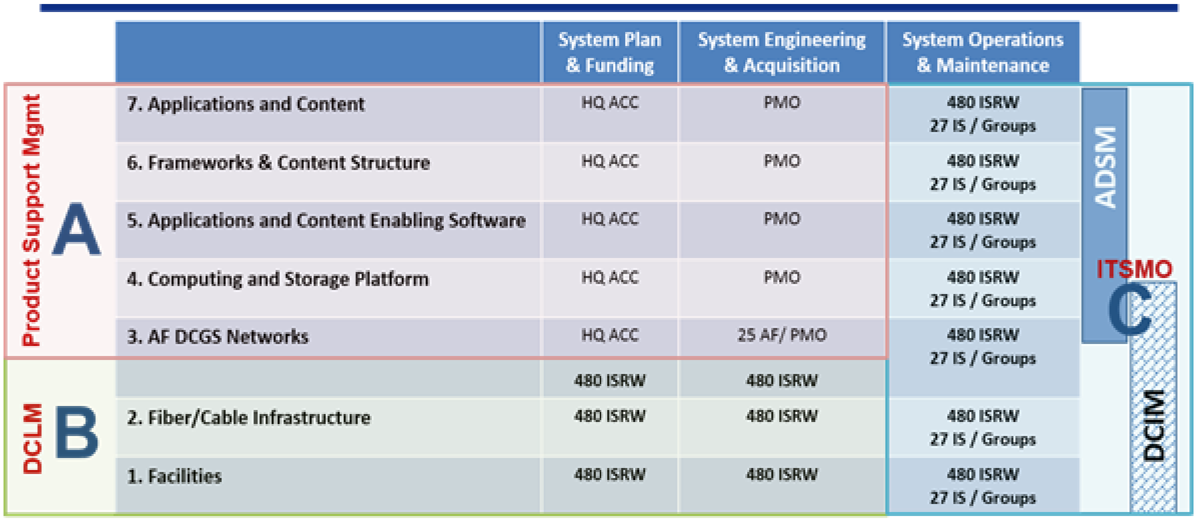
Figure 4. Milestone C Demarcation between Acquisition and Operation.


Plan Support
Design Support
Provide Support
Milestones
A
B
C
Capability Gap
DOTMLPF
Materiel Solution
Material Solution
Assess Support Needs
Engineering & Manufacturing Development
Establish Product Support Package Requirements & Design
Technology Development
Develop & Test Product Support Package
Production & Deployment
Implement & Deploy Sustainment Strategy
Operations & Support
Sustain the Solution for the User

1.11. **Operational Engagement with Acquisition Prior to Milestone C .** Prior to milestone "C", Program management leadership and engineers discuss system planning and design with operational personnel as part of transition planning and support for successful system transitions. As program offices adopt additional Agile practices, there will be more engagement with operational personnel during planning and design. Planned systems, programs and IT services are monitored by operational personnel for situational awareness and future operational responsibilities. Various avenues are utilized to maintain visibility on future systems including attendance at relevant briefings, review of operational requirements definitions, technical exchange meetings, use of supportive technology (e.g.,1067 Tracking System) and case-by-case briefings by project managers resident within applicable Program of Record System Program Offices.

1.11.1. **Figure 5, Area A: Product Support Management.** The 480 ISRW supports HQ ACC, 25 AF, and PMO responsibilities for Layers 3 - 7 System Plan & Funding and System Engineering & Acquisition by providing effective Product Support Management. The 480 ISRW responsibilities in Area A include: Perform System related Operational Risk Management; Submit and Advocate 480 ISRW Operational Requirements; and Collaborate with Responsible Parties for Continual Improvement.

Figure 5. 480 ISRW System Management Responsibility Areas.



	System Plan & Funding	System Engineering & Acquisition	System Operations & Maintenance
7. Applications and Content	HQ ACC	PMO	480 ISRW 27 IS / Groups
6. Frameworks & Content Structure	HQ ACC	PMO	480 ISRW 27 IS / Groups
5. Applications and Content Enabling Software	HQ ACC	PMO	480 ISRW 27 IS / Groups
4. Computing and Storage Platform	HQ ACC	PMO	480 ISRW 27 IS / Groups
3. AF DCGS Networks	HQ ACC	25 AF/ PMO	480 ISRW 27 IS / Groups
	480 ISRW	480 ISRW	
2. Fiber/Cable Infrastructure	480 ISRW	480 ISRW	480 ISRW 27 IS / Groups
1. Facilities	480 ISRW	480 ISRW	480 ISRW 27 IS / Groups

1.11.2. **Figure 5 Area B: Data Center Lifecycle Management (DCLM).** The 480 ISRW is responsible for Data Center Lifecycle Management to provide power, space, cooling and connectivity infrastructure to meet System availability requirements. The 480 ISRW Data Center responsibilities in Area B of Figure 5 include: Capacity Planning; Engineering; System Deployment Planning & Support; Operational Monitoring & Management; and Asset Maintenance & Sustainment.

1.11.3. **Figure 5, Area C: System Operations and Maintenance.** The 480 ISRW is responsible for Mission System Operations and Maintenance. The 480 ISRW with the 27 IS and Groups provide System Operations. The 480 ISRW responsibilities in Area C of Figure 5 include: IT Service Management Oversight; Sustainment Oversight; Operational Service Agreements (OSA); Service Level Agreements (SLA); Memorandum of Understanding and Memorandum of Agreement (MOA) etc.);

Operational use of the Air Force DCGS Service Management (ADSM) system; and the Data Center Infrastructure Management (DCIM) system. The ADSM is a suite of system management tools that support baseline system engineering and acquisition responsibilities. It also supports some operational capability. DCIM is a suite of system management tools that support the management of System data center infrastructure. Both ADSM and DCIM will be used to support management of System related IT Services.

2. Roles and Responsibilities . The 480 ISRW operates and maintains the regionally aligned, globally networked ISR enterprise Air Force Distributed Common Ground System (DCGS) and related site specific and non-baseline ISR systems delivering tailored intelligence for immediate warfighter operations.

2.1. **Group Commanders.** Group Commanders will designate in writing a Communications Systems Officer (CSO) and provide a copy of the designation to 480 ISRW/SC. The CSOs provide System related technical advice to their commanders and will oversee the Mission System ITSM responsibilities.

2.2. **System Customer.** Commanders, Deputy Commanders, Directors of Operations and the Technical Director are System Customers. The System customer has critical operational responsibilities to mitigate System related risk to mission operations and retains these responsibilities no matter what organization manages System operations. They are the **primary stakeholders** of System operations and represent the System users throughout the Wing. To mitigate operational risk related to System operations, these Customer representatives have the following responsibilities:

2.2.1. Direct operations and defense of the System including issuing orders as required to operate and defend the System and direct System operations as required in support of requesting commanders.

2.2.2. Ensure Authorized Service Interruption (ASI) for System IT Services are approved and managed in alignment with AFI 17-201, *Command and Control (C2) For Cyberspace Operations*.

2.2.3. Ensure all Periods of Non-Disruption (POND) for System IT Services are approved and managed in alignment with AFI 17-201.

2.2.4. Evaluate System architecture, management and system capabilities and identify gaps that indicate risk to ISR operations.

2.2.5. Recommend System and ITSM improvements to address identified gaps.

2.2.6. Direct 480 ISRW users in the proper use and operation of the System.

2.2.7. Monitor improvements to System architecture, operational management and system capabilities against requirements, plans and operational priorities and operational goals.

2.2.8. Advise the 480 ISRW/SC regarding System plans, risks, capability gaps, performance issues, opportunities for improvement, operational requirements and operational priorities.

2.3. **The 480 ISRW ISR Systems Division (480 ISRW/SC).** The 480 ISRW/SC provides product support management, data center lifecycle management and operational ITSM oversight. It is responsible for overseeing operational System ITSM (planning support including deployment planning, strategic planning and requirements analysis; implementation including architectures, integration, direction and operational standards to ensure operational stakeholder requirements are met). The 480 ISRW/SC is responsible to govern ITSM operations for the Wing. The Chief of ISR Systems Division, 480 ISRW/SC, is the designated 480 ISRW CSO. The CSO has the following responsibilities:

2.3.1. Provide System ITSM operational governance and decision making.

2.3.1.1. Establish and maintain measurable standards, requirements, goals and objectives for Enterprise and Group ITSM operations and capabilities.

2.3.1.2. Evaluate System support for mission operational requirements, proposed plans and system strategies.

2.3.1.3. Communicate approved System strategies and plans to stakeholders and interested parties with a need to know.

2.3.1.4. Assign product support management roles and responsibilities for all System components.

2.3.1.5. Enable Quality Assurance and the Management Internal Control Toolset (MICT) with ITSM inspection and compliance reporting capabilities.

2.3.1.6. Work with System stakeholders and interested parties with a need to know to establish clearly defined, understood and accepted System ITSM roles and responsibilities.

2.3.1.7. Ensure ISR operational strategies take into account current and future System capabilities and that System plans satisfy current and ongoing ISR plans and strategies.

2.3.1.8. Ensure operational changes adhere to required change management processes and approved architectures.

2.3.1.9. Plan, program and budget for System data center engineering. Establish plans to ensure System infrastructure services meet mission requirements, ANSI TIA 942-A Tier 3 requirements and AF DCGS performance and availability requirements.

2.3.1.10. Provide planning, programming and budget requirements for System operations and maintenance.

2.3.1.11. Establish 480 ISRW System product support management capabilities to identify, collect, document, communicate, advocate, develop specific proposals for, gain acceptance or rejection of and participate in all lifecycle activities for 480 ISRW operational requirements.

2.3.1.12. Ensure System operations comply with all mandatory policies, directives, instructions, legislation and regulations.

2.3.1.13. Clearly define, communicate and enforce required policies and required operational management practices.

2.3.1.14. Evaluate, direct, and monitor the role of contractors and government personnel in System maintenance, management and leadership.

2.3.1.15. Ensure System IT Service OLAs and SLAs are created IAW AFI 17-100, as well as MPTO 00-33A-1001 and this instruction and reviewed by 480 ISRW/SC prior to signature by the commanders of the organizations involved (i.e., commander of provider and commander of receiver) in the SLA or OLA.

2.3.1.16. Use configuration management methods to ensure the integrity and interoperability of systems.

2.3.1.17. Identify and collect new requirements and incorporate in C4ISR infrastructure plans. Coordinate requirements with the ACC systems telecommunications engineering manager.

2.3.1.18. Approve communications and information system infrastructure blueprints, ensure architectural compliance, proper classification and functional support. Ensure appropriate information in the communications and information systems infrastructure blueprints is provided to 480 ISRW and sites' Civil Engineer's office for use in base comprehensive plans and military construction programs.

2.3.1.19. Provide guidance and procedures to identify and communicate special engineering, installation, operations and/or maintenance requirements for NSS, Special Access Programs (SAP) or Sensitive Compartmented Information (SCI) or other federal agency systems connected to the System or System data centers.

2.3.2. Evaluate System ITSM operations based on the 480 ISRW ITSM Framework (**see Paragraph 3**) and applicable DoD, AF, HQ ACC and DCGS related standards.

2.3.2.1. Evaluate operational capability to resolve quality problems, evaluate and analyze deficiencies, identify underlying causes and determine corrective actions.

2.3.2.2. Evaluate System and ITSM operational capabilities, ITSM Quality Assurance (QA) capabilities and ITSM training.

2.3.2.3. Establish product support management, data center lifecycle management and ITSM oversight capabilities.

2.3.2.4. Monitor improvements against approved goals and use of allocated resources.

2.3.2.5. Evaluate operational System ITSM role and responsibility assignments, AF DCGS ITSM related job qualification standards (JQS), training, understanding, acceptance and competence.

2.3.2.6. Evaluate System capacity plans as well as capacity planning effectiveness and efficiency.

2.3.2.7. Evaluate System architectures, risk and performance against requirements and goals.

2.3.2.8. Evaluate the allocation of System resources (human, technical, financial) against operational requirements, architectures, risk and performance.

2.3.2.9. Evaluate the allocation of resources for System maintenance.

2.3.2.10. Evaluate System inventory, supplies and spares.

2.3.2.11. Evaluate System IT services quality.

2.3.2.12. Evaluate System plans, policies and processes.

2.3.2.13. Evaluate System architecture, configuration and management knowledge stored in 480 ISRW knowledge systems.

2.3.2.14. Evaluate System standards completeness, conformance and gaps.

2.3.2.15. Evaluate Service Desk requirements, capabilities, first call resolution rate (FCRR) and first call resolution enablement rate (FCR-ER) from Tier 2 and 3 groups.

2.3.2.16. Evaluate ITSM capabilities and performance.

2.3.2.17. Identify opportunities for improvement to System ITSM cost, risk, quality and performance.

2.3.2.18. Evaluate alternatives for providing System IT services that balance operational risk, cost and agility.

2.3.3. Direct System ITSM operations.

2.3.3.1. Provide and maintain the 480 ISRW ITSM Framework (**see Paragraph 3**) to direct System ITSM operations.

2.3.3.2. Establish a periodic (annually, at a minimum) Wing-level planning forum to discuss current and future issues affecting System components and System related IT services.

2.3.3.3. Produce plans to improve System ITSM cost, risk, quality and performance in support of operational requirements.

2.3.3.4. Require adjustments to plans where capability gaps exist.

2.3.3.5. Provide training and development requirements for ITSM competencies.

2.3.3.6. Ensure that sufficient System inventory, supplies and spares are maintained to support availability requirements.

2.3.3.7. Require that System architecture and management information is stored and managed in 480 ISRW information systems.

2.3.3.8. Establish requirements for System first call resolution rate and the first call resolution enablement rates from Tier 2 and 3 groups.

2.3.3.9. Establish standards for System data center facilities and data center management.

2.3.3.10. Direct the planning and implementation of enterprise and site data center monitoring capabilities.

2.3.3.11. Direct the monitoring, analysis and documentation of data center capacity requirements.

2.3.3.12. Ensure that System power, space and cooling monitoring capabilities provide information required for System capacity analysis, requirements development and planning.

2.3.4. Monitor System ITSM operations.

2.3.4.1. Monitor adherence to system architectures, identified risks and system performance against requirements and goals.

2.3.4.2. Monitor the allocation of System resources (human, technical, financial) against operational requirements, architectures, risk and performance.

2.3.4.3. Monitor the allocation of resources for System maintenance including: inventory, supplies and spares.

2.3.4.4. Monitor System IT services quality and ITSM capability.

2.3.4.5. Monitor System programs and projects to ensure support and ongoing alignment with operational requirements.

2.3.4.6. Monitor the storage and management of system architectures, configuration information and management knowledge in 480 ISRW knowledge systems.

2.3.4.7. Monitor adherence to System standards.

2.3.4.8. Monitor Communications Focal Point Service Desk capabilities, first call resolution rate and first call resolution enablement from Tier 2 and 3 groups.

2.3.4.9. Monitor System ITSM capabilities.

2.3.4.10. Monitor system and management costs, risks, quality and performance.

2.3.5. Provide Data Center Lifecycle Management. System Data Centers (**see Figure 2, JARM Layers 1 and 2**) include System data center facilities, facilities subsystems, racks and cables and network connectivity. System Data Centers provide the power, space, cooling and connectivity required for System operation and support for new or changed System deployments. The 480 ISRW/SC will collaborate with 480 ISRW/CE to plan and program System data center facilities, facility subsystems, and rack and cable infrastructure changes. Planning, engineering and coordination for System data center facilities changes, includes the following activities:

2.3.5.1. Develop plans to ensure System data center facilities achieve American Nation Standards Institute Telecommunications Industry Association (ANSI TIA) 942A Tier 3 level of availability.

2.3.5.2. Ensure System data center facilities achieve availability requirements.

2.3.5.3. Monitor Enterprise and Group level capacity planning to ensure the System has sufficient power, space and cooling to meet availability and performance requirements.

2.3.5.4. Ensure System data center facilities and facilities support systems conform to applicable DoD, AF, and AF DCGS architecture requirements.

2.3.5.5. Ensure System data center architectures contain up to date and accurate facilities architecture information.

2.3.5.6. Support enterprise and local data center operational change control.

2.3.5.7. Ensure data center power, space and cooling monitoring capabilities are effective and support accurate System planning.

2.3.5.8. Ensure System data center facilities conform to applicable DoD, AF, AF DCGS, 480 ISRW and System architectures.

2.4. **The 27th Intelligence Squadron (27 IS).** The 27 IS is the Enterprise IT Service Operations Manager with the following responsibilities:

2.4.1. Establish an enterprise operations System ITSM capability development plan to continually improve enterprise and local site ITSM capabilities a s described in the 480 ISRW ITSM Framework **(See Paragraph 6**).

2.4.1.1. Assign a 27 IS CSO, data center managers and process managers as needed for operational ITSM processes.

2.4.2. Establish enterprise and local System infrastructure change and configuration management capabilities to ensure reliable and stable infrastructure operations that meet mission and System requirements.

2.4.3. Establish agreements with all hosted systems documenting operational change and configuration control responsibilities.

2.4.4. Establish System infrastructure service agreements between the Wing and responsible application managers covering all hosted systems.

2.4.5. Monitor System IT service performance and report service results to 480 ISRW/SC and the owning site/applicable Group.

2.4.6. Configure System ITSM and DCIM process infrastructure and information systems to provide management information needed for knowledge, configuration and change management.

2.4.7. Configure DCIM tools and process infrastructure to collect information needed for effective capacity planning, respond to operational events and incidents, and analyze and report operational results.

2.4.8. Manage System stakeholder relationships.

2.4.9. Operate and sustain the System infrastructure.

2.4.9.1. Participate in System design to promote sustainable solutions.

2.4.9.2. Provide affordable, reliable and effective support to meet performance, availability and security requirements.

2.4.9.3. Validate and verify system engineering design and measure the performance of the support operations.

2.4.9.4. Provide effective enterprise System ITSM capabilities with the minimal logistics footprint (e.g., the measurable size or "presence" of logistics support, including manpower, required to deploy, sustain, defend and move/add/change System components).

2.4.9.5. Develop integrated, streamlined operational processes.

2.4.9.6. Facilitate iterative technology enhancement during the System life cycle.

2.4.9.7. Provide support necessary to sustain the readiness and operational capability of the System infrastructure.

2.4.10. Monitor enterprise and local System power, space and cooling.

2.4.11. Monitor enterprise and local System computing, storage, network and virtualization services and system component availability, performance and capacity.

2.4.12. Establish enterprise and local operational configuration and change control of the System infrastructure.

2.4.13. Manage cybersecurity in accordance with applicable higher headquarters and 480 ISRW standards and requirements.

2.4.14. Collect information needed for System capacity planning.

2.4.15. Analyze operational results, planned changes and releases, strategic roadmaps and mission requirements to understand availability, performance and capacity requirements.

2.4.16. Provide System infrastructure capacity reporting to 480 ISRW/SC.

2.4.17. Review proposed plans with stakeholders to ensure that the plans support mission requirements and mission plans take into consideration current and planned System capacity.

2.4.18. Document the predicted and actual performance of the System infrastructure including component and resource utilization with estimates of future workload and capacity requirements for the enterprise. Perform predictive analysis to determine when and how much additional capacity should be acquired with references to proposals and cost estimates for recommended solutions. Provide proposed enterprise capacity plans to 480 ISRW/SC at least annually with additional updates if System capacity requirements change.

2.4.19. Provide System consulting for infrastructure impacting projects throughout the lifecycle from requirements through development, integration into the operational environment and post implementation operational review.

2.4.20. Develop the System infrastructure Asset Management Plan and manage System assets according to the plan. The asset management plan should define the strategy, management and technical processes for asset management. It also should define an asset classification scheme, the asset storage, handling and retrieval mechanism; and asset acceptance, certification, and retirement procedures.

2.4.21. Perform enterprise service management processes and functions in accordance with the 480 ISRW ITSM Framework (**see Paragraph 3**).

2.4.21.1. Enterprise System Server Management

2.4.21.2. Enterprise System Storage Management

2.4.21.3. Enterprise System Network Management

2.4.21.4. Enterprise System Cybersecurity Operations

2.4.21.5. Enterprise System Virtualization Management

2.4.21.6. 480 ISRW User Desktop and Mobile Asset Management

2.4.22. Support the Communications Focal Point by providing sufficient System information to enable agreed First Call Resolution and First Call Resolution Enablement Rates.

2.4.23. Provide enterprise System infrastructure reporting for stakeholders in alignment with 480 ISRW ITSM Framework (**see Paragraph 3**).

2.4.24. Coordinate with Group System IT service operations for all changes, incidents and problems that impact more than one site or enterprise operations.

2.4.25. Designate an enterprise service desk manager to coordinate with the 480 ISRW/SC and Groups to manage the enterprise System service desk information needed to achieve an agreed first call resolution rate (**See Paragraph 2.3.3.8**).

2.5. **Communications Focal Point (CFP).** Within the 480 ISRW ITSM roles and responsibilities, the CFP function is performed as described in Methods and Procedures Technical Order (MPTO) 00-33A-1001, *General Cyberspace Support Activities Management Procedures and Practice Requirements*, and is the System Service Desk. The CFP will provide a standardized and integrated CFP function that provides enterprise and local service desk capabilities. A 480 ISRW/SC waiver is required for other arrangements. The CFPs or other authorized arrangements will be designated at the 27 IS and Groups with the following responsibilities:

2.5.1. The 27 IS CFP will coordinate with Groups to develop and maintain enterprise system service desk FCRR and information management plans and submit them to 480 ISRW/SC for approval prior to execution. The enterprise plan takes into account all standard or non standard service desk arrangements and works towards standardization, shared information and improved FCRR at all locations.

2.5.2. The 27 IS CFP will manage enterprise service desk information and access to the service desk information system. The System service desk information system is an integrated solution made up of portions of ADSM, DCIM and other System ITSM tools.

2.5.3. The 27 IS and Group CFPs will tag every knowledge entry within the System service desk information system with the attributes listed in **Figure 6** at a minimum:

Figure 6. Knowledge Solution Attributes.

Attribute	Description
Knowledge Solution Type	1. **Type 1** The CFP should be able to resolve 100%. 2. **Type 2** The CFP should never be able to resolve and always requires escalation due to specialized knowledge, security clearance, data access or other specified constraint. 3. **Type 3** CFP should be able to resolve at least 50%. Additional specified information is to be collected and documented prior to escalation or assignment to higher tier support functions. 4. **Type 4** A known error with no currently available solution. 5. **Type 5** An unknown error with no available solution documentation.
Symptom Description	A description of common user identifiable characteristics of an incident or problem that the solution addresses.
Solution	Guidance for resolving the incident or request.
Escalation Guidance	Guidance for additional information to be collected prior to escalation and any business rules that apply to escalation.
System or Service	Systems and IT Services related to the Knowledge Solution
Related CI's and Assets	Configuration Items and IT Assets related to the Knowledge Solution
System Owner	Contact information for the controlling authority for the System related to the Knowledge Solution
Higher Tier Contacts	Contact information for Higher Tier contacts
Knowledge Solution Owner	Contact information for who manages the Knowledge Solution content.
Solution LoE Estimate	Estimated average level of effort to carry out the described solution (time, labor, system resources required to perform the solution)

2.5.4. Enterprise and Group CFPs will identify and track the knowledge solution used on each call, incident and request.

2.5.5. 27 IS Enterprise Operations and Group Operations CFPs will measure and report FCRR, FCR-ER, information system knowledge completeness, use, value and capability gaps including the reporting requirement listed in **Figure 7.** Achieving these results will require assigning knowledge management responsibilities and configuring the service desk information system in alignment with enterprise service desk management plans.

Figure 7. FCRR Reports.

Report	Description
Volume	Call, incident and request volume, trends, forecast
Solution Volume	The #, % Knowledge Solutions by Knowledge Solution Type, System, Service and higher tier function
Solution Usage Volume	# and % of calls, incidents and requests with a documented solution
Solution Gaps	# of calls, incidents or requests with no documented solution
Top Ten List	Top 10 knowledge solutions required to improve FCRR, an estimate of the improvement once the solutions are developed and available, and operational impact and value of the FCRR improvement
	FCRR & FCR-ER for each higher tier function
FCR-ER	Stack ranking for FCR-ER by System, Service and higher tier Groups with a description of the operational impact of gap between the agreed FCRR and the actual FCR-ER

2.6. **The Communications, Logistics and Systems (CLS) Units.** All CLS units assigned within the Groups and 27 IS (as applicable) will manage their Group's System ITSM operations, data center management and requirements management. The Group Commander will assign the CSO, normally the CLS Commander. The CSO will assign responsibilities for System IT service operations, data center management, System requirements management and representing Group requirements to the 480 ISRW/SC (i.e., the Wing CSO) in periodic Wing level System planning. Group CSO responsibilities include:

2.6.1. Document responsibility assignments for Group System data center management, System IT service operations, installation, maintenance and sustainment in a support agreement or in a Service Level Agreement (SLA) as applicable. Ensure SLAs are reviewed by the 480 ISRW/SC prior to signature.

2.6.2. Ensure System reliability through effective integration planning, operational change control and contingency planning.

2.6.3. Ensure conformance to System Architectures and Standards.

2.6.4. Ensure appropriate training for all Group assigned communications and information personnel with ITSM responsibilities.

2.6.5. Develop Group communications, information annexes, appendices, contingency plans, support plans and reporting. Review and assist with the development of tenant plans involving communications and information resources or activities.

2.6.6. Identify and collect communications and information systems infrastructure requirements and incorporate into the Cyberspace Infrastructure Planning System (CIPS) base communications and information systems blueprint, as necessary.

2.6.7. Coordinate Group's System communications and information systems blueprint with the host wing and other tenant units. Ensure the communications and information systems blueprint in CIPS, the installation comprehensive plan, and military construction programs complement each other (see AFI 32-7062, Air Force Comprehensive Planning).

2.6.8. If the commander delegates, serve as group-level approval authority for the Implementation Document and other requirements documents submitted for implementation of communications and information systems.

2.6.9. Serve as the overall interface with the base Science, Technology, Engineering and Mathematics workforce (STEM-B) to establish priorities and render decisions concerning the base communications and information infrastructure.

2.6.10. Manage System communications and information projects.

2.6.11. Manage a master file of Communications and Information Systems Installation Records (CSIR) for Group supported systems or facilities.

2.6.12. Manage Group infrastructure, host systems, and other systems as defined in support agreements, and establish a systems integration function.

2.6.13. Allocate group resources to conduct System operational activities.

2.6.14. Monitor Group System operation, performance, availability, changes, conformance with requirements, compliance with standards and risk.

2.6.15. Manage operational change control for Group's System infrastructure.

2.6.16. Maintain operational configuration information for the Group's Mission System.

2.6.17. Oversee the Group's Mission System infrastructure management control, a client service center communications focal point, network management, server administration and network information assurance services.

2.6.18. Provide technical and systems support for Mission System communications and computer systems.

2.6.19. Field and maintain local site Mission System infrastructure.

2.6.20. Perform monitoring and event management for the Group's Mission System infrastructure: servers, storage, network, virtualization, cables, data center power and cooling.

2.6.21. Perform Group service management processes and functions in accordance with the 480 ISRW ITSM Framework (**See Paragraph 3**), including:

2.6.21.1. The Group's Mission System Server Management.

2.6.21.2. The Group's Mission System Storage Management.

2.6.21.3. The Group's Mission System Network Management.

2.6.21.4. The Group's Mission System Cybersecurity Operations.

2.6.21.5. The Group's Mission System Virtualization Management.

2.6.21.6. The Group's User Desktop and Mobile Asset Management.

2.6.22. Perform System and ITSM quality assurance to resolve quality problems, evaluate and analyze deficiencies and problem areas to identify underlying causes and recommend corrective actions.

2.6.23. Report System ITSM information to stakeholders with a need to know.

2.6.24. For all hosted systems not managed by Group or 27 IS CLS units, SLAs/OLAs will be established documenting these responsibilities. Submit draft SLAs/OLAs ready for signature to the 480 ISRW/SCX org box (e-mail to: **480ISRWGXCX@us.af.mil**). After 480 ISRW/SC review, units may proceed with signatures and provide 480 ISRW/SCX org box with a copy of the final agreement.

2.6.25. Coordinate with the 27 IS, the enterprise IT service operations manager, for all changes, incidents and problems that impact more than one site or have an enterprise impact.

2.7. **Functional Systems Administrator (FSA).** FSAs will:

2.7.1. Provide an interface between program representatives and the CFP, the data center manager and the 27 IS as needed to support infrastructure IT service changes to shared or virtual infrastructure or other Mission System related data center service changes.

2.7.2. Create an SLA, OLA or MOA, as applicable for any transfer of administrative or support responsibilities to the CFP, the data center manager and the 27th IS as required to achieve required FCRRs, FCR-ERs or to support infrastructure IT service changes to shared or virtual infrastructure or other System related data center service changes.

2.7.3. Provide sufficient knowledge to the CFP to enable an agreed first call resolution rate.

3. The 480 ISRW IT Service Management Framework . The 480 ISRW ITSM Framework documents AF ITSM process and process capability assessment standards for System operations. It is maintained by the 480 ISRW/SC in an information system that supports enterprise access to all System stakeholders with a need to know. The framework includes the System operational ITSM process model and process capability assessment. The 480 ISRW ITSM Framework is not maintained in this instruction to enable it to continually improve as System ITSM capabilities evolve. Contact the 480 ISRW/SCX (e-mail: **480ISRWGXCX@us.af.mil**) for access.

JASON M. BROWN, Col, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 17-100, *Information Technology Service Management*, 16 September 2014

AFI 33-360, *Publications and Forms Management*, 01 December 2015

MPTO 00-33A-1001 *General Cyberspace Support Activities Management Procedures and Practice Requirements*, 1 May 2014

Abbreviations and Acronyms

ACC—Air Combat Command

ADSM—Air (A) Force Distributed (D) Common Ground System Service (S) Management (M) System

AFLCMC/HBG—Air Force Lifecycle Management Center/Command, Control Intelligence, Surveillance and Reconnaissance (C2ISR) Division

ANSI TIA—American National Standards Institute, Telecommunications Industry Association

CFP—Communications Focal Point

CIPS—Cyberspace Infrastructure Planning System

CLS—Communications, Logistics and Systems

CSO—Communications Systems Officer

DCGS—Distributed Common Ground System

DCIM—Data Center Infrastructure Management

DI2E—Defense Intelligence Information Enterprise

FCRR—First Call Resolution Rate

FCR-ER—First Call Resolution Enablement Rate

FSA—Functional Systems Administrator

IC ITE—Intelligence Community Information Technology Enterprise

ITSM—Information Technology Service Management

JARM—Joint Architecture Reference Model

MOA—Memorandum of Agreement

NSS—National Security System

PaaS—Platform-as-a-Service

PMO—Program Management Office

SLA—Service Level Agreement

SPO—System Program Office

WMA— Warfighting Mission Areas

Terms

Baseline System—The Air Force provisioned portion of the Distributed Common Ground System, the AN/GSQ-272 Sentinel System. Although officially designated a "weapons system," it consists of computer hardware and software connected together in a computer network devoted to processing and dissemination of Intelligence, Surveillance, and Reconnaissance (ISR) information. The baseline system meets a portion of 480 ISRW operational requirements for ISR systems.

First Call Resolution Rate—The first call resolution rate (FCRR) is the percent of calls or contacts that are resolved by the service desk on the first interaction with the caller. The First Call Resolution Enabalenment Rate (FCR-ER) is the percent of calls or contacts that the service desk has been provided knowledge solutions for to enable them to resolve on the first contact.

Mission System—The Mission System is a group of ISR systems that collectively provide the complete set of IT services that support, enable or automate operational ISR capabilities within 480 ISRW. The mission system includes the Air Force provisioned portion of the Distributed Common Ground System (the Baseline System) as well as enterprise and site specific non-baseline ISR systems required to support, enable or automate 480 ISRW operational capabilities. It includes all of the systems that are required to meet operational mission requirements. The mission system must operate effectively as a system of systems to support ISR information processing, exploitation and dissemination mission tasking requirements. Example Baseline Systems: APS, IQ, CIES, CIP, DSS-F, DTS, IESS, SYERS, TARS, FTU, CETS, DGIF. Example non-baseline ISR systems: ACES HY, CENTRIX, COIC, C3PED, CMCC, DGETS, UNCORN, USBICES, WEBTAS, Wolverine. Example Site Specific ISR Systems: BASHRNet, EPIE, JAISREE, PASS-K, Project Diamond, PRT.

Non Baseline Systems—. The non-baseline systems are systems that were developed to meet operational ISR requirements because the baseline system did not meet all of the 480 ISRW requirements. Example non-baseline ISR systems: Airborne Cueing and Exploitation Hyperspectral (ACES HY), Combined Enterprise Regional Information Exchange System (CENTRIXS), Consolidated Operations and Information Center (COIC), Collaboration, Collaboration, Command and Control of Processing, Exploitation and Dissemination (C3PED), Communications and Maintenance Control Center (CMCC), DCGS Google Earth Telemetry System (DGETS), Unified Collections Operations Reporting Network (UNICORN), United States Battlefield Information Collection and Exploitation System (USBICES), Wolverine, etc.

Service Desk Information System—A 480 ISRW information system for managing System service desk information needed to achieve an agreed first call resolution rate (FCRR).

Service Desk Tiered Levels of Support—Tier 1, sometimes called Level 1 or First Line support are the service desk agents that log calls, attempt to resolve calls on the first contact based on available knowledge. When the incidents or requests cannot be resolved they are escalated to Tier 2, also called Level 2 or Second Line Support. Tier 2 support is made up of support technicians with specialized skills, clearance or system access. They provide support for one or more specific systems. If Tier 2 support cannot resolve the incident or request the issue is escalated to Tier 3 support, also called Level 3 or Third Line support. Tier 3 support is made up of application developers, OEMs or other third parties.

Tier 1 or 1st Level Support:—Tier 1 Support - logs receives calls and attempts to resolve incidents and requests.

If there is no available— knowledge solution, the issue will be transferred to Tier 2 Support.

Tier 1 keeps users— informed about their status at agreed intervals.

Tier 2 or 2nd Level Support:—Tier 2 Support takes over Incidents which cannot be solved at Tier 1.

If necessary— it will request external support, e.g. from software or hardware manufacturers.

If no solution—can be found, the the incident is escalated to Tier 3.

Tier 3 or 3rd Level Support:—Tier 3 Support is typically located at hardware or software developers, OEMs or third-party suppliers.

Its services are—requested by Tier 2 if required for solving an Incident.

Site Specific Systems—Site specific non-baseline ISR systems developed to meet local mission requirements because the baseline system did not meet all of the local mission requirements. Example Site Specific ISR Systems: Broad Area Synoptic High Resolution Network (BASHRNet), European Command Partner Integration Environment (EPIE), Joint Airborne ISR Exploitation Experiment (JAISREE), PASS-K, Project Diamond, PRT, etc.

Special Purpose Processing Node (SPPN)—A fixed data center supporting special purpose functions that cannot (technically or economically) be supported by CDCs or IPNs due to association with infrastructure or equipment (e.g., communication and networking, manufacturing, training, education, meteorology, medical, modeling & simulation, test ranges, etc.). No general purpose processing or general purpose storage can be provided by or through a SPPN. SPPNs do not have direct connection to the Global Information Grid (GIG); they must connect through a CDC or IPN. (DoD CIO memorandum, "Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration," 11 July, 2013)

System Stakeholders—For the purposes of this document, stakeholders in System operations are: HQ ACC, 25 AF, 480 ISRW Commanders, Deputy Commanders, Directors of Operations, the 480 ISRW Technical Director, 480 ISRW/SC 27 IS and Group Leadership.