



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY
REFER TO: Joint Interoperability Test Command (JITC)

2 Mar 09

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Calendar Year 2008 Joint Interoperability Test Command (JITC) Interoperability Status Report

Reference: Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008

1. As required by CJCSI 6212.01, JITC is providing an annual report, enclosure 1, summarizing calendar year (CY) 2008 system interoperability test certification status.
2. During CY 2008, JITC supported 244 test activities involving 154 Department of Defense (DoD) systems. During this period, JITC issued 328 interoperability testing and certification related products: 161 Joint Interoperability Test Certifications; 9 Extension of Joint Interoperability Test Certifications; 69 Standards Conformance Certifications; 2 Standards Conformance Non-Certification; 70 Joint Interoperability Assessments; and 17 Standards Conformance Assessments.
3. This report describes the general methodology JITC used to determine interoperability status and summarizes interoperability status throughout DoD. Additional information is located at <http://jitic.fhu.disa.mil> and in our reports database at <http://jit.fhu.disa.mil/>.
4. The point of contact for this report is Ms. Susie Puffer, commercial (520) 538-0471, DSN 879-0471, or e-mail: lia.puffer@disa.mil. The mailing address is: Joint Interoperability Test Command, P.O. Box 12798, Fort Huachuca, Arizona 85670-2798.

for RONALD C. STEPHENS
Colonel, USA
Commander

1 Enclosure a/s

JITC Memo, JT, Calendar Year 2008 Joint Interoperability Test Command (JITC)
Interoperability Status Report

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT),
SAIS-IOQ

U.S. Marine Corps MARCORSSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities
Division, J68

CALENDAR YEAR 2008 JITC INTEROPERABILITY STATUS REPORT

OVERVIEW

This report complies with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01, "Interoperability and Supportability of Information Technology and National Security Systems:" The Defense Information Systems Agency (DISA) publishes an annual report containing a summary of systems tested for Information Technology (IT) and National Security Systems (NSS) interoperability by functional area.

JITC issued 328 interoperability testing and certification related products in 2008. (See Table 1 for details.) In addition, JITC supported other Joint Staff initiatives, such as the review of 78 Test Exemption and 26 Information Support Plan (ISP) and Legacy Waiver requests. JITC also processed 396 Interim Certificate to Operate (ICTO) requests in support of the Military Communications-Electronics Board (MCEB) Interoperability Test Panel (ITP).

JITC identifies key systems through various sources, including systems lists put together by the Office of the Secretary of Defense (OSD), Joint Forces Command (JFCOM), Combatant Commanders, and Assistant Secretary of Defense (Networks and Information Integration) (ASD (NII)). Current system information sources include the Office of the Secretary of Defense (OSD) Test and Evaluation Oversight List, the DoD Information Technology Portfolio Repository (DITPR), the Joint Command, Control, Communications, Computers and Intelligence (C4I), Program Assessment Tool-Empowered (JCPAT-E), the JITC System Tracking Program (STP) (<https://stp.fhu.disa.mil>), and the JITC Joint Interoperability Tool (JIT) (<http://jit.fhu.disa.mil>).

JITC regularly supports Combatant Command contingencies and exercises; this helps identify systems not on the various DoD tracking lists. JITC uses Combatant Command liaisons and JITC-assigned subject matter experts to identify other systems requiring interoperability testing and certification. JITC uses this approach to identify systems requiring interoperability certification due to the lack of a mature and fully populated DoD system registry.

SYSTEM TRACKING PROGRAM (STP)

The STP provides access to system, testing, and joint interoperability certification information, to include capabilities document citations, test plans, test reports, ICTO memoranda, and interoperability testing and certification related documents. The STP tracks a system's progress towards Joint Interoperability Test Certification. The STP tracked 1,800 active systems throughout 2008, and has 962 user accounts; 464 assigned to external customers such as the services, Combatant Commanders, Director, Operational Test & Evaluation (DOT&E), Joint Staff, and the General Accountability Office.

NET-READY KEY PERFORMANCE PARAMETER (NR-KPP)

The DoD continues to focus attention on interoperability and NR-KPP test and certification. The elements of the NR-KPP continue to evolve, but remain a testing challenge as we face a lack of Joint integrated architectures, Community Of Interest (COI) data strategy and service governance, Key Interface Profile (KIP) configuration management, and availability of validated reference implementations. During the reporting period, JITC assisted in revising CJCSI 6212.01, which redefines the elements of the NR-KPP. JITC provided comments on all sections of 6212, and revised the section specific to JITC test and certification to align with other changes in interoperability policy.

Accommodating changes to the NR-KPP will remain a challenge, as many of the reworked NR-KPP elements are new or still not fully mature. The impact will affect evaluation of net-centricity (going from a Net-Centric Operations and Warfare Reference Model (NCOW RM) basis to the DoD Information Enterprise Architecture (IEA) guidance), standards conformance with Global Information Grid (GIG) Technical Guidance (GTG)/GIG Enterprise Service Profile (GESP) vs. KIPs, and adds new reporting requirements for supportability issues such as Global Positioning System (GPS), Selective Availability Anti-Spoofing Module (SAASM), spectrum, and Joint Tactical Radio System (JTRS) compliance. An additional factor that must be addressed is the evolution of the DoD Architecture Framework (DoDAF) to version 2.0, with many new requirements to handle net-centric architecture artifacts. Of course, JITC will continue to work with the Joint Staff and other stakeholders to improve and mature all of the joint interoperability processes.

NET-CENTRIC TESTING

The DoD continues the migration to a Net-Centric architecture. JITC has been working to support a variety of key Net-Centric initiatives across the DoD to include:

- The development of Enterprise-level test metrics for assessing compliance with Net-Centric Data and Services Strategies and the Defense Information Enterprise Architecture.
- The execution of Net-Centric assessments during Enterprise and COI-level Net-Centric Data and Service Pilots.
- Close coordination with a variety of COIs in the development of data strategies, architectures and standards implementation profiles to promote interoperability.
- Strategic partnerships with DoD Capability Portfolio Managers, providing information to decision makers on the state of net-readiness within their portfolios to feed acquisition investment decisions.

SOA & NET-CENTRIC INSTRUMENTATION

JITC has invested in developing a core capability for instrumenting web service: Service-Oriented Architecture (SOA) based capabilities. There are several areas where JITC is focusing efforts to build an effective integrated web service testing capability. The primary focus areas are as follow:

- **Acquire training.** JITC contractor and government staff were trained on Commercial-off-the-Shelf (COTS) tools by commercial venders for web service testing. Most of this training occurred in FY08 and FY09. The primary training was on:
 - AmberPoint (SOA Management Systems), used for GIG SOA Enterprise Service Management (ESM)
 - iTKO LISA, used for web service testing
 - SOATest, used for web service testing
 - HP LoadRunner and SOA testing products

In addition to vendor training, other open source tools such as soapUI, eXtensible Markup Language (XML) Spy and Web Services - Interoperability (WS-I) organization Test Tools were used to access Web Service Description Language (WSDL) service descriptions, and develop web service operation calls, capture Simple Object Access Protocol (SOAP) requests and responses, and provide “proof of concept” testing for XML validation and WS-I conformance.

AmberPoint training has provided JITC the background for collaboration with DISA and AmberPoint to implement Test and Evaluation capabilities into the ESM architecture of the Net Centric Enterprise Services (NCES) SOA Foundation products. This may have one of the greatest potential returns on investment to DISA, JITC, and the service component Programs of Record (POR) in enabling an enterprise-wide capability for Test and evaluation (T&E) in both developmental and operational testing,

- **Supporting customer requirements.** JITC supports customer requirements for net-centric testing by supporting web service testing efforts on various programs, with two key programs being NCES and Net Enabled Command Capability (NECC). JITC has developed a set of core capabilities by demonstrating the ability to access and instrument web services (Defense Connect Online (DCO), Universal Description, Discovery, and Integration (UDDI), MetaData Registry (MDR), etc.) from JITC. JITC developed the capability to capture web service operations data for the purposes of executing distributed NR-KPP validation/conformance testing. JITC instrumented testing of available NCES core services and NECC Capability Modules on operational and test networks respectively. Various COTS and Government-off-the-Shelf (GOTS) tools are being used to access web services and provide "proof of concept" testing for NR-KPP conformance.
- **Collaboration with industry and academia.** JITC works with industry and academia through current contract vehicles, and by reaching out in collaboration with groups such as the Web Service Test Forum (WSTF) and the DoD Multi-Service SOA Consortium (MSC). By actively reaching out to industry and academia, JITC is developing the

relationships and social networks required to solve the problems related to web service T&E. These efforts are expanding JITC core capabilities by allowing JITC to bring in the subject matter expertise to help solve the complex problems with web service interoperability.

- **Modeling and Simulation (M&S) Verification, Validation and Accreditation (VV&A).** JITC supports internal and external customers with VV&A of M&S and web service tools used in developmental and operational testing. JITC is using Department of Defense Standard Practice Documentation of Verification, Validation and Accreditation, for Models and Simulations, MIL-STD-3022. JITC involvement with academia has greatly enhanced our capability to provide critical input to PORs by leveraging expertise within the University of Arizona and Arizona State University to evaluate M&S by internationally recognized subject matter experts in the field.

CERTIFICATION PROCESS IMPROVEMENT

JITC has taken several steps this year in working to improve both the quality and timeliness of certification documentation. As part of a two-phased approach to improve the certification process, JITC first set-up a workflow process using STP, the Policy Group review, and the Electronic Report Distribution (ERD) system to track part of the process flow.

Later this year, after considering several applications, JITC selected the Ultimus Adaptive Business Process Management (BPM) Suite to implement a pilot of an automated workflow to improve upon the initial workflow process established.

The Ultimus Adaptive BPM Suite is an enterprise software application designed to create an operational environment that will allow JITC to automate and improve the current document tracking process. The product's multiple modules will assist in seamlessly integrating the multiple application and review phases involved, and will support the needs of JITC stakeholders including management, policy, business office, and action officers.

The Ultimus BPM Suite employees modeling, analysis, and optimization capabilities throughout the development and operational timeframe deployed in easy-to-use graphical interfaces. The reporting and Business Activity Monitoring (BAM) are tailored to management and presented through performance dashboards, e-mail, desktop gauges or within process forms. JITC will be moving out with this effort in early 2009, and expects to expand the capability to the majority of JITC produced documents by year end.

INTEROPERABILITY STATUS

Reporting the interoperability status of DoD IT, including NSS, is impractical in the current environment as there is no complete, authoritative listing of such systems available. As a preliminary step towards reporting that information, JITC has examined the DITPR to develop a list of Acquisition Category (ACAT) I systems. Where possible, those have been associated with

corresponding entries in JITC’s STP and their status with respect to interoperability-related actions, i.e., interoperability certification or assessment, standards conformance certification or assessment, legacy waivers, or test exemptions, has been determined.

Through this process, 285 ACAT I DITPR program records were identified, of which 99 (35%) had corresponding STP entries. Figure 1, below, provides the specific numbers of programs/systems for which some interoperability effort has been accomplished for each type of action, broken down by ACAT I subcategories.

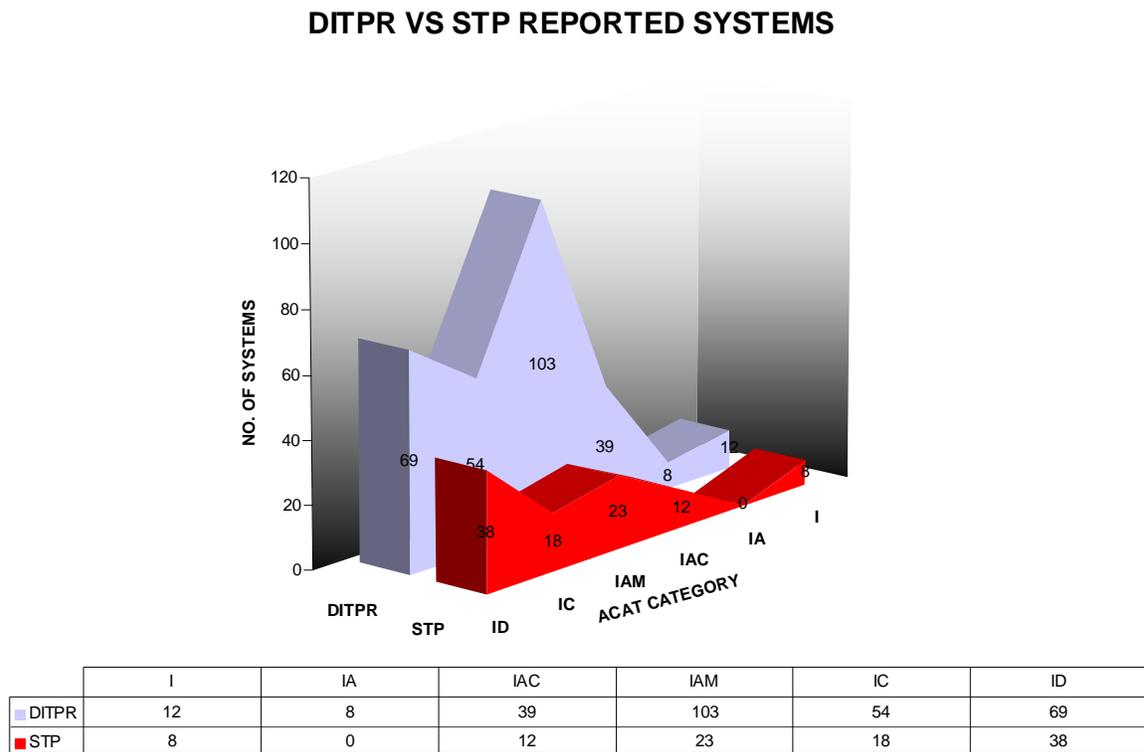


Figure 1. DITPR Records Matching STP Entries.

Figure 2, shows these programs/systems by type of activity (certification, ICTO, etc.). Some of the DITPR records may represent new systems that have not appeared on the interoperability radar because acquisition and development have not reached the appropriate milestones. Others may represent legacy systems or systems without joint interfaces (at least in current increments). However, a preliminary analysis indicates that the majority probably do have joint interoperability capabilities that should be addressed. (Note that one program, CITS, had approximately 50 separate DITPR records and is depicted with crosshatching to avoid distorting the overall interoperability picture. It should also be noted that at least some portions of CITS have been undergoing recent testing by JITC.)

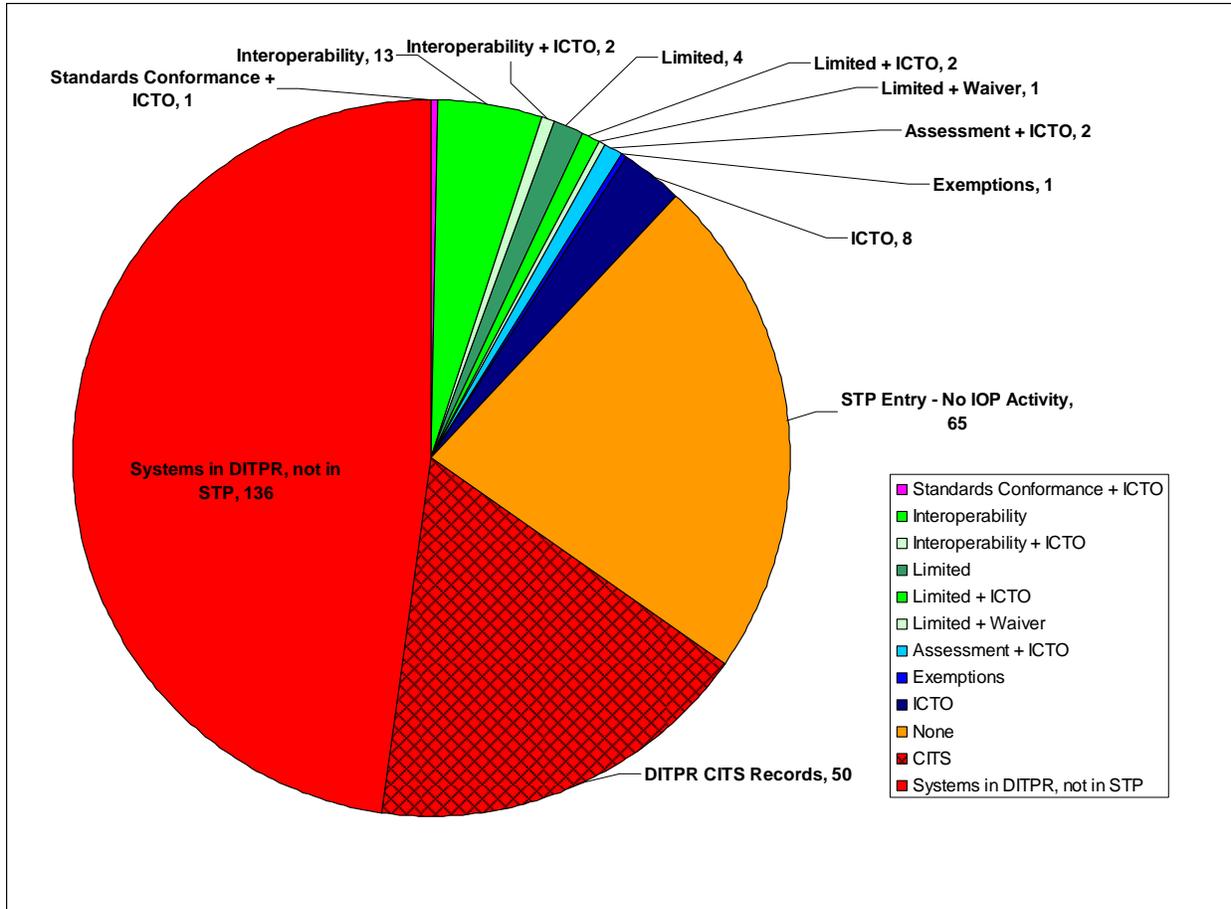


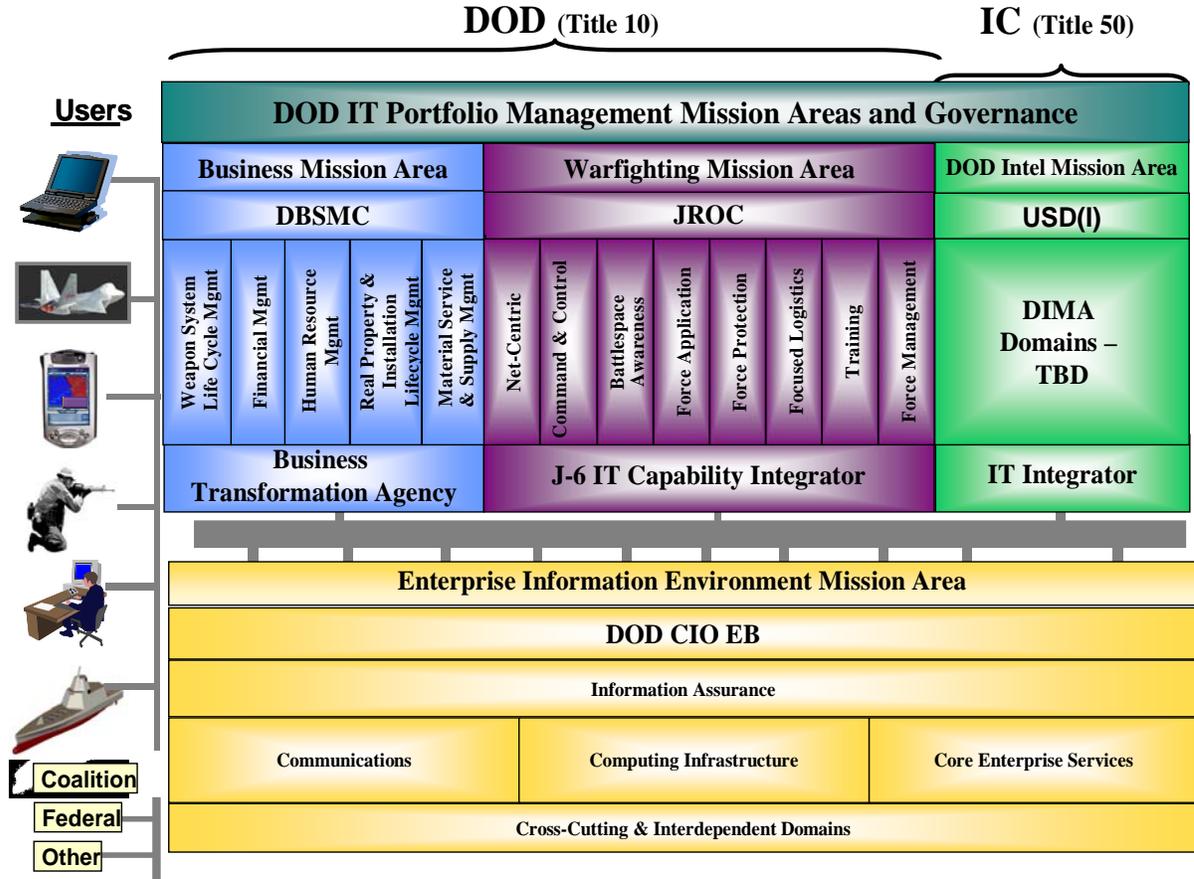
Figure 2. Interoperability Activity of DITPR ACAT I Programs/Systems.

JITC ORGANIZATIONAL STRUCTURE

JITC is organized to align with U.S. Code Title X core mission areas (Figure 3); to provide consistent best practices and processes across the organization; and support implementation of a risk-based test strategy that enables fast and agile testing. Figure 4 depicts JITC’s organizational structure. Figures 3 and 4 are color coded to show the correlation between the mission areas in Figure 3, and the portfolios in Figure 4.



IT Portfolio Management/Mission Area Organization



Legend

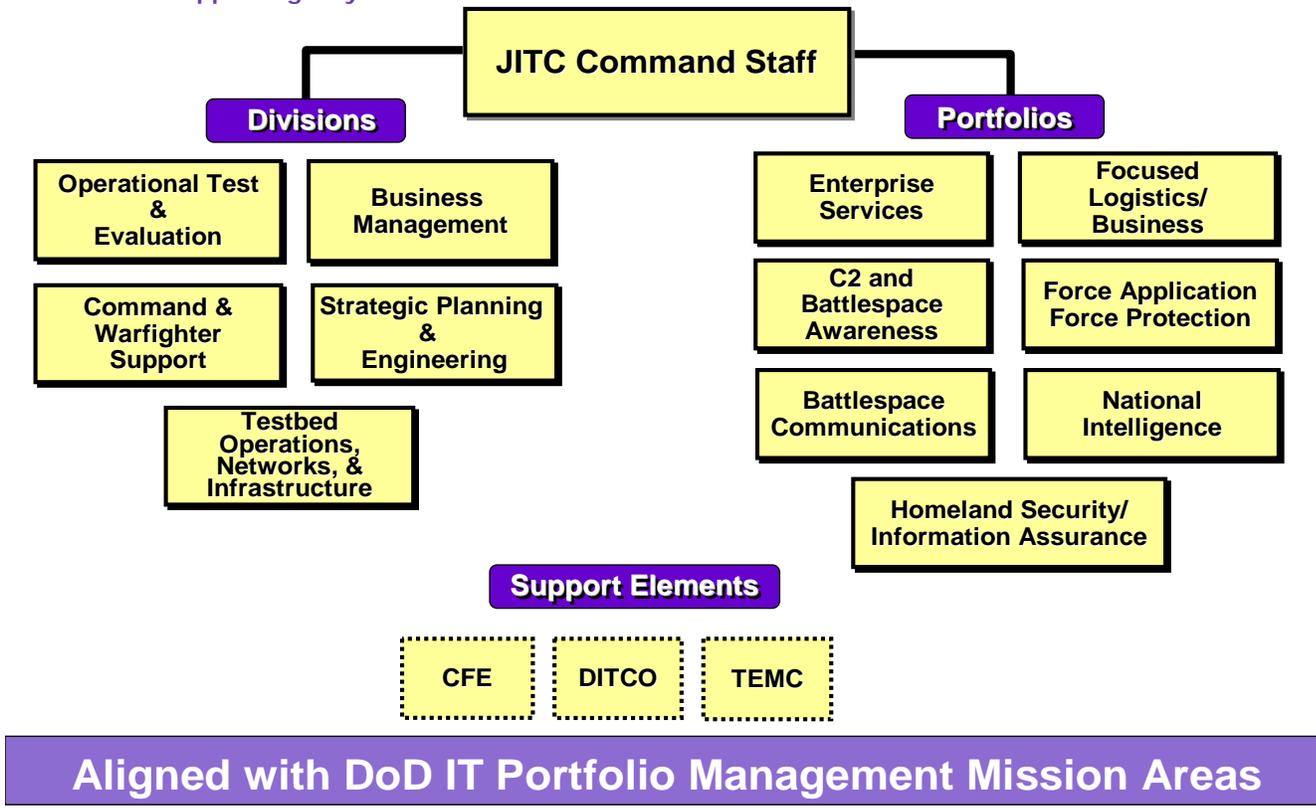
CIO Chief Information Officer
DBSMC Defense Business Systems Management Committee
DoD Department of Defense

EB Electronic Business
IC Intelligence Community
IT Information Technology
JROC Joint Requirements Oversight Council

Figure 3. Title X Core Mission Areas.

DISA Mission Support Structure

A Combat Support Agency



Legend
C2 Command and Control
CFE Chief Financial Executive
DITCO Defense Information Technology Contracting Office
JITC Joint Interoperability Test Command
TEM Test and Evaluation Management Center

Figure 4. JITC Organization.

JITC KEY FUNCTIONAL AREAS

JITC addresses interoperability across a broad spectrum of systems. For this report, JITC references one division and seven portfolios: Enterprise Services, Focused Logistics/Business, Command and Control (C2) and Battlespace Awareness, National Intelligence, Battlespace Communications, Force Application/Force Protection, and Homeland Security/Information Assurance portfolios. Table 1 shows the number of interoperability testing and certification related products issued in calendar year 2008 in these areas, as well as their respective status. The following paragraphs summarize the status of interoperability in these areas. Detailed

reports on these areas are in Appendices A through H. These appendices report total systems examined during the year. JITC reports interoperability status by the type of certification issued. These types are defined in CJCSI 6212.01. See Appendix I for details.

Table 1. CY 2008 Interoperability Status by Division/Portfolio.

Interoperability Status Category	JT1	JTA	JTB	JTC	JTD	JTE	JTF	JTG	Total
Interoperability Test Certification	0	0	4	3	4	20	3	0	34
Limited Interoperability Test Certification	1	0	3	6	10	9	8	0	37
Special Interoperability Test Certification	0	0	0	0	0	90	0	0	90
Extension of Joint Interoperability Test Certifications	0	0	0	1	0	8	0	0	9
Interoperability Assessment	1	0	0	12	7	19	30	1	70
Standards Conformance Certification	0	0	0	4	11	52	0	2	69
Standards Conformance Non-Certifications	0	0	0	0	3	0	0	0	3
Standards Conformance Assessment	0	0	0	0	2	14	0	0	16
Total	2	0	7	26	37	212	41	3	328
Legend									
C2	Command and Control			JTC	C2 Battlespace Awareness Portfolio				
CY	Calendar Year			JTD	Force Application/Force Protection Portfolio				
JT1	Operational Test and Evaluation Division			JTE	Battlespace Communications Portfolio				
JTA	Enterprise Services Portfolio			JTF	National Intelligence Portfolio				
JTB	Focused Logistics and Business Portfolio			JTG	Homeland Security/Information Assurance Portfolio				

JITC PORTFOLIOS/DIVISIONS

ENTERPRISE SERVICES PORTFOLIO SYSTEMS STATUS

JITC conducted testing on several DoD Enterprise Services programs. JITC tested all four product lines of the Net-Centric Enterprise Services (NCES) program: Collaboration, Content Discovery, Portal, and Service Oriented Architecture Foundation. The NCES services are progressing toward an interoperability certification. JITC also tested several DISA programs that are migrating to a Service Oriented Architecture, including Global Command and Control System - Joint (GCCS-J), and Global Combat Support System (GCSS).

FOCUSED LOGISTICS/BUSINESS PORTFOLIO SYSTEMS STATUS

Focused Logistics/Business Portfolio provided testing services to include developmental, operational, Independent Verification and Validation (IV&V), interoperability, and information assurance. Focused Logistics/Business Portfolio assisted programs in transitioning to a capability-based net-centric environment; ensured DoD testing and certification policy and

performance compliance of NSS/IT systems within the Business Mission Area, to include commercial vendor interoperability and standards conformance assessments; and served as lead DISA-JITC representative for full spectrum test support of all Joint logistics and business systems. See Appendix B for additional details.

COMMAND AND CONTROL (C2)/BATTLESPACE AWARENESS PORTFOLIO SYSTEMS STATUS

The diverse nature of DoD C2 systems presents significant interoperability challenges with potentially major operational impacts to the warfighter. JITC worked with several major transformational programs, including the Army's Future Combat Systems (FCS), the Net-Enabled Command Capability (NECC) that is poised to replace the Global Command and Control System (GCCS), and Unmanned Aircraft Systems (UASs) and their supporting infrastructure. To aid in identifying priority C2 systems and associated issues, JITC began a focused collaborative effort working with JFCOM in their capacity as the C2 Capability Portfolio Manager (CPM). JITC also provided significant support to the common data link (CDL), Global Positioning System (GPS), and the NATO Advanced Data Storage Interface (NADSI) communities. See Appendix C for additional details.

C2 CPM – JITC began assisting JFCOM with test and analysis support of the C2 Data Pilot effort, which is JFCOM's effort to improve overall Joint Force sourcing by COCOM planning staffs. JITC is providing Service-Oriented Architecture (SOA) expertise and evaluation methodologies to allow JFCOM to tap multiple authoritative data sources in a net-centric environment.

Unmanned Aircraft Systems (UAS) – JITC actively worked the test programs for Global Hawk Block 20/30, MQ-9 Reaper, Hunter, and Vertical Take-off Landing (VTOL) and anticipates test execution in the 2009 timeframe. Shadow was tested and received a limited interoperability certification.

Unmanned Systems Interoperability Profile (USIP) – JITC supported the task force in writing and finalizing USIP profile 1. USIP 1 provides a basic set of standards for transmitting Full Motion Video to ensure interoperability between Unmanned Aerial Systems and ground stations. The CDL specification was changed to incorporate the USIP 1 and was signed in December 2008.

CDL Testing – JITC provided core support to the CDL Executive Agent (EA), Secretary of the Air Force/Acquisition, Data Links (SAF/AQIZ). This included supporting the CDL Specification Design Team and serving as the designated EA test agent for all DoD CDL systems. JITC will also test most NATO systems for CDL compliance against STANAG 7085, the NATO version of the CDL specification.

GPS Testing – JITC provided support to the GPS JPO through our participation as part of the GPS Modification (Mod) III team. When the GPS Mod III capability is fielded, JITC will test the Master Control Stations and the GPS receiver's interface to systems. JITC verifies the GPS receiver is certified by one of the Service GPS Labs to ensure they are Selective

Availability Anti-Spoofing Module compliant, and using the TOPCON GPS receiver, checks the accuracy and timing of GPS receivers under test.

NADSI Testing – JITC provided support to the NADSI Custodian (SAF/AQ) dealing with STANAG 4575, which facilitates the digital storage of Intelligence, Surveillance, and Reconnaissance (ISR) data from sensor platforms, replacing the tape storage devices, at NATO ground stations. JITC, as part of the Custodian Support Team is the sole NADSI test facility and produces certification memoranda for the NADSI Custodian.

FORCE APPLICATION/FORCE PROTECTION PORTFOLIO SYSTEMS STATUS

Ground Based Mid-Course Defense System - Ground Based Mid-Course Defense (GMD) System is a capability based spiral development program that is currently undergoing Developmental Testing. JITC analysts are team members of the Ballistic Missile Defense Operational Test Agency (OTA), and continued to assess the GMD System for Interoperability in 2008. Elements assessed were the Upgraded Early Warning Radar (UEWR) System, In-Flight Interceptor Communications System (IFICS), GMD Fire Control Nodes (GFC), Aegis BMD, and the Command & Control Battle Management Communications (C2BMC). JITC participated in integrated and distributed ground test events, an element readiness test, and assessed real world operational test data collected during the Fast Shield event. Each of these events provided JITC the opportunity to collect and analyze data with the goal of assessing interoperability performance. These events also provided an opportunity to assess the warfighter's performance while exercising their Tactics, Techniques, and Procedures (TTP). The JITC team used the results from these tests to provide quarterly updates to the OTA Team Operational Assessment Briefing and Database and an annual update to the OTA Team Operational Assessment Report. This report is submitted to the Director, Operational Test and Evaluation (DOT&E) who reports annually to the United States Congress. See Appendix D for additional details.

Theater/Regional (T/R) Ballistic Missile Defense - Theater/Regional (T/R) Ballistic Missile Defense Systems (BMDS) are a subset of the Ballistic Air and Missile Defense Family of Systems (FoS) and consists of Major Defense Acquisition Programs, Command and Control Systems, and related programs and initiatives. Testing has been ongoing by the Ballistic Missile Defense Operational Test Agency (OTA) Team. JITC became involved with the T/R BMDS OTA Team at the end of 2008 and has reviewed existing documents, made contact with OTA and T/R element personnel, and attended planning and coordination meetings to coordinate future testing schedules. JITC is analyzing testing conducted between T/R elements during the Joint Defense of Israel 2008 (JDIE08) and early Integration Test #1 (EIT#1) conducted in June 2008. JITC participated in the BMD stakeholder meeting during November 2008 to review documents and provide inputs to the 2008 BMDS Regional Operational Assessment Report.

Theater High-Altitude Area Defense (THAAD) - THAAD is a mobile ground-based theater missile defense (TMD) system designed to protect forward-deployed military forces, population centers, and civilian assets from ballistic missile attacks. THAAD is a core element of the T/R BMDS FoS layered defense architecture. JITC assessed THAAD's voice communication systems based on participation in two DoD Interoperability Communications Exercises (DICE) between January and June 2008. THAAD participated in the JDIE08 EIT#1

and in FTT-09. JITC has produced a Draft Interoperability Certification Evaluation Plan (ICEP) and reviewed the Draft Information Support Plan (ISP), Draft Capabilities Production Document, and the Test Plan for FTT-10a. JITC has made contact with program office personnel and attended planning and coordination meetings. Future test event observations include FTT-10a in March of 2009.

Joint Tactical Ground Station (JTAGS) - JTAGS is a transportable information processing system that receives and processes in-theater, direct down-link data from Overhead non-imaging infrared satellites that include the Defense Support Program and the Space Based Infrared System. JTAGS mission supports all Theater Missile Defense (TMD) pillars, which includes attack operations, active defense, passive defense, and battle management/command, control, communications, computers and intelligence. JITC was funded to support JTAGS in October 2008, and subsequently contacted the JTAGS Product Office (PO) to review system documentation, including the Operational Requirements Document. The program has no Joint Staff certified requirements; JITC is working with JTAGS PO to define the requirements and provide recommendations to achieve an interoperability certification. JITC is working with the JTAGS development team to identify test events and opportunities to obtain test data from JTAGS's multiple interfaces. JTAGS is scheduled as a system under test at JITC during Joint Interoperability Test (JIT) 09-05, August 2009. The JIT 09-05 is a Joint Tactical Data Link-16 conformance to standards test with emphasis on ballistic missile defense systems.

Patriot Advanced Capability – 3 (PAC-3) - The PAC-3 is a high-rate-of-fire, Surface-to-Air Missile System designed and employed to defend key military or civil assets against T/R Ballistic Missiles, Air Breathing Threats, and Cruise Missiles operating as the lower tier of the Army Theater Air and Missile Defense (TAMD) force. PAC-3 is an integral component of the T/R BMDS Family of Systems (FoS) and must be able to process and exchange information with FoS members. JITC last assessed the system in May 2007 and provided a Limited Joint Interoperability Certification memorandum for PAC-3 Post Deployment Build -6 (PDB-6). Testing of PAC-3 PDB-6.5 is now ongoing but JITC has not been funded to observe or assess this build. PAC-3 will participate in various tests during the coming year in conjunction with ongoing MDA testing of BMDS.

Link 16 Implementation - In 2008, the JITC GMD analysis team performed an in-depth review of the Link 16 implementation by the BMDS Theater/Regional elements. The purpose of the review was to find potential areas of concern in implementation among the elements. The JITC team initially attempted to use the eSMART software to generate a matrix that would quickly identify the gaps in implementation. The eSMART database, however, did not contain the implementation data for the elements under consideration, nor was the computer hardware sufficiently robust to handle the comparison algorithms. The JITC team undertook the comparison manually and the resulting product was an implementation matrix that quickly delineated areas of implementation concern at the message word level. The implementation matrix is a list of the Link 16 messages and words that may be exchanged between BMDS Theater/Regional elements and indicates whether they are transmitted and/or received. The matrix further highlights specific messages and words that are implemented by one or more elements but not implemented by others.

The GMD Communications Network (GCN) Transition Project Interoperability Assessment - JITC is supporting Defense Information Systems Agency (DISA) by identifying and employing interoperability risk mitigation processes and procedures for the transition of the GCN Long-Haul Communication (LHC) from Boeing, the current Missile Defense Agency (MDA) lead service integrator, who now controls these leased circuits to the DISA Defense Information Systems Network (DISN). JITC supported the development and review of the GCN Critical Item Description Specifications and related GCN transition plans and provided input as requested. JITC FA/FP personnel conducted coordination efforts with Boeing and the JITC Battlespace Communications Portfolio by assisting in the consolidation of planned milestones, transition action items, and circuit testing requirements. JITC has assisted this transition effort by developing test cases and procedures which have been published in the Boeing, MDA, and DISA transition test plans.

Chemical, Biological, Nuclear, and Radiological (CBRN) Programs - JITC executed one evaluation of Chemical and Biological Defense Program systems and published five interoperability reports and assessments during 2008. In response to an urgent request from the Joint Biological Standoff Detection System (JBSDS) Program Office, JITC conducted the JBSDS Increment 1 Interoperability evaluation from March through October 2007, at Aberdeen Proving Ground, Maryland, and at Dugway Proving Ground (DPG), Utah. JITC issued a JBSDS Increment 1 Interoperability Assessment Report and an Assessment Memorandum in March 2008. JITC collected interoperability performance data for the Joint Biological Point Detection System (JBPDS) Increment 1 during the JBPDS Increment 1 MOT&E Phase VI conducted at DPG and Eglin Air Force Base, Florida from 9 September through 9 November 2007, and published a JBPDS Increment 1 Joint Interoperability Test Report and a Joint Interoperability Test Certification in July 2008. JITC also participated in a JBPDS Increment 1 System Level Demonstration conducted by the Program Manager at Pope Air Force Base, North Carolina from July through August 2008. The event was conducted to demonstrate the enhancements implemented by the developer based on shortfalls identified during the MOT&E. Because the changes did not impact the results published in the JITC test report and certification memorandum, JITC did not produce additional JBPDS report documents. Finally, the JITC participated in the Multi-Service Operational Test and Evaluation (MOT&E) of the Joint Warning and Reporting Network Increment 1 and the Joint Effects Model Increment 1. The MOT&E was conducted in a realistic environment at Fort Hood, Texas using service operators as participants. Since the MOT&E was conducted using developmental hosts, the JITC issued a Joint Interoperability Assessment Memorandum for the system.

Army Programs/Central Technical Support Facility (CTSF) - JITC supported interoperability risk reduction testing for the Air and Missile Defense Planning and Control System (AMDPCS)/Air Defense Airspace Management (ADAM) Cell and Tactical Airspace Integration System (TAIS). JITC collaborated with personnel assigned to the Army Central Technical Support Facility (CTSF) at Fort Hood, Texas to conduct joint interoperability testing in conjunction with Army Interoperability Certification testing conducted by the CTSF. JITC provided joint interoperability test cases/threads to CTSF personnel to validate critical ADAM Cell Joint Interoperability requirements. Potential adverse ADAM Cell discrepancies were reported in the JITC ADAM Cell test report. JITC participated in two separate TAIS test

activities to assess potential risks associated with radar fusion/tracking and critical joint data exchange requirements.

Identification, Friend or Foe (IFF) Programs - JITC provided interoperability testing and certification support for Navy Mode S IFF upgrades, the USAF F-15 Mode 5 IFF upgrade, and the Mode S IFF upgrade to the AN/APX-111 as integrated into the F/A-18.

The Mode S IFF program produced certifications for the EA-6B, P-3C, and EP-3 aircraft. These and future Mode S programs utilize a shared test plan which significantly reduces the amount of redundant work which has resulted in a savings of approximately \$100,000 to Navy programs.

The F-15 Mode 5 IFF upgrade is still in development and JITC participation is greatly streamlining the process. Once fully developed, certification is expected to be smooth since JITC has been a part of the development since early in the program lifecycle.

The AN/APX-111 F/A-18 Mode S IFF upgrade was developed separately by the Navy from their other Mode S IFF programs. Several discrepancies were noted in the DoD Air Traffic Control Radar System (ATCRBS), IFF, Mark XII/XIIA, Systems (AIMS) report in all operational IFF modes including critical links and mode 4. After discussions with the DoD AIMS program office a resolution white paper was issued by the DoD AIMS program office which stated that the AN/APX-111 discrepancies do not pose a risk to safety of flight or interoperability. The current discrepancies are being addressed by the F/A-18 program office and an acceptable timeline for resolution is set. Based on this information, JITC agreed to accept the conditional box level conformance certification and will progress ahead with interoperability certification of the AN/APX-111.

Tactical Gateway Programs - Tactical Gateway Programs that JITC supported during 2008 include the Roll on Beyond-Line-of Sight Enhancement (ROBE), Pocket J, Situation Awareness Data Link (SADL), Joint Range Extension (JRE), the Air Defense Systems Integrator (ADSI), the Common Link Integration Processing (CLIP) program, Objective Gateway (OG), Interim Gateway (IG), and the Joint Interface Control Officer (JICO) Support System (JSS). JITC supported numerous JSS activities during 2008 to include JSS training, JSS technical order reviews, JSS capability gap reviews, JSS Human-Machine Interface reviews, JSS Test and Evaluation integrated product team meetings, and JSS qualification testing. JITC has been a leader in the JSS Six Sigma team project, which has already helped improve test processes and lower defect rates from the engineering release of the JSS to the production ready release of the JSS. JITC supported testing of the testing of the IG system, which was pushed for by real-world needs. Testing included two flight tests, Air Force System Interoperability test (AFSIT), and ground testing of the modular gateway system. JITC continues to support ADSI development and certification, and has participated in service level testing for Version 14.1, 14.1.1, and 14.1.1sp2.

SMART Weapons/Network Enabled Weapons - JITC participated in Joint Air-to-Surface Standoff Missile (JASSM) flight testing. During data analysis, JITC and the program office uncovered a critical Global Position System deficiency. The JASSM program

office will correct this issue before starting production and delivery of the upgraded JASSM round. JITC has started a Network Enabled Weapons Testing program with the initiation of the Joint Stand-Off Weapon (JSOW C-1) certification task, and has also initiated contact with all other NEW Increment 1 systems (Small Diameter Bomb II, HARPOON, and JASSM).

USN Surface Platforms - USN Surface platforms that JITC supported during 2008 included the Guided Missile Destroyer (DDG)-1000, the Nuclear-Powered Aircraft carrier (CVN) -78, the Joint High Speed Vessel (JHSV), the Landing Helicopter Assault (LHA) - 6, the Littoral Combat Ship (LCS), the Landing Platform Dock (LPD) – 17, the Mobile Launch Platform, the dry cargo-ammunition ship (T-AKE), and the Maritime Pre-positioned force. JITC also participated in three T-AKE DT events and two T-AKE OT events. These events will provide the necessary data for joint interoperability certification of the T-AKE.

USN Sub-surface Platforms - USN Sub-surface platforms that JITC supported during 2008 included the Virginia (VA) Class Submarine. JITC participated in three DT/OT events for VA Sub program, which will result in a joint interoperability certification for the VA Class Submarine.

Rotary Wing Platforms - Rotary wing platforms that JITC supported during 2008 included the CV-22, MV-22, VH-60N, and the VH-71 program. JITC was involved in the Armed Reconnaissance Helicopter (ARH) program until the project was cancelled in late CY08.

Surveillance Platforms - Surveillance Platforms that JITC supported during 2008 included the P-8, Air Operations Center Weapons System (AOC WS) and E-3 40/45 upgrade. The E-3 completed assessment of E-3 40/45 Link 16 standards conformance test. This test will lead to future certification of the E-3 40/45 (expected in FY 11). JITC witnessed AOC WS version 10.1 tests in the Republic of Korea. Based on current Joint Staff direction, the ASOC WS version 10.1 will not require certification but AOC 10.2 will in the near future.

Special Operation Platforms/Systems - Special operation platforms/systems that JITC supported during 2008 included the AC-130 U/H, HC/MC-130, CV-22 SHAFT, AC-XX, Cursor on Target (COT), and the Battlefield Air Operations (BAO) Kit. JITC has established a sustainable COT testing environment in order to provide applicable joint certifications and assessments of the varying usages of the COT schema. JITC participated in the AC-130 U/H DT/OT events and the AC-130 U/H Air Force System Interoperability Test (AFSIT).

Fighter Platforms - Fighter Platforms that JITC supported during 2008 included the F-35/Joint Strike Fighter, EA-18G, F-22A and the F-16 40/50. JITC participated in five EA-18G OT and DT events for Navy Fighter/Attack Aircraft and their subsystems. This resulted in the collection of data to leverage towards an E/A-18G full joint interoperability certification in FY09/10. JITC participated in two F-16 Block 40/50 DT/OT events and one AFSIT event which were leveraged to issue two limited joint certifications. JITC participated in numerous test events to support re-certification of the F-22A, full Interoperability Certification will be complete in calendar year 2009.

Bomber Platforms - The JITC conducted initial coordination with the B-2 program office to develop a common understanding of B-2 test requirements and to identify the best strategy to validate all B-2 mission capabilities. JITC participated in several B-1 Digital Communications Improvement (DCI) test planning meetings to discuss and review the DCI ground test plan and in numerous B-1 FIDL Sub-Integrated Test Team meetings to review B-1 schedule updates for Ground and Operational Testing. JITC will continue to support both the B-1 and B-2 programs as they progress towards interoperability certification next year.

Support Platforms - The Joint Cargo Aircraft (JCA) is on schedule towards joint interoperability certification during FY10. Testing started on a production representative aircraft, and barring major setbacks with coordination of the JCA TEMP and ISP, we expect the platform to complete all joint certification requirements by the end of calendar year 2009. The C-130 Avionics Modernization Program flew the first production representative aircraft in mid-January 09. This program is scheduled to begin IOT&E during early FY11. While the solicitation in support of the KC-45 Aerial Tanker was cancelled by the SECDEF, activities continued in support of the program office. JITC will develop interoperability certification criteria based on approved JCIDS documents during the expected source selection process.

Tactical Data Links - JITC examined thirteen U.S. systems that employ Tactical Data Links in 2008. Additionally, eight previously tested, fielded systems participated to serve as proof for joint interoperability. JITC tested these systems using a combination of 47 different interfaces.

North Atlantic Treaty Organization (NATO) Data Links - JITC tests North Atlantic Treaty Organization (NATO) systems/software to determine the extent their software conforms to NATO Standardization Agreement (STANAG) 5511, 5516, and 5616 requirements. NATO nations then determine the extent to which their systems are interoperable. JITC executed two NATO Tactical Data Link Interoperability Tests (NTDLIOTs) in 2008. Command and control systems from the NATO Programming Centre (NPC), NATO Consultation, Command and Control Agency (NC3A), Germany, Italy, United Kingdom, France, Spain, Norway, and the U.S. participated in testing. The JITC test support included preplanning, test execution, post test, and technical workshop meetings. The JITC provides U.S. representation to the NATO Tactical Data Interoperability Testing Syndicate (TDLITS). The migration to STANAG 5602, Edition 3 (SIMPLE - Standard Interface for Multiple Platform Link Evaluation), which required NATO interoperability tests use Transmission Control Protocol/Internet Protocol (TCP/IP) over the Combined Federated Battle Lab Network, was a successful transition for a full compliment of systems. However, there are sites that have not completed their migration and still employ the traditional method of network connectivity via Integrated Services Digital Network (ISDN) through the European data hub at NC3A.

United States Pacific Command (USPACOM) Area Data Links - JITC participates with DISA and USPACOM J6 in Command and Control Interoperability Boards. The Command also tests Pacific Rim Country systems, when requested to determine the extent their software conforms to Military Standards 6011 and 6016, and interoperability Tactical Data Link Branch Interoperability Status FY2008 2A.doc between USPACOM AOR systems and US Forces. JITC executed no USPACOM testing in 2008.

Foreign National Support of Tactical Data Link Testing - JITC participated with a commercial vendor in support of a Standards Conformance Assessment of the Australian Airborne Early Warning and Control (AEW&C) (Wedgetail) in accordance with MIL-STD-6016C, MIL-STD-6011C, MIL-STD-6020 Appendix A, AEW&C Link-16 Interface Requirement Specification (IRS) 3.1 (based on OS-516.2 Change 1), OS-411.3 (including Appendix D, ADF implementation), and the message forwarding capability in OS-516.2, Change 1, Appendix H.

Variable Message Format - JITC examined three Variable Message Format (VMF) systems in 2008.

United States Message Text Formats - JITC examined three United States Message Text Format (USMTF) systems in 2008.

Reimbursable Programs - In addition, JITC examined one U.S. system and one New Zealand system that employ Tactical Data Link in 2008 under reimbursable tasking.

BATTLESPACE COMMUNICATIONS PORTFOLIO SYSTEMS STATUS

Battlespace communications provides the transport links between all warfighters and the applications and services that support them. Continued advances in technologies, as well as the convergence of voice, video, and data facilitated improved communications, but also gave rise to a diverse mix of interoperability challenges. Indeed, the vast majority of requests for help that JITC received through our warfighter hotline dealt with communications systems. Accordingly, JITC put significant effort into the testing and certification of upgraded and emerging communications systems and technologies. JITC's Battlespace Communications Portfolio is responsible for all communications interoperability testing, from small wireless devices to optical networks, from secure facsimile systems to secure video teleconferencing capabilities, from tactical radios to the Defense Integrated Services Network, and from IPv6 enhancements to everything-over-IP implementations. See Appendix E for additional details.

DoD Interoperability Communication Exercise (DICE) – DICE continued as a key interoperability venue for tactical communications systems within DoD and our federal and state partners. The three DICE events of 2008 accommodated 59 participants: 17 Interoperability Test & Evaluations, 10 technology experiments/demonstrations, and 32 Tactics, Techniques and Procedures. Participants included components of each active military service, elements of the Air National Guard and the Army National Guard, U. S. Northern Command, and the Department of Homeland Security's Federal Emergency Management Agency.

Coalition Warrior Interoperability Demonstration (CWID) - CWID is the Chairman of the Joint Chiefs of Staff-directed annual event that serves to find solutions to capability gaps that can be fielded within a 12-18 month timeframe. CWID 2008 was conducted at four primary sites in the United States, the Host Combatant Command site at HQ USEUCOM in Stuttgart, Germany and at numerous Coalition Partner sites, to include NATO. JITC, as the chair of the CWID Assessment Working Group, led the Interoperability, Warfighter Utility, and Information

Assurance assessments of forty-one CWID trials and provided independent validation of each trial's ability to meet the requirements associated with the capability gaps outlined in the CWID 2008 Objectives. Results of these assessments were recorded and included in the CWID 2008 Final Report for distribution to senior leaders in the Department of Defense.

Advanced Internet Protocol Technologies Capability (AIPTC) - The AIPTC Test capability completed thirty-two IPv6 special product certifications and provided significant input to the IPv6 Test and Evaluation Master Plan and the Test and Evaluation Report provided to Congress. The standalone IPv6 special certification program ended in 2008, however IPv6 will continue to be assessed as systems are tested for Net-Readiness and components are tested for inclusion on the Unified Capabilities Approved Products List.

Unified Capabilities (UC) Test Program - JITC began testing products against the Unified Capabilities Requirements that DoD published in December 2007. There were more than 120 telecommunication products that were submitted for Approved Products List (APL) testing (Information Assurance [IA] and Interoperability [IO]) at JITC. Fifty-five products successfully completed IO and IA testing and were added to the UC APL. There were also 43 desktop reviews conducted for products already on the APL, which resulted in 43 updates of existing IO certification memoranda.

Real Time Services (RTS) Test Program - The RTS test program was created to assist vendors in developing and troubleshooting prototype devices to be part of the new IP end-to-end architecture. The program has assessed eight systems, providing vendors with invaluable deficiency reports necessary for vendors to redevelop their products and return to JITC for follow-on testing. As the products and technologies mature, this effort will converge under the Unified Capabilities test program.

Public Key Infrastructure (PKI) and Public Key Enabled (PKE) - JITC provided interoperability testing support to the DoD PKI Program Office on 132 Change Requests. The PKI lab completed a system modernization upgrade to replace all existing hardware and software which included 35 new servers. PKE testing provided information and guidance to 12 vendors, performed 4 product assessments, and certified 11 applications as PKI-compliant. Additionally, support to the DoD PKI Federal Bridge program included providing PKE testing information and guidance to 13 federal agencies that wanted to connect to the DOD PKI and certified 11 of those agencies for DoD PKI interoperability.

Defense Red Switch Network - Defense Red Switch Network (DRSN) completed testing of new operational software versions for the Secure Digital Switch (SDS), the Digital Small Switch (DSS), and the Digital Small Switch model 2A (DSS-2A). The DRSN lab played a significant role in the development of the Voice over Secure Internet Protocol (VoSIP) gateway to the DRSN and provided test support for the development of the Secure Mobile Environment Personal Electronic Device (SME PED). The DRSN continued to support the warfighter by conducting over seven DSS and five SDS Operation and Maintenance (O&M) and database maintenance courses. A total of 102 students completed DRSN training.

Ultrahigh Frequency (UHF) SATCOM Test Facility - Completed test procedures for UHF Integrated Waveform (IW) Phase One requirements and began validating them against vendor terminals implementing these standards. Formal testing will begin in CY 2009.

Transformational Communication Systems - Wideband Global System and Phoenix SATCOM terminals were tested together, highlighting the Ka-Band becoming available for the warfighter. In conjunction with the Joint Tactical Radio System (JTRS) Test Facility, test procedures for the Mobile User Objective System terminals are being prepared to test and certify these terminals as they become ready in CY 2009.

NATIONAL INTELLIGENCE PORTFOLIO SYSTEMS STATUS

The overarching U.S. Defense Intelligence Enterprise specifically emphasizes the need to focus DoD efforts on improving interoperability among and between our national and coalition partners. Within that framework, JITC has continued to seek means and pursue opportunities to support key customers (and ultimately our warfighters), by providing agile yet robust test support to a number of key intelligence community test activities. See Appendix F for additional details.

Distributed Common Ground/Surface Systems (DCGS) – The JITC DCGS team led Test & Evaluation (T&E) efforts of the joint/interagency DCGS T&E Focus Team. Key accomplishments for the year included:

- **T&E Focus Team (FT) Restructured** – The DCGS FT was restructured under the new Under Secretary of Defense, Intelligence USD (I), DCGS Governance Construct, which resulted in better defined relationships between the various DCGS boards and working groups. This new organizational structure will improve support to the DCGS Family of Systems as they provide needed capabilities to the warfighter.
- **DCGS Distributed Development and Test Enterprise (DDTE) Transition** – The DDTE transitioned to the Defense Information Systems Network Leading Edge Services. This effort was completed during Empire Challenge 2008 (EC-08), resulting in a twelve node DDTE configuration that provides testers the capability to communicate in an operational realistic environment. The DDTE provides a robust capability for future distributed test activities.

Intelligence, Surveillance, and Reconnaissance (ISR) Support - The JITC led test planning activities for EC-08). Empire Challenge (an annual event sponsored by the Under Secretary of Defense [Intelligence]) is conducted to assess the ability of joint and coalition forces to process/share ISR data between various platforms and ground processing systems. Participation in EC-08 enabled JITC to play a key part in demonstrating the ability of various ISR systems to fuse/exchange data from different sources and ultimately support critical decision making for the warfighters. The JITC testers conducted a number of interoperability assessments and standards conformance tests of various service/agency intelligence data processing systems during the event. The scope of standards work assessed the compliance of the data produced by 10 platforms/systems to the Motion Imagery Standards Profile, 9 platforms/systems to

National Imagery Transmission Format Standards (NITFS) 2.1; and 3 platforms/systems to the Ground Moving Target Indicator Format (GMTIF) suite of standards.

Defense Intelligence Agency (DIA) Department of Defense Intelligence Information Systems (DoDIIS) – JITC provided interoperability testing for DoDIIS Intelligence Mission Systems (IMSs). During CY 2008, JITC completed interoperability assessments on 21 DoDIIS systems (see Appendix G), supporting the intelligence community’s evolving architecture. JITC conducted interoperability testing at DIA testing facilities in the National Capital Region (NCR), as well as at major operational sites including U.S. Strategic Command (STRATCOM), Offutt Air Force Base, Nebraska and at U.S. Central Command (CENTCOM), MacDill Air Force Base, Florida.

National Geospatial-Intelligence Agency (NGA) Systems – JITC conducted interoperability testing for the NGA Test Organization (NTO). JITC performed interoperability testing at the NGA NTO Newington, Virginia testing facilities, as well as at major operational sites, including the Joint Analysis Center, Molesworth, England and at STRATCOM. Details of testing are in Appendix F.

Joint Tactical Terminal – Briefcase (JTT-B) Version 5 - The JTT-B Version 5 was evaluated for interoperability from 9 to 12 October 2008. The U.S. Army Special Operations Command (USASOC) deferred testing the JTT-B General Purpose Link (GPL). As a result, the JTT-B Version 5 received a Limited Joint Interoperability Certification.

HOMELAND SECURITY/INFORMATION ASSURANCE PORTFOLIO SYSTEMS STATUS

Homeland Security/Information Assurance Portfolio provided the full range of testing services, technical support, coordination, and oversight to the DoD, the Department of Homeland Security (DHS), and various federal, state and local governments to ensure seamless acquisition, integration, and Information Assurance of systems supporting the DoD and the National Command Authority. JITC portfolios were supported with information assurance expertise to ensure integration with all test activities. The DOT&E Exercise Interoperability/Information Assurance (I&IA) Assessments program was supported by performing I&IA assessments at COCOM exercises. See Appendix G for additional details.

OPERATIONAL TEST & EVALUATION (OT&E) DIVISION SYSTEMS STATUS

JITC OT&E Division conducted 12 operational test events in calendar year 2008; of these, 9 were conducted under OSD oversight. Table 2, below, lists the systems tested. The scope of testing ranged from minor operational assessments to complete Initial or Follow-on OT&Es. Proponents for the programs include Combatant Commands, military services, and various DoD agencies. Interoperability was a critical area evaluated during every operational test and was a factor considered in determining the system’s operational effectiveness. See Appendix A for additional details.

Table 2. JITC Operational Test Programs in 2008.

PROGRAM	CATEGORY
Common Foods Management System (CFMS)	Logistics
DoD Teleport (2 tests)	Communications
Enterprise Business Modernization (EBM)	Logistics
Global Command and Control Systems - Joint (GCCS-J) (3 tests)	Command & Control
Global Combat Support System Combatant Commander/Joint Task Force (GCSS-CC/JTF)	Logistics
Identification Friend or Foe (IFF) Mode 5 Cryptographic Program (2 tests)	Security
Net-Enabled Command Capability (NECC)	Command & Control
Network-Centric Enterprise Services (NCES)	Command & Control
Public Key Infrastructure (PKI)	Security

JITC will continue to support DISA acquisition programs as its designated Operational Test Agency (OTA), along with supporting other DoD Services, Combatant Commands, and agencies with Operational Test and Evaluation (OT&E) services. With the maturation of the NR-KPP test processes and the continued increase in net-centric acquisition programs, a natural migration towards more integrated or combined DT and OT is occurring. OTAs will rely upon DT-type events to provide much of the data necessary to assess the NR-KPP and information assurance, and to resolve the associated critical operational issues. We anticipate earlier involvement and more participation in non-OT events.

TEST OPERATIONS SUPPORT

Testbed Operations, Networks, and Infrastructure Division had four major modernization efforts underway in CY 2008. Efforts to seek updated and consolidated common services to support NECC and NCES testing, which have common equipment and maximize equipment usage, lead to a cost savings by better utilizing space.

Distributed Test Operations - The DTOC, still being developed, will supply centralized control for JITC testing efforts and allows JITC's Commander to have knowledge of the entire scope of test operations within and around the Command. The DTOC currently has a view of all current and upcoming tests along with their status, hotline actions, circuit conditions, near real-time network health statistics, and plans to include accountability tracking for TDY personnel, open trouble tickets command-wide, and real time newsworthy event reporting.

DNCC Tech Control - Efforts are underway to standardize all configurable laboratory spaces under one centralized office, connected through DNCC. This effort will place DISA/JITC at the forefront of technology and testing by updating and centralizing all laboratory assets (e.g. workstations, equipment, racks, and work areas). DISN has asked JITC's Test Operations and the Distributed Network Control Center (DNCC) to act as the red side control center for the DISN LES. DNCC is now managing multiple testing networks and supporting testing efforts as JITC supports the NECC and NCES testing efforts.

SYSCON - Test Operations and the SYSCON serves as a hub for internal and external testing and provide direct connectivity to the tactical edge equipment. JITC provides support for many events throughout the year that use many of the SYSCON's assets. This includes testing in support of system interoperability certification efforts and DICE. The updated SYSCON will directly support the Program Manager by securing a WIN-T tactical hub, and by configuring the Joint Multi-Switch Node to service Navy, Air Force, and Marine switching systems. The new equipment and configurations will provide the necessary backbone for JITC to conduct everything over IP (EoIP) testing for the Army.

COMSEC - The COMSEC Lab has been converted to configurable lab spaces under direct control of JT5. Test Operations and the COMSEC facility serve as a hub for internal and external testing requiring secure space and access to various cryptographic equipment, keying material, and secure networks. Outdated equipment, work areas, and compartmentalized assets have been consolidated and have proven to be a cost savings measure by better utilizing space and assets.

HOTLINE SUPPORT

Background: JITC began providing this service to the Warfighter during Operation JUST CAUSE in 1989 and it continues today. Our goal is to provide rapid response to interoperability problems with C4I systems, equipment, and networks to the warfighter deployed during war, real-world contingencies, and exercises, as well as day-to-day operations.

We receive numerous requests for operational assistance resulting from a variety of reasons. A large number of requests, but not all, are due to:

- JITC having documented technical interfaces and configurations not widely published by program managers, equipment manufacturers, or known by operators and maintainers.
- The customer's lack of readily available interface documentation and knowledge of the particular equipment in question that may or may not be generally available to the maintenance community.
- Our reputation of providing total warfighter support and quick solutions to time-sensitive situations where both experienced and inexperienced operators and maintainers lack formal training and are under extreme pressure to establish communications in either a war, real-world contingency, exercise, or routine operational environment.

The Hotline can be accessed several ways:

- The web, at <http://jitic.fhu.disa.mil/support.html>
- E-mail, at Hotline@disa.mil
- Commercial telephone, at 1-800-LET-JITC (1-800-538-5482)
- DSN telephone, at TRY-JITC (879-5482)

Table 3, below, shows the calls documented in FY 08, and the period FY 93 through FY 08 (we began documenting this support in FY 93). It is organized so the two periods can be compared.

In addition, the table shows highlights of the calls (type of support requested, the leading customers, suspected cause of why the calls were made, suspected impacts if they were not supported, calls resulting in a test, exercises and contingencies supported, and calls supporting the war on terrorism).

Table 3. FY 93 through FY 08 and FY 08 Hotline Call Highlights.

Highlight Area	FY 93 through FY 08 Hotline Calls	FY 08 Hotline Calls
Note: Rounding may affect the individual % and the % totals presented in this table		
Number of calls documented	<ul style="list-style-type: none"> • 3886 calls • The average number of calls for the 15 FYs is 243. • Seven FYs (93, 94, 95, 98, 99, 00, and 01) are below the average • The leading FY is FY 07 (381 calls), followed by FY 08 (365), FY 03 (329), FY 04 (322), FY 05 (318), FY 06 (311), FY 96 (285), FY 97 (259 calls), and FY 02 (258 calls) 	<ul style="list-style-type: none"> • 365 calls • FY 08 calls are 9% of the total FY 93 through 08 calls • FY 08 calls are 50% above the average of FY 93 through 08 calls
Leading support areas	<p style="text-align: center;"><u>The number of calls and % of the 3886 calls</u></p> <ul style="list-style-type: none"> • EKMS = 768 calls (20%) • Voice switch = 766 calls (20%) • COMSEC = 568 calls (15%) • Secure facsimile = 537 calls (14%) • Data network = 486 calls (13%) • Transmission (other than satellite) = 246 calls (6%) • Other = 207 calls (5%) • Satellite = 195 calls (5%) • VTC = 113 calls (3%) 	<p style="text-align: center;"><u>The number of calls and % of the 365 calls</u></p> <ul style="list-style-type: none"> • EKMS = 206 (56%) • Transmission (other than satellite) = 39 calls (11%) • Voice switch = 37 calls (10%) • Data network = 18 calls (5%) • COMSEC = 17 calls (5%) • Secure facsimile = 15 calls (4%) • VTC = 15 calls (4%) • Satellite = 11 calls (3%) • Other = 7 calls (2%)
<i>Note: "Other" in this instance is an area of support, which includes calls on areas such as records management, collaboration tools, certification process, and military standards.</i>		
Leading customers	<p style="text-align: center;"><u>The number of calls and % of the 3886 calls</u></p> <ul style="list-style-type: none"> • Services = 1967 calls (51%) • Others = 1240 calls (32%) • Combatant Commands = 679 calls (17%) 	<p style="text-align: center;"><u>The number of calls and % of the 365 calls</u></p> <ul style="list-style-type: none"> • Services = 108 calls (30%) • Combatant Commands = 19 calls (5%) • Others = 238 calls (65%)
<i>Note: "Others" in this instance is a group of customers, which includes Joint agencies, industry, DOD, and other (agencies such as IRS, BLM, Supreme Court, FBI, NSA, CIA, Canadian National Defense, National Security Council, Nuclear Regulatory Commission, Department of the Treasury, FEMA, etc.). Due to the sensitivity of the EKMS support, these calls are only tracked by the requesting Service and as Other which includes Department of Defense and civilian government agencies.</i>		
The Services' use of the Hotline	<p style="text-align: center;"><u>The number of calls and % of the 3886 calls</u></p> <ul style="list-style-type: none"> • Army = 723 calls (19%) • Air Force = 589 calls (15%) • Navy = 236 calls (6%) • National Guard = 222 calls (6%) • Marines = 197 calls (5%) 	<p style="text-align: center;"><u>The number of calls and % of the 365 calls</u></p> <ul style="list-style-type: none"> • Army = 45 calls (12%) • Air Force = 29 calls (8%) • Navy = 16 calls (4%) • National Guard = 10 calls (3%) • Marines = 8 calls (2%)
The Combatant Commands' use of the Hotline	<p style="text-align: center;"><u>The number of calls and % of the 3886 calls</u></p> <ul style="list-style-type: none"> • USCENTCOM = 234 calls (6%) • USPACOM = 139 calls (4%) • USEUCOM = 110 calls (3%) • USSOCOM = 53 calls (1%) • USJFCOM = 42 calls (1%) • USNORTHCOM = 40 calls (1%) 	<p style="text-align: center;"><u>The number of calls and % of the 365 calls</u></p> <ul style="list-style-type: none"> • USCENTCOM = 4 calls (1%) • USPACOM = 4 calls (1%) • USSOCOM = 4 calls (1%) • USNORTHCOM = 3 calls (1%) • USTRANSCOM = 2 calls (1%) • USEUR = 1 call (less than 1%)

Highlight Area	FY 93 through FY 08 Hotline Calls	FY 08 Hotline Calls
	<ul style="list-style-type: none"> • USSOUTHCOM = 27 calls (1%) • USSPACECOM = 15 calls (less than 1%) • USTRANSCOM = 11 calls (less than 1%) • USSTRATCOM = 8 calls (less than 1%) 	<ul style="list-style-type: none"> • USJFCOM = 1 call (less than 1%) • USSOUTHCOM = No calls (0%) • USSTRATCOM = No calls (0%) • USSPACECOM = No calls (0%)
Suspected cause the call was made (Note 1)	<p align="center"><u>The number of calls and % of the 3886 calls</u></p> <ul style="list-style-type: none"> • Procedures = 1987 calls (51%) • Equipment = 1697 calls (44%) • People = 202 calls (5%) 	<p align="center"><u>The number of calls and % of the 365 calls</u></p> <ul style="list-style-type: none"> • Equipment = 251 calls (69%) • Procedures = 105 calls (29%) • People = 9 calls (2%)
<p>Note 1: People = lack of training, operator error, or failure to plan Equipment = equipment failed, new equipment fielding, lack of equipment, or use of uncertified interfaces Procedures = lack of, or incorrect, procedures or documentation Undetermined = problem not resolved, not isolated, or cleared while troubleshooting</p> <p>Note 2: Equipment = equipment could not be installed Circuit = circuit could not be installed Other = general information, information on test results, assistance with a procurement decision, assistance with testing, traffic loading, training, or problem cleared while troubleshooting</p>		
Calls requiring a test	<ul style="list-style-type: none"> • 310 calls (8% of the 3886 calls) • Voice switch = 137 calls (44% of the calls requiring a test) • Secure facsimile = 50 calls (16% of the calls requiring a test) • COMSEC = 33 calls (11% of the calls requiring a test) • Data network = 32 calls (10% of the calls requiring a test) • VTC = 22 calls (7% of the calls requiring a test) • Transmission (other than satellite) = 17 calls (5% of the calls requiring a test) • Satellite = 14 calls (5% of the calls requiring a test) • Other = 3 calls (less than 1% of the calls requiring a test) • EKMS = 2 calls (less than 1% of the calls requiring a test) 	<ul style="list-style-type: none"> • 19 calls (5% of the 365 FY 08 calls and 6% of the 310 FY 93 through FY 07 calls requiring a test) • Voice switch = 10 calls (53% of the FY 081 calls requiring a test) • Satellite = 3 calls (16% of the FY 08 calls requiring a test) • Transmission other than satellite = 3 calls (16% of the FY 08 calls requiring a test) • VTC = 2 calls (11% of the FY 08 calls requiring a test) • EKMS = 1 call (5% of the FY 08 calls requiring a test)
Calls supporting an exercise	<ul style="list-style-type: none"> • 221 calls (6% of the 3886 calls) • 55 exercise series supported • 122 individual exercises supported 	<ul style="list-style-type: none"> • 5 calls (1% of the 365 FY 08 calls and 2% of the 221 FY 93 through FY 08 calls supporting an exercise) • 4 exercises supported
Calls supporting a contingency	<ul style="list-style-type: none"> • 379 calls (10% of the 3886 calls) • 20 contingencies supported • 244 of the 379 calls (64%) have supported ENDURING FREEDOM (EF) 	<ul style="list-style-type: none"> • 11 calls (3% of the 365 FY 08 calls and 3% of the 379 FY 93 through FY 08 calls supporting a contingency) • One contingency supported (EF)
Calls supporting the war on terrorism	<ul style="list-style-type: none"> • Total war on terrorism calls = 383 calls (10% of the 3886 calls) <ul style="list-style-type: none"> ➢ Operation IRAQI FREEDOM = 139 calls (4% of the 3886) ➢ ENDURING FREEDOM = 244 calls (6% of the 3886 calls) • Total war on terrorism calls requiring a test = 95 (31% of the 310 calls requiring a test, and 25% of the 383 war on terrorism calls) 	<ul style="list-style-type: none"> • Total FY 08 war on terrorism calls = 26 calls (7% of the 365 calls) <ul style="list-style-type: none"> ➢ Operation IRAQI FREEDOM = 15 calls (4% of the 365 calls) ➢ ENDURING FREEDOM = 11 calls (3% of the 365 calls) • Total FY 08 war on terrorism calls requiring a test = 6 (32% of the 19 FY 08 calls requiring a test, and 23% of the FY 08 war on terrorism calls)

MILITARY COMMUNICATIONS-ELECTRONICS BOARD (MCEB) BRIEFINGS

JITC did not brief the MCEB on behalf of the Joint Staff in 2008.

SUMMARY

In 2008, the DoD improved interoperability throughout the Joint Force by adding systems to the ranks of certified systems and assessing numerous others for interoperability. Because determining the number of deployed systems in DoD is problematic, it is difficult to determine the overall status of interoperability throughout DoD. The total number of certified systems does not tell us the entire story. Much was accomplished, but much remains to be done as the number of new and legacy systems in the DoD inventory is vast and constantly changing.

APPENDICES:

- A OT&E Division
- B Focused Logistics/Business
- C C2 Battlespace Awareness
- D Force Application/Force Protection
- E Battlespace Communications
- F National Intelligence
- G Homeland Security/Information Assurance
- H Interoperability Test Certification Types

APPENDIX A

OT&E Division – JT1 Interoperability Status

Number of Systems	Interoperability Status Category
1	Limited Joint Interoperability Certification
<ul style="list-style-type: none">Limited Joint Interoperability Test Certification of the Department of Defense Teleport Generation One (DoD Teleport GEN 1) Initial Operational Capability 2 FOT&E 3 (IOC 2 FOT&E III)	
1	Interoperability Assessment
<ul style="list-style-type: none">Joint Interoperability Assessment of the Department of Defense (DoD) Teleport, Generation Two (Gen 2) Phase One (P1)	

APPENDIX B

Focused Logistics and Business Portfolio – JTB Interoperability Status

Number of Systems	Interoperability Status Category
4	Joint Interoperability Certification
	<ul style="list-style-type: none">• Joint Interoperability Certification of the Navy Enterprise Resource Planning (ERP) Template 1, Increment 1.0• Joint Interoperability Certification of the Optimized Organizational Maintenance Activity (OOMA) Version 831-01.05.10• Joint Interoperability Certification of the Global Decision Support System (GDSS) Version 2.1.1• Joint Interoperability Certification of the Distribution Planning and Management System (DPMS) Version 4.1
3	Limited Joint Interoperability Certification
	<ul style="list-style-type: none">• Limited Joint Interoperability Certification of the Theater Medical Information Program-Joint (TMIT-J) Block 2, Release 1, Service Pack 2• Limited Joint Interoperability Certification of the Patient Accounting System/Coding and Compliance Editor (PAS/CCE) Version 1.1.9.2• Limited Joint Interoperability Certification of the Armed Forces Health Longitudinal Technology Application (AHLTA) Block 2, Release 2, Version 3.3

APPENDIX C

C2 Battlespace Awareness Portfolio - JTC Interoperability Status

Number of Systems	Interoperability Status Category
3	Joint Interoperability Certification
	<ul style="list-style-type: none"> • Joint Interoperability Test Certification of the EA-6B Prowler Improved Capability II (EA-6B ICAP II) , Block 3 • Joint Interoperability Test Certification of the Multifunctional Information Distribution System (MIDS) on Ship (MOS) Model 4 Ships • Joint Interoperability Test Certification of the EA-6B Prowler Improved Capability III, Block 3, with Operational Flight Program 8.21
6	Limited Joint Interoperability Certification
	<ul style="list-style-type: none"> • Limited Joint Interoperability Test Certification of the Automatic Identification System (AIS) Version 2.1 • Limited Joint Interoperability Test Certification of the F-16 C/D (Block 40/42), Operational Flight Program (OFF) M4.1A+ • Limited Joint Interoperability Test Certification of the F-16 (Block 40/50) Common Configuration Implementation Program (F-16 CCIP), Operational Flight Program 4.3+ • Limited Joint Interoperability Test Certification of E-2C Group II+ Hawkeye 2000 (HE2K), Software Configuration Set - 05 • Limited Joint Interoperability Test Certification of the F-16 C/D (Block 40/50) Common Configuration Implementation Program (F-16 CCIP), Operational Flight Program M4.2A+ • Limited Joint Interoperability Test Certification of the Shadow Tactical Unmanned Aerial Vehicle (TUAV) RQ-7B •
1	Interoperability Certification Extension
	<ul style="list-style-type: none"> • Extension of the Joint Interoperability Test Certification of the EA-6B Improved Capability III (ICAP III), Block 3, with Operational Flight Program (OFF) 8.21, with extension to OFF 8.25
12	Joint Interoperability Assessment
	<ul style="list-style-type: none"> • Joint Interoperability Assessment of the Arrow Weapon System (AWS), Block 3.5 • Joint Interoperability Assessment of the F-16 (Block 40/42) (F-16), Operational Flight Program M4.1A+ • Joint Interoperability Assessment of the Battle Control Center - AFCENT (BC3), Version 1.1 • Joint Interoperability Assessment of the B-1B Joint Mission Planning System, Version .3.2.0105 Mission Planning Environment, Version 3.0 (JMPS) • Joint Interoperability Assessment of the F-15 C/E Suite 5 Joint Mission Planning System, Version 1.3.2.0105 Mission Planning Environment, Version 1.3.4 (JMPS) • Joint Interoperability Assessment of the EA-6B Improved Capability II, Block 4 Joint Mission Planning System-Maritime, Version 1.2.3.0292 Mission Planning Environment, Version 3.0.0.3 • Joint Interoperability Assessment for Joint Mission Planning System-Maritime Version 1.2.3.0268, Mission Planning Environment Version 2.0.4.2 with the E-2C Hawkeye • Joint Interoperability Assessment of the EA-6B Improved Capability III, Block 3 Joint Mission Planning System-Maritime, Version 1.2.3.0292 Mission Planning Environment, Version 4.0.0.5 • Joint Interoperability Assessment of the Joint Mission Planning System-Maritime, Version 1.1.1.5070 Mission Planning System, Version 2.0.13.1 EA-6B Improved Capability (ICAP) II , Block 3 (JMPS-M EA-6B V2.0.13.1) • Joint Interoperability Assessment of the Joint Mission Planning System-Maritime, Version 1.2.3.0268 Mission Planning Environment, Version 1.0.3.3 MV-22 (JMPS-M MV-22 V1.0.3.3) (NA) • Joint Interoperability Assessment of the Joint Mission Planning System-Maritime, Version 1.2.3.0291 Mission Planning Environment, Version 2.0.20.7 F-18 E/F (JMPS-M F-18 E/F V2.0.20.7) • Joint Interoperability Assessment of the Joint Mission Planning System-Maritime, Version 1.2.3.0292 Mission Planning System, Version 2.0.6.1 AV-8B (JMPS-M AV-8B V2.0.6.1)

Number of Systems	Interoperability Status Category
4	Standards Conformance Certification
	<ul style="list-style-type: none"> <li data-bbox="240 289 1365 411">• Military Standard (MIL-STD) 6011C, MIL-STD-6016C, MIL-STD-6020, and MIL-STD-3011 Standards Conformance Certification of Battle Control Center - United States Central Command Air Forces, Version 1.1, with Multi Source Correlator Tracker, Version 4.8.3.2, Joint Range Extension, Version 5.0 Update 5, and Joint Air Defense Systems Integrator, Version 12.3.1P2 <li data-bbox="240 415 1365 478">• Military Standard (MIL-STD) 6011C, and MIL-STD-6016C Standards Conformance Certification of E-2C Hawkeye 2000, Systems Configuration Set-05, Version 5.4.11. <li data-bbox="240 483 1365 541">• Military Standard 6016C Standards Conformance Certification of F-16 (Block40/42/50/52) Common Configuration Implementation Program (CCIP), Operational Flight Program Version M4.3+ <li data-bbox="240 546 1008 567">• Standards Conformance Certification of the Prophet, Version 1.0.21

APPENDIX D

Force Application/Force Protection Portfolio - JTD Interoperability Status

Number of Systems	Interoperability Status Category
4	Joint Interoperability Certification
	<ul style="list-style-type: none"> • Joint Interoperability Test Certification of the Advanced Targeting Forward Looking Infrared (ATFLIR) System • Joint Interoperability Test Certification of the F/A-18 E/F (F/A-18) Advanced Targeting Forward Looking Infrared (ATFLIR) System • Joint Interoperability Test Certification of the Joint Biological Point Detection System (JBPDS) Increment (Incr) 1 • Joint Interoperability Test Certification of the MH-47G Special Operations Chinook Aircraft
10	Limited Joint Interoperability Certification
	<ul style="list-style-type: none"> • Limited Joint Interoperability Certification of the United States Army Advanced Field Artillery Tactical Data System (AFATDS), Block II, Version 6.5 • Limited Joint Interoperability Certification of the A/OA-10C Precision Engagement (PE), Suite 3.3B, with Operational Flight Program (OFP) 3.3B4 • Limited Joint Interoperability Certification of the A/OA-10C Precision Engagement (PE), Suite 3.2C, with Operational Flight Program (OFP) 3.2C5 • Limited Joint Interoperability Test Certification of the RT-1763B/AN/APX-111 (V), Combined Interrogator/Transponder (CIT), Part Number 1007101G-20, Software Version 17C-005U/H4E, for U.S. Navy F/A-18E/F Mark XII Identification, Friend or Foe (IFF) Systems/Mode Select (Mode S) Transponder Upgrade • Limited Joint Interoperability Certification of the CV-22 Block 10 Osprey • Limited Joint Interoperability Certification of the MH-47G Service Life Extension Program (SLEP) Communications System • Limited Joint Interoperability Test Certification of the AN/SYQ-27 Mission Planning System, Fire Control, Version 3.5, aka Naval Fires Control System (NFCS) • Limited Joint Interoperability Test Certification of the MV-22 Block 10 Osprey • Limited Joint Interoperability Certification of the Target Location, Designation, and Hand-Off System (TLDHS), Block II, Version 1.1.2 (Certified May 19 2008) • Limited Joint Interoperability Certification of the Target Location, Designation, and Hand-Off System (TLDHS), Block II, Version 1.1.2 (Certified Sept. 30 2008)
7	Joint Interoperability Assessment
	<ul style="list-style-type: none"> • Joint Interoperability Assessment of the E-3G Airborne Warning and Control System (AWACS) Block 40/45 mission computer Link 11/16 developmental software • Joint Interoperability Assessment of the Amphibious Transport Dock, United States Ship (USS) San Antonio, Version (LPD 17) • Joint Interoperability Assessment of the UH-1Y Utility Helicopter, Increment I Ultrahigh Frequency (UHF) Satellite Communications (SATCOM) Antenna Relocation • Joint Interoperability Assessment of the Joint Chemical Agent Detector, Increment 1 • Joint Interoperability Assessment of the Joint Biological Standoff Detection System (JBSDS) Increment 1 • Joint Interoperability Assessment of the Next Generation Command and Control Processor (NGC2P) /Common Data Link Management System (CDLMS), Version 3.4.4.2.1-4 • Joint Interoperability Assessment of the Joint Air-to-Surface Standoff Missile (JASSM), Block 2 Variant with the Trimble JASSM Anti-Jam Global Positioning System (GPS) Receiver – Selective Availability Anti-Spoofing Module (SAASM) (JAGR-S)
11	Standards Conformance Certification
	<ul style="list-style-type: none"> • Military Standard (MIL-STD) 6011C, MIL-STD-6016C, and MIL-STD-6020 Standards Conformance

Number of Systems	Interoperability Status Category
	<p>Certification of Advanced Combat Direction System (Block 0), Version C10.27A, with Command and Control Processor, Version M4R4.14A06</p> <ul style="list-style-type: none"> • Military Standard (MIL-STD) 6011C and MIL-STD-6020 Standards Conformance Certification of Advanced Combat Direction System (ACDS) (Block 0), Version C10.27A.1, with Command and Control Processor (C2P) Rehost, Version R4R4.60200A • Military Standard (MIL-STD) 6016C and MIL-STD-3011 Standards Conformance Certification of B-1B Digital Communications Improvement (DCI), Version 1.0 • Military Standard 6040A Standards Conformance Certification of Common Message Processor, Version 4.7.7.0 • Military Standard 6017A Standards Conformance Certification of Common Message Processor, Version 5.1.2.0 • Military Standard (MIL-STD) 6011C and MIL-STD-6016C Standards Conformance Certification of E-2C Group II, Version N11 • Military Standard (MIL-STD) 6011C and MIL-STD-6016C Standards Conformance Certification of Forward Area Air Defense Command, Control, and Intelligence (FAAD C2I), Version 5.4B-11.0 • Military Standard 6040, 2006 Change 1 Baseline, Standards Conformance Certification of IRIS Forms, Version 2.4 • Military Standard 6016C Standards Conformance Certification of Special Information Systems (Rivet Joint) (SIS(RJ)), Version S0912-914-3 (8) • Military Standard 6040A Standards Conformance Certification of United States Message Text Format Test Tool (MTT), Version 8.0 • Variable Message Format (VMF) Technical Interface Design Plan (Test Edition), Reissue 5; Military Standard (MIL-STD) 6017; and MIL-STD-6017A Standards Conformance Certification of VMF Test Tool (VTT), Version 8.0
2	Standards Conformance Assessment
	<ul style="list-style-type: none"> • Software Block 3 Message Set Assessment of VMF Test Tool (VTT), Version 8.0 • Military Standard (MIL-STD) 6016C, MIL-STD-3011, and MIL-STD-6017A Standards Conformance Assessment of Situation Awareness Data Link 11xy Versions 11.4.0.9.5 and 11.4.0.9.5.1
3	Standards Conformance Non Cert
	<ul style="list-style-type: none"> • Military Standard (MIL-STD) 6011C, MIL-STD-6016C, MIL-STD-6020, and MIL-STD-3011 Standards Conformance Non-Certification of Common Aviation Command and Control System, Version 6.01, with Common Data Link Management System, Version 3.5 • Technical Interface Design Plan (Test Edition) (TIDP-TE) Reissue 5 (R5), Military Standard 6017, and Interface Requirements Specification (IRS) for the Command and Control Personal Computer (C2PC), Version 7.0.2, Standards Conformance Non-Certification of Joint Tactical Common Operational Picture Workstation, Version 1.0.0.0.19 • Military Standard (MIL-STD) 3011, MIL-STD-6011C, and MIL-STD-6016C Standards Conformance Non-Certification of the Interoperability Engineering System (IES), Version 2.24a

APPENDIX E

Battlespace Communications Portfolio - JTE Interoperability Status

Number of Systems	Interoperability Status Category
20	Joint Interoperability Certification
	<ul style="list-style-type: none"> • Joint Interoperability Certification of the United States Northern Command (USNORTHCOM) Mobile Command Platform-Sentinel (MCP-S), Version 1.0 • Joint Interoperability Certification of the Asynchronous Transfer Mode Microwave System (ATM-MS), Version 1.0 • Joint Interoperability Test Certification of the Asynchronous Transfer Mode Microwave System (ATM-MS), Version 1.0.1 • Joint Interoperability Test Certification of the Automated Digital Network System (ADNS), Increment IIa • Joint Interoperability Test Certification of the Automated Digital Network System (ADNS) Increment II, Patrol Coastal Network (PCN) Variant • Joint Interoperability Certification Letter for the Combined Enterprise Regional Information Exchange System-Maritime (CENTRIXS-M) AN/USQ-185B Variant (V) 1 • Joint Interoperability Test Certification of the Deployable Communications Capabilities Vehicle (DCCV), Version 2.1 • Joint Interoperability Test Certification of the Defense Information System Network (DISN) Asynchronous Transfer Mode (ATM) System Unclassified (DATMS/U), Version 1.x • Joint Interoperability Test Certification of the Theater Deployable Communications (TDC) Integrated Communications Element (ICE) Version 3 • Joint Interoperability Test Certification of the United States Northern Command (USNORTHCOM) Emergency Response Vehicle (ERV), Version 1 • Joint Interoperability Test Certification of the United States Northern Command (USNORTHCOM) Mobile Command Platform (MCP), Version 1 • Joint Interoperability Test Certification of the Joint Incident Site Communications Capability (JISCC), Version 2.34 • Joint Interoperability Test Certification of the Joint Incident Site Communications Capability (JISCC), Version Block II • Joint Interoperability Test Certification of the Air National Guard Joint Incident Site Communications Capability (JISCC), A-6 Variant • Joint Interoperability Test Certification of the United States Northern Command (USNORTHCOM), Joint Task Force Civil Support (JTF-CS), Tactical Package (TACPAC), Medium/Heavy Deployable Communications Package, Version 1 • Joint Interoperability Test Certification of the Combined Joint Task Force-82 (CJTF-82) Minuteman Mobile Switching Center (MSC), Version 1.0 • Joint Interoperability Test Certification of the AN/UMK-4(V)4 Naval Integrated Tactical Environmental System - Mobile Variant IV (NITES IV) • Joint Interoperability Test Certification of the Sensitive Compartmented Information (SCI) AN/USQ-148D Variant (V) 2 Network • Joint Interoperability Test Certification Letter for the Submarine Local Area Network (SubLAN) AN/USQ-177 • Joint Interoperability Certification of the Wireless for the Warfighter (W4W) Package, Version 1.0
9	Limited Joint Interoperability Certification
	<ul style="list-style-type: none"> • Limited Joint Interoperability Test Certification of the Weapons of Mass Destruction-Civil Support Team (WMD-CST) Analytical Laboratory System Increment 1, (ALS1) Version 1.0 • Limited Joint Interoperability Test Certification of the Automated Digital Network System (ADNS), Increment II Family of Systems (FoS) • Limited Joint Interoperability Test Certification of the Interoperable Communications Extension System (ICE-S), Version 1.1 • Limited Joint Interoperability Test Certification of the Lightweight Multi-band Satellite Terminal (LMST) AN/USC-65(V)1 and 2

Number of Systems	Interoperability Status Category
	<ul style="list-style-type: none"> • Limited Joint Interoperability Test Certification of the Pacific Star Communications 5500, Version 2.1 • Limited Joint Interoperability Test Certification of the Multi-Channel Satellite Terminals, Phoenix AN/TSC-156/156A/156B • Limited Joint Interoperability Test Certification of the Theater Deployable Communications (TDC) Expeditionary Package (EXP), Block 45 • Limited Joint Interoperability Certification of the United States Marine Corps (USMC) Transition Switch Module (TSM) • Limited Joint Interoperability Test Certification of the Wideband Global Satellite Communications System, Satellite Identifier 1462 WPAC
90	Special Interoperability Certification
	<ul style="list-style-type: none"> • Special Interoperability Test Certification of ADTRAN Total Access (TA) 1500 with Software Release 3.4 • Special Interoperability Test Certification of ADTRAN Total Access (TA) 1500 with Software Release 3.4 • Special Interoperability Test Certification of the Aethra Vega X3 with Software Release 11.4.14 • Special Interoperability Test Certification of the Aethra Vega X5 with Software Release 11.4.14 • Special Interoperability Test Certification of the Aethra Vega X7 System with Software Release 11.4.14 • Special Interoperability Test Certification of the Amcom Software Inc. Smart Center™, Event Notification and Response (e.Notify), and Smart Web™ Version 4.0.6.1 • Special Interoperability Test Certification of the Amcom Software Inc., Computer Telephony Integration (CTI) Cisco Smart Console Workstation Release 4.0.6 with the Cisco Catalyst 2960 software version 12.2 (25) • Special Interoperability Test Certification of the Amcom Software Inc., Computer Telephony Integration (CTI) Basic Operator Services System (BOSS) Workstation, Release 4.0.6 • Special Interoperability Test Certification of the Amcom Software Inc., Computer Telephony Integration (CTI) Release 4.0.6 with Alcatel-Lucent's 8520 and 8528T Integrated Services Digital Network (ISDN) Voice Terminal Hard Consoles • Special Interoperability Test Certification of the Captaris RightFax Enterprise Suite Version 9.3 FP2 SR3 with Dialogic Brooktrout Fax Boards • Special Interoperability Test Certification of the Cisco Assured Services Local Area Network (ASLAN) and non-ASLAN with Specified Software Releases • Special Interoperability Test Certification of Cisco CallManager (CCM) Version 4.2(3) Service Release (SR) 3, with Internetwork Operating System (IOS) Software Release 12.4(9) T1 • Special Interoperability Test Certification of the Cisco Internet Protocol Video Conference (IPVC) 3545 Video Teleconference (VTC) Multipoint Control Unit (MCU) Version 5.5.0.0.52 with Cisco IPVC 3540 Gateway Version 5.5.0.0.5 and 3545 Gateway Version 5.5.0.0.5 • Special Interoperability Test Certification of the Cisco Optical Network System (ONS) 15310 with Software Release 8.0.0 (08.00-007A-27.16) • Special Interoperability Test Certification of the Cisco Optical Network System (ONS) 15454 with Software Release 8.0.0 (08.00-007A-27.16) • Special Interoperability Test Certification of the Cisco Unity Unified Messaging System Software Release 5.0(1) with the Cisco CallManager • Special Interoperability Test Certification of the Cisco Unity Unified Messaging System Software Release 5.0(1) with Private Branch Exchange Internet Protocol Media Gateway (PIMG) Digital Interface • Special Interoperability Test Certification of the Cisco Unity Unified Messaging System Software Release 5.0(1) with Private Branch Exchange Internet Protocol Media Gateway (PIMG) Analog Interface • Special Interoperability Test Certification of the Cisco Unity Unified Messaging System Software Release 5.0(1) with T1 Internet Protocol Media Gateway (TIMG) Interface • Special Interoperability Test Certification of the Dialogic Communications Corporation (DCC)-USA Communicator! NXT with Software Release 4.0 • Special Interoperability Test Certification of Quantum Autoloader SuperLoader3 backup device

Number of Systems	Interoperability Status Category
	<p>Running Build Number v55-0 and InterNiche 3.1 Dual Stack Core and Quantum Scalar i500 Midrange Scalable Tape Library backup device Running Firmware Version 410G.GS007 and Linux Kernel 2.6.11-1 for Internet Protocol Version 6 (IPv6) Capability</p> <ul style="list-style-type: none"> • Special Interoperability Test Certification of TechGuard PoliWall Version 1.21.00 with Ethernet Interface and TechGuard PoliWall Version 1.21.00 with Fiber Interface for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of Cisco Catalyst 4500 Family of Layer 3 Switches with Supervisor Engine 6-E Running Internetworking Operating System Version 12.2(40)SG, for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of Cisco Catalyst 6500 Family of Layer 3 Switches with Supervisor Engine 720 Running Internetworking Operating System Version 12.2(33)SXH for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of Ambriel Technologies AT-X-S4400 Internet Protocol Version 4/Internet Protocol Version 6 (IPv6) Translator Family of Servers for IPv6 Capability • Special Interoperability Test Certification of the IBM Storage System TS3100 Tape Library Express and IBM Storage System TS3200 Tape Library Express Families of Tape Libraries Running Nucleus Net Version 5.4b, Nucleus Net Internet Protocol (IP) Version 6 (IPv6) Version 1.4b, Firmware Version 6.20/2.6EZ, and Nucleus Version 1.15 Operating System (OS) Running a Linux-Based Kernel and the IBM Storage System TS3400 Tape Library Running CENTE Version 1.30, Firmware Version 0001.6000, and uTRON Version 4.0 OS Running a Linux-Based Kernel for IPv6 Capability • Special Interoperability Test Certification of the Sun Microsystems SPARC T2000 and X86 V40z 32-bit and 64-bit Platforms Running Solaris 10 for IPv6 Capability • Special Interoperability Test Certification of the Datatek Applications, Inc., Internet Protocol Version 4/Internet Protocol Version 6 (IPv6) Transformer Running Software Version 2.1.4 for IPv6 Capability • Special Interoperability Test Certification of the Xerox Phaser 6360DT Running System Firmware 1.3.7.P, Family of Color Printers for IPv6 Capability • Special Interoperability Test Certification of Cisco 2811 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33)SRB1 System for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of the Red Hat Enterprise Linux 5.2 Server and Client running on the IBM P-Series High Volume Open Power Personal Computer Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32 and 64-bit x86 Laptop, and Dell Precision T5400 32 and 64 bit x86 Desktop for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Novell SuSE Linux Enterprise Server 10, Service Pack 2 Running on an IBM P-Series High Volume Open Power Personal Computer Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32 and 64-bit x86 Laptop, and Dell Precision T5400 32 and 64-bit x86 Desktop for IPv6 Capability • Special Interoperability Test Certification of the Dell PowerVault Storage System TL2000 and Dell PowerVault Storage System TL4000 Tape Libraries with an Embedded Transmission Control Protocol/Internet Protocol (TCP/IP) Dual Stack Core Running Firmware Version 6.60 for Internet Control Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of Microsoft Windows Server 2008 Standard Service Pack 1 Build 6.0.6001 Running on the Dell Power Edge R900, Dell Power Edge 2950, and Dell Power Edge 1950 Servers for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of the Dell MD-3000i, Running Firmware Version 06.70.17.60 for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of Cisco 3845 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33)SRB1 System for Internet Protocol Version 6 (IPv6) Capability • Special Certification of Quantum Autoloader SuperLoader3 backup device Running Build Number v61-0 and InterNiche 3.1 Dual Stack Core and Quantum Scalar i500 Midrange Scalable Tape Library backup device Running Firmware Version 500G.GS001 and Linux Kernel 2.6.11-1 for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of the Hewlett-Packard Jet Direct 635n/690n Print Server Card Firmware Version (V).38.05 for Internet Protocol Version 6 (IPv6) Capability

Number of Systems	Interoperability Status Category
	<ul style="list-style-type: none"> • Special Interoperability Test Certification of Broadcom Transmission Control Protocol (TCP)/Internet Protocol (IP) Offload Engine (TOE) part number BCM5709 and BCM57710 Network Interface Cards for IP Version 6 (IPv6) Capability • Special Interoperability Test Certification of the Quantum Scalar i2000, Firmware 571.GS00101 with the Datatek Internet Protocol (IP) Version 4/IP Version 6 (IPv6) Translator Version 2.1.4, Disk 040908.1, Build 033108.1 for IPv6 Capability • Special Interoperability Test Certification of Dell 5330DN Printer Family for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of Dell 5110CN Printer Family for Internet Protocol Version 6 (IPv6) Capability • Special Interoperability Test Certification of the Dell OptiPlex 755 Family of Host/Workstations Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell OptiPlex 740 Family of Host/Workstations Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell Latitude D630 Family of Host/Workstations Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell EqualLogic PS Series Array, Firmware Version 4.0.0 for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Fortinet FortiGate 400A and 3600, 3.00, Build 0726.080716 Family of Information Assurance Devices for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the IBM AIX Server and AIX Virtual Input/Output Server Running Version 0833A-611PV661b Service Pack 1 for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the McAfee IntruShield I-Series and M-Series Sensors for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of Microsoft Windows Vista, Service Pack 1, Operating System Running on the Dell OptiPlex 755, OptiPlex 740, and Latitude D630 Workstations for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Fortinet FortiGate 400A and 3600, 3.00, Build 0726.080716 Family of Information Assurance Devices for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Tandberg 3000MXP Running Software Version F7.1 Family for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Tandberg Video Communication Server Running Software Version X2.0 for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Tandberg Management Suite Version 11.9.1, Running on Microsoft Windows Server 2003 Enterprise Service Pack 2, Build 5.2.3790, for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Tandberg MPS 800 Running Software Version J4.4 Family for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Juniper SSG 550M Firewall Running ScreenOS Version 6.2 Software for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Juniper SSG 320M Firewall Running ScreenOS Version 6.2 Software for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Juniper SSG 20 Firewall Running ScreenOS Version 6.2 Software for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Juniper NS-5400 Firewall Running ScreenOS Version 6.2 Software for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Juniper ISG-2000 Firewall Running ScreenOS Version 6.2 Software for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Polycom HDX 9000x Product Family, Running Software Version 2.0.5_J for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Brocade SilkWorm 200E Fiber Channel Switch

Number of Systems	Interoperability Status Category
	<p>Running Fabric Operating System Version 6.2 Software for Internet Protocol Version 6 Capability</p> <ul style="list-style-type: none"> • Special Interoperability Test Certification of the Hewlett-Packard LaserJet P2055, Firmware Version V37.07.SD, Family of Printers for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell 3130CN Running Software Version 2.1.0 (0/9), Printer Family for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell Latitude E5500 and Precision M6400 32-bit Family of Notebook Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of Dell 2330DN Printer Running Software Version FPN.APS.F001abd-0 for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell OptiPlex 360 32-bit and 64-bit Family of Desktop Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell OptiPlex 160 32-bit Desktop Computer Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell Precision M6400 64-bit Notebook Computer Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell Latitude E6500 32-bit and 64-bit Family of Notebook Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Dell OptiPlex 960 32-bit and 64-bit Family of Desktop Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of Quantum Scalar i2000 Tape Library for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the IBM z/OS Version 1.10 Operating System for IBM Mainframe Computer Systems for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard xw9400 Workstation Family Running Microsoft Windows Vista Service Pack 1 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard ProLiant DL380 Family of Servers Running the Windows Server 2008 Service Pack 1 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard ProLiant DL380 Family of Servers Running the SUSE Linux Enterprise Server 10 Service Pack 2 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard ProLiant DL380 Family of Servers Running the Red Hat Enterprise Linux RHEL5.2 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard (HP) 9000 RP3440 Systems Family of Servers Running the HP-UX 11i v3 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard (HP) Integrity RX2660 Systems Family of Servers Running the HP-UX 11i v3 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard Integrity RX2660 Family of Servers Running the Red Hat Enterprise Linux RHEL5.2 Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the Hewlett-Packard Integrity RX2660 Family of Servers Running the SUSE Linux Enterprise Server 10 Service Pack 2, Operating System for Internet Protocol Version 6 Capability • Special Interoperability Test Certification of the LiteScape Biometric Secure Profile Authentication Reader (SPAR)™ with Secure Profile Management (SPM) Version 3.0 Net4.0 for Linux 2.4

Number of Systems	Interoperability Status Category
	<ul style="list-style-type: none"> • Special Interoperability Test Certification of Mitel 3300 Internet Protocol Communications Platform (ICP) with Software Release 8.0.6.1_2 • Special Interoperability Test Certification of NET VX900 with Software Release 4.3.5 Version 55 • Special Interoperability Test Certification of Nortel Communication Server (CS) 2100 Extended Architecture Core (XACore) with Software Release Succession Enterprise (SE)09.1 and specified Software Patch Groups • Special Interoperability Test Certification of the Nortel Optical Multiservice Edge (OME) 6500 with Software Release 4.01 • Special Interoperability Test Certification of the Polycom HDX 9000 Series with Software Release 2.0.0J • Special Interoperability Test Certification of Real Time Monitors, Inc. Switch Expert with Software Release 6.0 • Special Interoperability Test Certification of the Tekelec Eagle® Signal Transfer Point (STP) with Software Release 35.6.1-56.52.0 • Special Interoperability Test Certification of the Mobile Subscriber Equipment (MSE) and Tri-Service Tactical Communications Program's (TRI-TAC) Common Baseline Circuit Switch (CBCS) software, Version RD302210
8	Interoperability Certification Extension
	<ul style="list-style-type: none"> • Extension of the Special Interoperability Test Certification of the Avaya S8710 and S8720 Digital Switching Systems with Software Release Communication Manager (CM) 4.0 (R014x.00.2.731.7: Super Patch 14419) to include the S8700 with Software Release CM 4.0 (R014x.00.2.731.7: Super Patch 14419) • Extension of the Special Interoperability Test Certification of the Callware Technologies Callegra UC TM Server with Software Release 6.14-Joint Interoperability Test Command (JITC) • Extension of the Special Interoperability Test Certification of the Alcatel-Lucent Class 5 Electronic Switching System (5ESS) Digital Switching System and Compact Digital Exchange (CDX) both with Software Release 5E16.2, Broadcast Warning Message (BWM) 07-0003 • Extension of the Special Interoperability Test Certification of the Alcatel-Lucent Class 5 Electronic Switching System (5ESS) Very Compact Digital Exchange (VCDX) Digital Switching System with Software Release 5E16.2, Broadcast Warning Message (BWM) 07-0003 • Extension of the Special Interoperability Test Certification of Extreme Assured Services Voice Application Local Area Network (ASVALAN) and Voice Application Local Area Network (VALAN) with Native Operating System 11.6.1.9 • Extension of the Special Interoperability Test Certification of the Foundry Assured Services Voice Application Local Area Network (ASVALAN) and Voice Application Local Area Network (VALAN) with Specified Software Releases • Joint Interoperability Certification Extension for the Integrated Shipboard Network System (ISNS), AN/USQ-153A Variant (V) 1 • Extension of the Special Interoperability Test Certification of Plant Equipment Incorporated (PEI) VESTA M-1 Version 2.4
19	Joint Interoperability Assessment
	<ul style="list-style-type: none"> • Joint Interoperability Assessment of the Applied Marine Technology, Inc. (AMTI), A320 20-Watt Multi-band Amplifier, software versions 3.0 and 4.0 • Joint Interoperability Assessment of the Applied Marine Technology, Inc. (AMTI), A3575 50/75-Watt Multi-band Amplifier, software versions 0.6 and 1.0 • Interoperability Assessment of the Rockwell Collins AN/ARC-210 (RT-1851(C)) Warrior Airborne Communications System, software version 984-1560-002, in Single Channel Ground and Airborne Radio System (SINCGARS) mode • Interoperability Assessment of the Harris AN/PRC-117G (RF-7800M) Single-Channel, Multi-Band, Manpack Radio (AN/PRC-117G) • Interoperability Assessment of the Harris AN/PRC-152 Multi-Band Radio (AN/PRC-152) • Joint Interoperability Assessment of the Motorola AN/PRC-153 Ultrahigh Frequency Modulation Handheld Radio, Software Version 08.50.01 • Joint Interoperability Assessment of the Asynchronous Transfer Mode Microwave System (ATM-MS),

Number of Systems	Interoperability Status Category
	<p>Version 1.0</p> <ul style="list-style-type: none"> • Joint Interoperability Assessment of the AN/PRQ-7 Combat Survivor Evader Locator (CSEL) • Joint Interoperability Assessment of the Commercial Broadband Satellite Program (CBSP) Small Ship Variant (SSV) • Joint Interoperability Assessment Letter of the Integrated Shipboard Network System (ISNS), AN/USQ-153A, Variant (V) 5 • Joint Interoperability Assessment Letter of the Integrated Shipboard Network System (ISNS), AN/USQ-153A, Variant (V) 9 • Interoperability Assessment of the Interoperable Communications Extension System (ICE-S) Emergency Alert System Restoration Capability (EAS-RC), version 1.1 • Joint Interoperability Assessment of the United States Marine Corps (USMC), Joint Enhanced Core Communications System (JECCS) Block II • Joint Interoperability Assessment of the Thales AN/PRC-148(V)4 Joint Tactical Radio System Enhanced Multi-Band Inter/Intra Team Radio (JEM), Software Version 03.01.05.0032 • Joint Interoperability Assessment of the United States Army Alaska (USARAK) Mobile Command and Control Vehicle (MC2V), Version 1.0 • Joint Interoperability Assessment of the Rockwell Collins RT-1851A(C) SINCGARS • Joint Interoperability Assessment of the Southwest Asia Commercialization of Communications (SWACC), Version 1.0 • Joint Interoperability Assessment of the Harris VRC-110 Vehicle Mounted Radio • Joint Interoperability Test Assessment of the Wideband Global Satellite Communication (SATCOM) System (WGS)
52	Standards Conformance Certification
	<ul style="list-style-type: none"> • Military Standard (MIL-STD)-188-183 standards conformance certification for the AN/ARC-234(C)(V)1, AN/ARC-234(C)(V)2, AN/ARC-234A(C)(V)1, and AN/ARC-234A(C)(V)2 configurations of the Airborne Integrated Terminal Group (AITG) • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/ARC-234(C)(V)1, AN/ARC-234(C)(V)2, AN/ARC-234A(C)(V)1, and AN/ARC-234A(C)(V)2 configurations of the Airborne Integrated Terminal Group (AITG) • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/ARC-234(C)(V)1, AN/ARC-234(C)(V)2, AN/ARC-234A(C)(V)1, and AN/ARC-234A(C)(V)2 configurations of the Airborne Integrated Terminal Group (AITG) • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/ARC-210(V) (Dual RT-1851(C)/ARC) Airborne Communications System with the AM-7628/ARC-210 Amplifier/Filter • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/ARC-210(V) (Dual RT-1851(C)/ARC) Airborne Communications System with the AM-7628/ARC-210 Amplifier/Filter • Military Standard (MIL-STD)-188-183 standards conformance certification for the AN/ARC-210(V) (Dual RT-1851(C)/ARC) Airborne Communications System with the AM-7628/ARC-210 Amplifier/Filter • Military Standard (MIL-STD)-188-183 standards conformance certification for the AN/PRC-117F(C)(V) Ultrahigh Frequency (UHF) Manpack Satellite Terminal • Military Standard (MIL-STD)-188-182 standards conformance certification for the AN/PRC-117F(C)(V) Ultrahigh Frequency (UHF) Manpack Satellite Terminal • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/PRC-117F(C)(V) Ultrahigh Frequency (UHF) Manpack Satellite Terminal • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/PRC-117F(C) Ultra High Frequency (UHF) Manpack Satellite Terminal • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/PRC-117F(C) Ultra High Frequency (UHF) Manpack Satellite Terminal • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/PRC-117G(V)1(C) Multiband Multimission Manpack Radio • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/PRC-

Number of Systems	Interoperability Status Category
	<p>117G(V)1(C) Multiband Multimission Manpack Radio</p> <ul style="list-style-type: none"> • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/PRC-117G(V)1(C) Multiband Multimission Manpack Radio • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/VRC-110 Multiband Vehicular Radio System • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/VRC-110 Multiband Vehicular Radio System • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/VRC-110 Multiband Vehicular Radio System • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/PRC-152(V)1(C) Multiband Handheld Radio • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/PRC-152(V)1(C) Multiband Handheld Radio • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/PRC-152(V)1(C) Multiband Handheld Radio • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/VRC-103(V)1 Ultra High Frequency (UHF) Vehicular Mounted Satellite Terminal • Military Standard (MIL-STD)-188-182 standards conformance certification for the AN/VRC-103(V)1 Ultra High Frequency (UHF) Vehicular Mounted Satellite Terminal • Military Standard (MIL-STD)-188-183 standards conformance certification for the AN/VRC-103(V)1 Ultra High Frequency (UHF) Vehicular Mounted Satellite Terminal • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/VRC-03(V)1 Ultra High Frequency (UHF) Vehicular Mounted Satellite Terminal • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/VRC-03(V)1 Ultra High Frequency (UHF) Vehicular Mounted Satellite Terminal • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/USC-61(C) Digital Modular Radio (DMR) RFA Software release 02.01.02 • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/USC-61(C) Digital Modular Radio (DMR) System RFA Software release 02.01.02 • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/USC-61(C) Digital Modular Radio (DMR) System RFA Software release 02.01.02 • Military Standard (MIL-STD)-188-181B standards conformance certification for the AN/USC-61(C) Digital Modular Radio (DMR) System RFA Software release 04.20.03 • Military Standard (MIL-STD)-188-182A standards conformance certification for the AN/USC-61(C) Digital Modular Radio (DMR) System RFA Software release 04.20.03 • Military Standard (MIL-STD)-188-183A standards conformance certification for the AN/USC-61(C) Digital Modular Radio (DMR) System RFA Software release 04.20.03 • Military Standard (MIL-STD) 188-110B and Appendix C (High Frequency (HF) Data Modem Waveforms for Data Rates Above 2400 Bits Per Second (BPS)) Conformance Certification Test for Rockwell Collins Modem (MDM) Q9604 HF Four Channel Data Modem Version 12.07 • Military Standard (MIL-STD) 188-110B and Appendix C (High Frequency (HF) Data Modem Waveforms for Data Rates Above 2400 Bits Per Second (BPS)) Conformance Certification Test for Rockwell Collins Modem (MDM) Q9604 HF Four Channel Data Modem Version 11.04 • North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG) 5066 Edition 1 (Annexes A, B, C, and D) Conformance Certification of the Rockwell Collins High Frequency (HF) Messenger Version (V) 3.7 E-Mail Software with Optional Subnet Client, Compressed File Transfer Protocol (CFTP) • North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG) 5066 Edition 1 (Annexes A, B, C, and D) Conformance Certification of the Rockwell Collins High Frequency (HF) Messenger Version (V) 3.7 E-Mail Software with Optional Subnet Client, HF Mail Transfer Protocol (HMTP) • Military Standard (MIL-STD)-188-141B Conformance Certification of the AN/URC-146(V) High Frequency (HF) Shipboard Automatic Link Establishment (ALE) Radio (HFSAR) System • Military Standard (MIL-STD)-188-183 Conformance Certification of the MD-1324(C)/U Modem with

Number of Systems	Interoperability Status Category
	<p>the RT-1107(V)15/WSC-3(V) Transceiver (Certification 700.32033)</p> <ul style="list-style-type: none"> • Military Standard (MIL-STD)-188-181A Conformance Certification of the MD-1324(C)/U Modem with the RT-1107(V)15/WSC-3(V) Transceiver (Certification 698.32033) • Military Standard (MIL-STD)-188-182A Conformance Certification of the MD-1324(C)/U Modem with the RT-1107(V)15/WSC-3(V) Transceiver (Certification 699.32033) • Military Standard (MIL-STD)-188-182A Conformance Certification of the MD-1324(C)/U Modem with the RT-1107(V)17/WSC-3(V) Transceiver (Certification 686.32033) • Military Standard (MIL-STD)-188-183 Conformance Certification of the MD-1324(C)/U Modem with the RT-1107(V)17/WSC-3(V) Transceiver • Military Standard (MIL-STD)-188-181A Conformance Certification of the MD-1324(C)/U Modem with the RT-1107(V)17/WSC-3(V) Transceiver (Certification 685.32033) • Military Standard (MIL-STD)-188-161D and North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG) 5000 Type I digital facsimile standards conformance certification for the Ricoh SMFC210M Secure Digital Facsimile with firmware Version 2.08 • STANAG 4415 standards conformance certification for Rockwell Collins MDM-Q9604 modem with sys apps version 12.07 • STANAG 4529 standards conformance certification for Rockwell Collins MDM-Q9604 modem with sys apps version 12.07 • DTR to the AN/ARC-231 (RT-1808A(C)/U MOD 7) Airborne Communications System • Military Standard (MIL-STD)-188-182A standards conformance certification for the Ultrahigh Frequency (UHF) Naval Satellite Communications (SATCOM) Terminal Sistema Italiano di Comunicazioni Riservate ed Allarmi (SICRAL) • Military Standard (MIL-STD)-188-183 standards conformance certification for the Ultrahigh Frequency (UHF) Naval Satellite Communications (SATCOM) Terminal Sistema Italiano di Comunicazioni Riservate ed Allarmi (SICRAL) • Military Standard (MIL-STD)-188-181A standards conformance certification for the Ultrahigh Frequency (UHF) Naval Satellite Communications (SATCOM) Terminal Sistema Italiano di Comunicazioni Riservate ed Allarmi (SICRAL) • Military Standard (MIL-STD)-188-182A Conformance Certification of the RT-1828(P)/G Ultrahigh Frequency (UHF) Satellite Communications (SATCOM) Terminal with Ophir High Power Amplifier (HPA) Models 4039 and 4039R, and the Cidaal Electronics Model LNA-30U-MS(D) Low Noise Amplifier (LNA) (Certification 707.32033) • Military Standard (MIL-STD)-188-183 Conformance Certification of the RT-1828(P)/G Ultrahigh Frequency (UHF) Satellite Communications (SATCOM) Terminal with Ophir High Power Amplifier (HPA) Models 4039 and 4039R, and the Cidaal Electronics Model LNA-30U-MS(D) Low Noise Amplifier (LNA) (Certification 708.32033) • Military Standard (MIL-STD)-188-181B Conformance Certification of the RT-1828(P)/G Ultrahigh Frequency (UHF) Satellite Communications (SATCOM) Terminal with Ophir High Power Amplifier (HPA) Models 4039 and 4039R, and the Cidaal Electronics Model LNA-30U-MS(D) Low Noise Amplifier (LNA) (Certification 706.32033)
14	Standards Conformance Assessment
	<ul style="list-style-type: none"> • RTCA/DO-186A, EUROCAE ED-23B, and TSO-C169 Very High Frequency (VHF) Amplitude Modulation (AM) Air Traffic Control (ATC) Standards Conformance Assessment of the AN/ARC-210 (RT-1851(C)) Warrior with a VHF Collocation Filter • RTCA/DO-186A, EUROCAE ED-23B, and TSO-C169 Very High Frequency (VHF) Amplitude Modulation (AM) Air Traffic Control (ATC) Standards Conformance Assessment of the AN/ARC-210 (RT-1851(C)) Warrior, SW Version 984-1560-002 • (U) Military Standard-188-241 Single Channel Ground and Airborne Radio System (SINCGARS) Compliance Assessment of the AN/PRC-117F RT-1796(P)(C)/PRC, SW Version 4.3.1.4 • (U) Joint Interoperability Engineering Organization Specification 9120A, Have Quick/Have Quick II Conformance Assessment of the AN/PRC-117F RT-1796(P)(C)/PRC • Military Standard (MIL-STD) -188-243, Tactical Single Channel Ultrahigh Frequency (UHF) Radio Communications Conformance Assessment of the AN/PRC-117F RT-1796(P)(C)/PRC, SW Version

Number of Systems	Interoperability Status Category
4.3.1.4	<ul style="list-style-type: none"> • Military Standard (MIL-STD)-188-242, Tactical Single Channel Very High Frequency (VHF) Radio Equipment Conformance Assessment of the AN/PRC-117F RT-1796(P)(C)/PRC • Military Standard (MIL-STD)-188-242, Tactical Single Channel Very High Frequency (VHF) Radio Equipment Conformance Assessment of the AN/PSC-5D RT-1672(C)/U, Software Version 04.00.05 • Military Standard (MIL-STD)-188-243, Tactical Single Channel Ultrahigh Frequency (UHF) Radio Communications Conformance Assessment of the AN/PSC-5D RT-1672(C)/U, Software Version 04.00.05 • (U) Military Standard-188-241-2 Single Channel Ground and Airborne Radio System (SINCGARS) Compliance Assessment of the AN/PSC-5D RT-1672D(C)/U, SW Version 4.00.05 • (U) Joint Interoperability Engineering Organization Specification 9120A, Have Quick/Have Quick II Conformance Assessment of the AN/PSC-5D RT-1672D(C)/U, SW Version 4.00.05 • Military Standard (MIL-STD)-188-184 Conformance Assessment of the Personal Digital Assistant (PDA)-184 Data Controller • Military Standard (MIL-STD)-188-184 Conformance Assessment of the ViaSat Data Controller (VDC)-600 Personal Data Controller II • Military Standard (MIL-STD)-188-184 Conformance Assessment of the ViaSat Data Controller (VDC)-500 Advanced Data Controller for Internet Protocol (ADC/IP) • Military Standard (MIL-STD)-188-181A conformance assessment of the Wedgetail Broadcast Intelligence (BI) Tactical Data Processor

APPENDIX F

National Intelligence Portfolio - JTF Interoperability Status

Number of Systems	Interoperability Status Category
3	Joint Interoperability Certification
	<ul style="list-style-type: none"> • Joint Interoperability Test Certification of the Distributed Common Ground System-Army (DCGS-A), Version (V) 3.1.1 Basic Analyst Laptop (BAL) • Joint Interoperability Test Certification of the JOURNEYMAN Dissemination Modernization Increment 1, Spiral 1 • Joint Interoperability Test Certification of the Distributed Common Ground/Surface System-Marine Corps, Technical Control and Analysis Center, Version (V) 4.0.1
8	Limited Joint Interoperability Certification
	<ul style="list-style-type: none"> • Limited Joint Interoperability Certification for the Deployable Joint Command and Control System Increment 1, Spiral 1.1.1 • Limited Joint Interoperability Test Certification of the Deployable Joint Command and Control System, Rapid Response Kit, Version 1.0 • Limited Joint Interoperability Test Certification of the Deployable Joint Command and Control System, Rapid Response Kit, Version 1.0 • Limited Joint Interoperability Certification for the Deployable Joint Command and Control System (DJC2) Increment 1, Spiral 1.2 • Limited Joint Interoperability Certification for the SHAREDVISION (SV) Increment 1 • Limited Joint Interoperability Test Certification of the Ship's Signal Exploitation Equipment Increment E (SSEE Inc E) • Limited Joint Interoperability Test Certification of the Ship's Signal Exploitation Equipment (SSEE) Increment (Inc) E, Version (V) 3.9.3 Variant (3) • Limited Joint Interoperability Test Certification of the Tactical Exploitation Group Main (TEG-M), Version 10.0
30	Joint Interoperability Assessment
	<ul style="list-style-type: none"> • Joint Interoperability Assessment of the Active Earthscape, Version 2.0.2 • Joint Interoperability Assessment of the Broadcast Request Imagery Technology Environment (BRITE), Version 3.0.2.2 • Joint Interoperability Assessment for the Centralized Allocation Enterprise for Surveillance and Reconnaissance (CAESAR), Version (V) 2.0 • Joint Interoperability Assessment for the Collaborative Force Analysis, Sustainment and Transportation (CFAST), Version 5.0 • Joint Interoperability Assessment for the Combating Terrorism Knowledge Base (CTKB), Version (V) 3.0 • Joint Interoperability Assessment for the Combating Terrorism Knowledge Base (CTKB), Version 3.1 • Joint Interoperability Assessment for the Combined Theater Analyst Vetted Relational System (CTAVRS), Version (V) 3.0 • Joint Interoperability Assessment for the Defense Counterintelligence Information System (DCIIS) Portico, Version 7.0 • Joint Interoperability Assessment of the Defense Intelligence Operations Coordination Center (DIOCC) OverWatch, Version 2.0 • Joint Interoperability Assessment for the Department of Defense Intelligence Information System (DoDIIS) Portal, Version 1.0 • Joint Interoperability Assessment for the Department of Defense Intelligence Information System (DoDIIS) Portal, Version 1.1 • Joint Interoperability Assessment for the Direct-access User Knowledge Environment (DUKE), Version 5.3 • Joint Interoperability Assessment for the Imagery Exploitation Support System Version 5.3.2.0.01 • Joint Interoperability Assessment for the Information Warfare Planning Capability (IWPC), Version (V) 4.2

Number of Systems	Interoperability Status Category
	<ul style="list-style-type: none"> • Joint Interoperability Assessment for the Infrastructure Operations Tools Access (IOTA), Version 2.0 • Joint Interoperability Assessment of the Joint Force Projection (JFP) Version 2.3 • Joint Interoperability Assessment of the VisuaLinks (VL), Version 5.1 • Joint Interoperability Assessment for the Modernized Integrated Database (MIDB), Version 2.1.3.6.1 • Joint Interoperability Assessment for the Modernized Integrated Database (MIDB), Version 2.1.3.7 • Limited Joint Interoperability Assessment of the Multi-Sensor Aerospace-Ground Joint Intelligence, Surveillance, and Reconnaissance Interoperability Coalition (MAJIIC) • Joint Interoperability Assessment of the Measurement and Signature Intelligence (MASINT) Requirements System/MASINT Data Broker (MRS/MDB), Version 4.0.1 • Joint Interoperability Assessment for the National System for Geospatial-Intelligence Library Environment Fiscal Year 2007 Epoch Capability • Joint Interoperability Assessment for the Planning Tool for Resource Integration, Synchronization, and Management (PRISM), Version 4.2 • Joint Interoperability Assessment for the Secure Messaging and Routing Terminal Next Generation (SMART.neXt), Version (V) 3.1 • Joint Interoperability Assessment of the Sensitive Compartmented Information Global Command and Control System – Integrated Imagery and Intelligence (SCI GCCS-I3), Version 4.2 • Joint Interoperability Assessment for the Tripwire Analytic Capability (TAC) Version (V) 5.1.1 • Joint Interoperability Assessment for the Tripwire Analytic Capability (TAC), Version 6.0 • Joint Interoperability Assessment for the Web Intelligence Search Engine Autonomy and Endeca (WISE A&E), Version 1.0 • Joint Interoperability Assessment for the Web-enabled Timeline Analysis System (WebTAS), Version (V) 3.1 • Joint Interoperability Assessment for the Web-enabled Timeline Analysis System (WebTAS), Version 3.3

APPENDIX G

Homeland Security/Information Assurance Portfolio - JTG Interoperability Status

Number of Systems	Interoperability Status Category
1	Interoperability Assessment
	<ul style="list-style-type: none">Joint Interoperability Assessment for the Direct-access User Knowledge Environment (DUKE) Version (V) 5.2
2	Standards Conformance Certification
	<ul style="list-style-type: none">Department of Defense Electronic Biometric Transmission Specification, Version (V) 1.2 Conformance Certification of the Sensitive Site Exploitation (SSE) Identification (ID) Kit-Fusion V1.0Department of Defense Electronic Biometric Transmission Specification Version (V) 1.2 Conformance Certification of the Tactical Biometric Collection and Matching System (TBCMS) V5.1.0

APPENDIX H

Interoperability Test Certification Types

Joint Interoperability Test Certification - JITC issues this certification when a system has adequately demonstrated interoperability for at least all critical threshold requirements pertaining to a specific increment. This certification attests that the system's interoperability is sufficient to support a fielding decision. Evaluation should continue until the status of all objective interoperability requirements can be determined and reported.

Limited Joint Interoperability Test Certification - JITC issues this certification when a system has adequately demonstrated interoperability for a subset of interoperability requirements (has not met all threshold requirements). A "limited" certification may not be sufficient to allow fielding. If military necessity warrants fielding of the system for the demonstrated capabilities, the system sponsor should contact the Joint Staff J-6 to request a formal modification of the Net Ready-Key Performance Parameter (or legacy Interoperability-KPP) or the Military Communications-Electronics Board/Interoperability Test Panel for an Interim Certificate to Operate.

Special Interoperability Test Certification - JITC issues this certification for systems or system components (e.g., network infrastructure components) that require interoperability test certification but are not subject to the Joint Capabilities Integration and Development System process, and generally do not individually need requirements certified by J-6 (e.g., commercial switches being procured to operate in the Defense Switched Network, in-line encryption devices). JITC will work with J-6 to verify that the item is not subject to J-6 certification.

Interoperability Assessment - JITC issues this document following testing (Operational Assessments, JITC compatibility and interoperability assessments) to provide feedback concerning interoperability strengths and weaknesses when a certification is not appropriate. An interoperability assessment is not sufficient to allow fielding.

Standards Conformance Certification - JITC issues this certification after technical testing against published standards/standards profiles documented in the Technical View-1 created in the DISRonline tool to describe the degree of conformance to that standard/profile (e.g., conformance to Military Standard -188-181 Demand Assigned Multiple Access Satellite Communications). A standards conformance certification is not sufficient to allow fielding. Additional testing beyond that needed for a standard may be required to determine compliance with standards profiles.