NOT MEASUREMENT SENSTIVE

MIL-HDBK-524
26 June 2012

DEPARTMENT OF DEFENSE HANDBOOK

INTEROPERABLE SYSTEMS MANAGEMENT AND REQUIREMENTS TRANSFORMATION (iSMART) PROCESS

THIS HANDBOOK IS FOR GUIDANCE ONLY.
DO NOT CITE THIS DOCUMENT AS A REQUIREMENT.

AMSC NA **FSC 5895**

Foreword

1. This handbook is approved for use by all Departments and Agencies of the Department of Defense (DOD).
2. This DOD Handbook is based on the Joint interoperable Systems Management and Requirements Transformation (iSMART) Handbook of 1 September 2008, to which all Services are signatories. The iSMART Handbook is a collaborative effort between the Services and the Joint Staff to promote development of interoperable systems at the tactical edge of the Global Information Grid (GIG). The iSMART process is a systems engineering approach to achieving effective interoperability in a cost-effective manner. A common system engineering method initiated at the beginning of system development significantly increases the probability of fielding systems that maximize contribution to joint capabilities. iSMART provides the focus needed for the efficient use of resources, including money, time, manpower, and facilities. The end state of the iSMART process is the rapid transfer of tactical digital information to and between sensors, shooters, and Command and Control (C2) nodes to maximize war fighting capabilities.
3. The iSMART process complements existing DOD acquisition policy. iSMART bridges the gap between the high-level specification of platform capabilities and the technical-level documentation of computer program performance necessary to implement interoperable tactical data links. It translates high level requirements into the bit-level implementation that meets those requirements, while maintaining Allied, Joint and Service interoperability. Without iSMART, platform implementation of the tactical data link related information exchange systems which comprise the Tactical Data Enterprise Services (TDES) is often based on legacy/stovepipe requirements, and the results can be a non-interoperable system that does not support the joint war fighting efforts. Early application of the iSMART process in the development cycle ensures accurate specification of requirements, at a significant cost-savings to the program.
4. Implementation and refinement of the iSMART process is evolving, and platforms from all the Services are in various stages of executing the iSMART process. Platforms that have implemented iSMART early in the acquisition cycle are realizing the benefits of planned interoperability such as early problem correction, timely cost decisions, and full documentation of a platform's information exchange capabilities.
5. There are several objectives to be achieved before the value of the iSMART process will be realized. These include establishing DOD policy, resolving funding issues, developing joint Concepts of Network Employment (CONE) by mission area, and the development and management of joint tools to aid in the use of the iSMART process.
6. Currently, each Service bears the cost to implement iSMART, and funding support of the iSMART execution process is inconsistent across the Services. To resolve these issues, the Joint Staff and the Defense Information Systems Agency (DISA) are in the process of

advocating iSMART implementation policy and funding mandates. These mandates will result in improved platform interoperability throughout DOD and improved mission effectiveness in joint mission areas.

7. Access to this document is available at the DSPO's Assist Standards Repository located at https://assist.dla.mil/

8. Comments, suggestions, or questions on this document should be addressed to SPAWAR Systems Center Pacific, Attn: Code 591, 53560 Hull St., San Diego, CA 92152-5001 or emailed to ismart@navy.mil.

TABLE OF CONTENTS

PARAGRAPH PAGE

PARAGRAPH PAGE

FIGURES

FIGURE PAGE

TABLES

TABLE PAGE

1. SCOPE

1.1. Application. This handbook provides guidance and describes the systems engineering approach to determine the information exchange requirements for Information Technology/National Security Systems (IT/NSS) and weapon systems implementing tactical digital data links.

This Page Intentionally Left Blank

2. APPLICABLE DOCUMENTS

2.1. General. Unless otherwise specified, the following documents are those listed in the latest issue of the Department of Defense Index of Specifications and Standards (DODISS) and supplement cited in the solicitation, and form a part of this handbook to the extent specified herein.

2.2. Government Documents.

2.2.1. Specifications, Standards, and Handbooks.

MILITARY

Capability Development Document (CDD)	–	Tactical Data Link Transformation (TDL-T), 22 January 2004
Military Standard (MIL-STD) 6016 series (C and later editions)	–	Tactical Data Link Transformation (TDL-T), 22 January 2004

2.2.2. Other Government Publications. This standard supplements, but does not supersede the regulations for each Service. All offices responsible for tactical data links should have a copy of the references applicable to their Service. The following government publications are referenced in this standard:

JOINT CHIEFS OF STAFF

Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6212.01series	–	Interoperability and Supportability of Information Technology and National Security Systems
United States Joint Forces Command (USJFCOM) Joint Battle Management Command and Control (JBMC2) Joint Close Air Support (JCAS) Joint Mission Thread (JMT)	–	Event 1 Desk Top Analysis, 15 June 2006
JROCM 131-06, Policy for Implementing CJCSI 6212.01series	–	Net-Ready Key Performance Parameter (NR-KPP) Requirements in Capabilities Documents
CJCSI 6610.01series	–	Tactical Data Link Standardization Implementation Plan
Joint Requirements Oversight Council Memo (JROCM) 261-06	–	Cost Performance and Interdependency Chart Implementing Directive
CJCSI 3170.01series	–	Joint Capabilities Integration and Development System, 1 May 2007
The 16th Chairman's Guidance to the Joint Staff	–	1 October 2005
Joint Battle Management Command and Control Roadmap Ver. 2.0	–	20 January 2006

DEPARTMENT OF DEFENSE

Department of Defense Architecture Framework (DODAF) Version 2.0	–	Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
Department of Defense Document (DODD) 4630.05 series		
Department Of Defense Instruction (DODI) 4630.08 series	–	Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
DOD Information Enterprise Architecture (IEA), Version 1.2	–	
Global Information Grid (GIG) Technical Guidance (GTG)	–	GIG Joint Tactical Edge Service Guidance
DISA Key Interface Profile (KIP) 4, Joint Task Force (JTF) Components to JTF Headquarters, 31 March 2005	–	(In transition to an equivalent GIG Technical Profile (GTP)

(Copies of specifications, standards, handbooks, drawings, publications, and other government documents required by contractors in connection with specific acquisition functions should be obtained from the contracting activity or as directed by the contracting officer.)

2.3. Non-Government Publications. The following document applies to the extent specified in this document. Unless otherwise specified, documents which are DOD adopted are those listed in the latest issue of the DODISS cited in the solicitation. Documents not listed in the DODISS are the issues of the documents cited in the solicitation.

2.4. Order of Precedence. In the event of a conflict between the text of this standard and the references cited, the conflict should be referred to the military service specialists who are subject matter experts in the implementation of tactical data links. Nothing in this standard should supersede applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1. Acronyms.

The following acronyms are used in this handbook.

ACAT	Acquisition Category
ACDS	Advanced Combat Direction System
AFC2IC	Air Force Command and Control Integration Center
AMRDEC	Aviation and Missile Research, Development, and Engineering Center
AoA	Analysis of Alternatives
APIS	Actual Platform Implementation Specification
ASW	Anti-Submarine Warfare
BAMS	Broad Area Maritime Surveillance
BMD	Ballistic Missile Defense
C&L	Capabilities & Limitations
C2	Command and Control
CBA	Capabilities Based Assessment
CDD	Capability Development Document
CDLMS	Common Data Link Management System
CECOM	US Army Communications and Electronics Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CLIP	Common Link Integration Processing
CMF	Common Message Format
CNR	Combat Net Radio
COCOM	Combatant Commanders
COI	Community of Interest
CONE	Concepts of Network Employment
CPM	Capability Portfolio Management
CPD	Capabilities Production Document
C/S/A	Commands/Services/Agencies

CTP	Common Tactical Picture
CVN	Multi-Purpose Aircraft Carrier (Nuclear-Powered)
CYBERFOR	Navy Cyber Forces
DEM	Data Exchange Medium
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DODD	Department of Defense Document
DODI	Department of Defense Instruction
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
EIPT	Engineering Integrated Process Team
EMC	Electromagnetic Compatibility
eSMART	Enhanced iSMART
EW	Electronic Warfare
FORSCOM	Forces Command
GIG	Global Information Grid
GTG	GIG Technical Guidance
GTP	GIG Technical Profiles
HMI	Human Machine Interface
IA	Information Assurance or Interoperability Authority
I&S	Interoperability & Supportability
IAW	In Accordance With
IBS	Integrated Broadcast Service
ICD	Initial Capabilities Document
ID	Identity
IEA	Information Enterprise Architecture
IEP	Interoperability Enhancement Process
IER	Information Exchange Requirement
I-KPP	Interoperability-Key Performance Parameter

IO	Interoperability
IOA	Interoperability Assessment
IOC	Initial Operating Capability
IOE	Interoperability Evaluation
IOM	Interoperability Matrix
IPT	Integrated Process Team
iSMART	interoperable Systems Management and Requirements Transformation
ISP	Information Support Plans
IT	Information Technology
JBMC2	Joint Battle Management Command & Control (C2)
JC&L	Joint Capabilities & Limitations
JCAS	Joint Close Air Support
JCD	Joint Capability Documents
JCIDS	Joint Capabilities Integration and Development System
JDNO	Joint Data Network Officer
JICO	Joint Interface Control Officer
JID	Joint Interoperability Division
JIT	Joint Interoperability Testing
JITC	Joint Interoperability Test Command
JMT	Joint Mission Thread
JREAP	Joint Range Extension Application Protocol
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memo
JSF	Joint Strike Fighter
JSOW	Joint Standoff Weapon
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JTMP	Joint Tactical Data Enterprise Services Migration Plan
JU	JTIDS/MIDS Unit

KPP	Key Performance Parameters
MAJCOMs	Major Commands
MCTSSA	Marine Corps Tactical Systems Support Activity
MDA	Missile Defense Agency
MIDS	Multifunctional Information Distribution System
MIL-STD	Military Standard
MIP	Message Implementation Plan
MMA	Multi-Mission Maritime Aircraft
MMH	Multi-Mission Helicopter
MS	Milestone
NBC	Nuclear, Biological, Chemical
NCOE	Net-Centric Operational Environment
NCOW RM	Net-Centric Operations and Warfare Reference Model
NDD	National Difference Document
NDF	Network Design Facility
NEW	Network Enabled Weapon
NGC2P	Next Generation Command and Control Processor
NII	Network and Information Integration
NPG	Network Participation Group
NR-KPP	Net-Ready Key Performance Parameter
NSS	National Security System
OASD	Office of the Assistant Secretary of Defense
OPNAVINST	Office of the Chief of Naval Operations Instruction
OTHG	Over-The-Horizon Gold
OV	Operational View
PDA	Program Development Agency
PIDD	Platform Implementation Difference Document
PM	Program Manager

PO	Program Office
POC	Point of Contact
PPBE	Planning, Programming, Budget, and Execution
PPLI	Precise Participant Location and Identification
PRDD	Platform Requirements Difference Document
PRS	Platform Requirements Specification
PTUC	Participating Test Unit Coordinator
RFP	Request for Proposal
SA	Situational Awareness
SDD	Service Difference Document or System Development & Demonstration
SED	Software Engineering Directorate
SINCGARS	Single Channel Ground-Air Radio System
SLT	Service Level Testing
SME	Subject Matter Expert
SOP	Standard Operating Procedures
SPO	System Program Office
SRS	Service Requirements Specification
SSDS	Ship's Self Defense System
StdV	Standards View
SUT	System Under Test
SV	System View
TADIL	Tactical Digital Information Link
TDES	Tactical Data Enterprise Services
TDL	Tactical Data Link
TDL-T	Tactical Data Link Transformation
TN	Track Number
TR	Trouble Report
TTP	Tactics, Techniques and Procedures
UAS	Unmanned Air Systems

USA	United States Army
USAF	United States Air Force
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USN	United States Navy
VMF	Variable Message Format
WAN	Wide Area Network

4. INTRODUCTION

4.1. iSmart Background

4.1.1. .Joint combat operations are most effective when sensors, shooters and Command and Control (C2) units are fully network enabled with user-defined, accurate, timely, and secure information. Implementation and integration of networks operating at the tactical edge to fulfill information architectural requirements are a key component to executing joint operations.

4.1.2. Interoperability is the key to combat effectiveness, and it should be considered and evaluated throughout the life cycle of all systems that exchange digital information pertinent to the warfighter. The iSMART process provides a pragmatic approach to achieving effective interoperability in a cost-effective manner and provides the focus needed for the efficient use of resources: money, time, manpower, and facilities. Successful implementation of the iSMART process is the rapid, unambiguous transfer of tactical digital information to and between sensors, shooters, and C2 nodes to maximize warfighting capabilities.

4.1.3. To field the required level of capability at the tactical edge, the Services have recognized the need for a disciplined process to implement digital information-sharing networks. Implementation of an effective/common/joint engineering approach to Military Standard (MIL-STD) compliance results in:

a. Improved awareness and a greater level of detail of platform performance during the capability definition process.

b. Mitigated ambiguities and a greater understanding between Service program managers and system developers.

c. Unambiguous definition of requirements that system developers can satisfy.

d. Clarity and efficiency in certification and testing of net-enabled systems.

e. Joint Mission Area assessments conducted at an improved level of detail required to deliver combat capability.

f. Improved Service-validated implementation detail used to support the objective Joint Capabilities and Limitations (JC&L).

4.1.4. The iSMART Military Handbook is a collaborative effort between the Tactical Data Enterprise Services (TDES) Community of Interest (COI), Services, Agencies and the Joint Staff to promote the development of interoperable systems at the tactical edge of the Global Information Grid (GIG) and facilitate transformation to a net-centric operating environment.

4.1.5. This Handbook provides guidance to address Link 16 documentation and interoperability assessments using the iSMART process and tools. iSMART tools are being developed for use by other TDES information exchange systems.

4.1.6. The iSMART Handbook supports the following Joint Battle Management Command & Control (JBMC2) Roadmap capability objectives:

a. "Focus on Combatant Commanders/Services/Agencies (C/S/As) interoperability at the operational and tactical levels, under the direction of the Secretary of Defense, and ensure linkages to national/strategic levels."

b. "Ensure that current essential JBMC2 capabilities are integrated and interoperable to support key mission areas (e.g. Missile Defense, Joint Fires)."

4.1.7. The iSMART Handbook supports the following priorities of the Chairman of the Joint Chiefs of Staff (CJCS):

a. "Accelerate Transformation"

1. Transformation is a continual process, not an end state.

2. Transformation is as much a mindset and a culture as it is a technology or platform.

3. Transformation is a willingness to embrace innovation and accept analyzed risk."

b. "Strengthen Joint Warfighting"

1. Focus on transitioning from an interoperable to an interdependent force.

2. Individual Service perspectives brought together jointly foster better solutions."

4.1.8. The iSMART process can support Capability Portfolio Management (CPM) objectives by facilitating technical information sharing, collaboration and interoperability assessments by Service and Joint system engineers at key milestones of a platform's life cycle.

4.2. Department of Defense (DOD) Decision Support Process and iSMART

4.2.1. The Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System and the Planning, Programming, Budgeting, and Execution (PPBE) process are the principal DOD decision support processes for transforming the military forces to support the national military strategy, defense strategy, and Combatant Commanders' (COCOMs) warfighting requirements. Interoperability is of primary importance in these processes.

Simultaneous migration of emerging capabilities to the Net-Centric Operational Environment (NCOE) makes interoperability a continuing challenge. To identify required levels of interoperability, earlier versions of Chairman, Joint Chiefs of Staff Instructions (CJCSI) 6212.01

called out the Interoperability-Key Performance Parameter (I-KPP), which was subsequently replaced by the Net Ready-KPP (NR-KPP) to improve interoperability. These efforts proved insufficient to identify the level of detail needed to guide programmatics to achieve interoperability of tactical digital information-sharing systems. Implementing iSMART fills this gap.

4.2.2. CJCSI 6212.01series requires Tactical Data Link (TDL) platform implementation details at the bit-level prior to Milestone C, and encourages capability developers to leverage the iSMART process, the iSMART toolset, and the Joint Capabilities and Limitations (JC&L) document to develop these implementation details and improve tactical data and sensor interoperability.

4.2.3. The Joint Requirements Oversight Council (JROC)-approved Tactical Data Link Transformation (TDL-T) Capability Development Document (CDD), 22 January 2004, identified iSMART as one of five core components of the transformation. The iSMART toolset is defined as "the tools to support the process to identify and define TDL capabilities."

4.2.4. The relationship of the iSMART process to the program life cycle is described in Paragraph 6.1.

4.3. Related iSMART Activities

4.3.1. The Office of the Assistant Secretary of Defense (OASD) Network and Information Integration (NII) policy document, the Joint TDES Migration Plan (JTMP), introduces the Interoperability Enhancement Process (IEP), which was initiated to improve Joint war fighting capabilities. The IEP is a path to meet the joint requirement of common bit-level documentation that is needed to conduct joint mission area assessment and facilitate implementation of JC&L. The iSMART partners endorse the IEP concept and its objective to conduct joint mission area assessments.

4.3.2. The JBMC2 Joint Close Air Support (JCAS) Joint Mission Thread (JMT) Engineering Integrated Process Team (EIPT) recommended the iSMART process for implementation throughout DOD. The Joint Staff advocates policy and funding directives to support iSMART implementation to improve joint mission area effectiveness.

4.3.3. iSMART is equally relevant to all tactical data link Data Exchange Medium (DEM). This can benefit users of the TDES that is comprised of: Link 16, Link 11, Variable Message Format (VMF), Link 22, Integrated Broadcast Service (IBS), and Joint Range Extension Application Protocol (JREAP). iSMART tools are also being developed for possible use to assist in documentation of other MIL-STDs including MIL-STD 188-220 and MIL-STD 2045-47001.

4.3.4. The term "TDL" means Tactical Data Link, but is also used generically in this Handbook to describe any tactical data link information-exchange medium.

4.4. Definition and Benefits

4.4.1. iSMART is a disciplined process supported by a database and a toolset. The process captures the full extent of information processing by a system, allows analysis of the information flow between systems, and manages information exchange requirements throughout the life cycle of a system.

4.4.1.1. iSMART benefits

a. A method for translating high-level interoperability requirements into specific data exchange requirements.

b. A means to document deviations from the standard (both intentional and unintentional).

c. A feedback mechanism to document deficiencies identified by assessments and testing.

d. The means to promulgate interoperability reports to warfighters, with which they can make appropriate decisions.

4.4.2. iSMART assists program developers in correctly implementing data links on a platform and provides the end-user with information about the platform so that the platform may be used to maximum advantage. All stakeholders will benefit from the iSMART process.

4.5. Program Offices/Program Managers/Program Development Agencies (POs/PMs/PDAs)

These will benefit by reviewing the documents of platforms that have implemented iSMART and using those documents to assist in making their own implementation decisions. The availability of these documents, as well as a platform's implementation, will significantly assist developers in achieving interoperability.

a. Acquisition planners – Will benefit by analyzing previous capability gaps and deviation information to make informed decisions about funding and priority of new capabilities and enhancements to existing capabilities.

b. Support agencies – Training and Doctrine Commands, Forces Command (FORSCOM) Joint Interoperability Division (JID) and Service Network Design Facilities (NDF) will benefit by reviewing platform capabilities and mission assignments to support leader education and TDL network design requirements. iSMART also supports Joint Interoperability Test Command (JITC) certification, testing, and interoperability assessment mission.

c. Tactical and system operators – Will benefit by joint mission area operational assessment of a system's ability to interoperate with other tactical systems. Using

the iSMART interoperability assessment capability, JC&L operational assessments and Tactics, Techniques and Procedures (TTP) can be developed to execute COCOM-defined kill chains. JC&L products are available through Service and Joint training and support commands.

d. 4.4.2.1 iSMART aids the development of key JCIDS documents such as the Initial Capabilities Document (ICD), the Capabilities Development Document (CDD) and the Capability Production Document (CPD) and supports development of the NR-KPP. The iSMART process not only simplifies the JCIDS process, but also improves integrity in the interoperability arena.

4.6. Purpose

4.6.1. This Handbook provides step-by-step instructions for using the iSMART process to develop a platform's TDL implementation that supports interoperability and the GIG. A platform is considered an air, land, surface or subsurface operational entity, system, technology or application in which one or more tactical data link is being implemented. All platforms that exchange information are required to have an NR-KPP, as mandated by the JCIDS process by CJCSI 6212.01.

4.6.2. The successful implementation of Link 16 (i.e., program achieves certification) is an objective requirement of the NR-KPP. Since it is impossible for the JCIDS documentation to specify requirements for every platform and TDL, platforms that have successfully implemented the iSMART process will be moving toward compliance with the NR-KPP. Paragraph 5 will demonstrate how iSMART complements and supports JCIDS requirements.

4.7. iSMART Handbook Approach

4.7.1. The iSMART Military Handbook is a comprehensive, collaborative approach with close participation from Service TDES Interoperability Authorities. The interoperability stakeholders and iSMART partners agree:

a. A common systems-engineering method initiated at the beginning of new system development, or during a fielded system's upgrade, significantly increases the probability of delivering systems that maximize contribution to joint capabilities.

b. Interoperability is one component of capability development. Tactical data link related/dependent sensors, weapons and C2 systems should only include the level of interoperability that has been properly validated.

c. Interoperability is a key tenet throughout a system's life cycle.

d. Implementation of iSMART will permit the Services to tailor the required and actual level of interoperability to facilitate the efficient use of funds.

e. Critical and unique Service processes should be identified and preserved as outlined in the Service appendices.

f. Platforms from all the Services are in various stages of executing the iSMART process.

g. The iSMART Military Handbook solidifies the Services' goals to field capabilities that support executing COCOM Joint Mission Threads.

4.7.2. This Handbook describes a recommended "best practices" approach. The Service appendices identify where deviations exist and where those take precedence.

5. THE iSMART Process

5.1. Background

5.1.1. The iSMART process provides a means

a. Describe data exchanges derived from high-level requirements.

b. Successfully integrate new systems into the operational GIG.

c. Identify data exchange deficiencies for resolution by acquisition authorities.

d. d. Identify and resolve interoperability issues from the earliest life cycle stages, thereby minimizing the costs associated with achieving interoperability.

e. Identify capability gaps of fielded systems.

f. Use resources effectively and efficiently.

5.1.2. The iSMART process is a systems-engineering approach to achieving effective interoperability in a cost-effective manner. iSMART provides the focus needed for the efficient use of resources, including money, time, manpower and facilities. The iSMART process, depicted in FIGURE 1, follows these steps:

a. The operational proponent and capabilities proponent, as the government lead, identifies the data exchanges necessary to satisfy the operational requirements of the platform. For example, if one of the operational requirements is to perform Time Sensitive Strike, the exchange of imagery might be a necessary information exchange.

b. The PO/PM/PDA identifies the Data Exchange Medium (DEM) (i.e. Link 16, VMF, IBS, etc.) capable of supporting the required information exchanges. The preferred DEM for the exchange is identified with supporting rationale provided. Information exchange requirements that have no associated DEM are also identified as gaps.

c. The PO/PM/PDA identifies potential solutions for capability gaps. A capability gap is a particular information exchange that does not have a supporting DEM.

d. The corresponding JCIDS documents are developed in parallel with the iSMART process. This documentation is explained in detail in Paragraph 6.

e. The PO/PM/PDA establishes an Integrated Process Team (IPT) to develop the message exchange requirements for each identified DEM/capability set. The IPT should consist of the PO/PM/PDA, Program Developer and the TDES Interoperability Authorities. TDES Interoperability Authorities in this document are;

1. US Air Force Command and Control Integration Center (AFC2IC)

2. U. S. Navy SPAWAR Systems Center, Pacific (SSC PAC), Code 591

3. US Army CIO G6 (SAIS AOJ)

4. US Marine Corps Tactical Systems Support Activity (MCTSSA)

5. Missile Defense Agency (MDA-BC).

Contact information is in the Service/Agency appendices.

5.1.3. The IPT should be responsible for:

a. Developing the high-level message implementation requirements for the platform to include message, word and action value/message use implementation.

b. Obtaining approval from higher authority to proceed with the planned implementation.

c. From the high-level message implementation requirements, developing the precise protocol and bit-level implementation requirements for the platform.

d. Obtaining final Service approval of the platform requirements from higher authority.

e. Populating the Information Exchange Requirements (IER), and the Interoperability Matrix (IOM).

f. Developing platform host software requirements in accordance with the Platform Requirements Specification (PRS). The program developer is tasked with developing the host computer program in which the data link protocols are implemented in accordance with the Service approved PRS. The program developer draws on the experience of the IPT members to resolve problems that are encountered.

g. Deviations from the baseline standard are documented and catalogued in the Platform Requirements Difference Document (PRDD). The PRDD defines the required deviations from the platform's baseline standard. A deviation is any difference from the requirements of the baseline standard.

h. Obtaining the Service interoperability certification.

i. After the platform host software is implemented and tested, the Actual Platform Implementation Specification (APIS) is created. The APIS documents the fielded or actual implementation data of that platform.

j. All fielded or actual deviations from the baseline standard after the platform implementation has been tested are documented in the Platform Implementation Difference Document (PIDD).

k. Obtaining joint interoperability certification.

l. Obtaining feedback during life-cycle process.

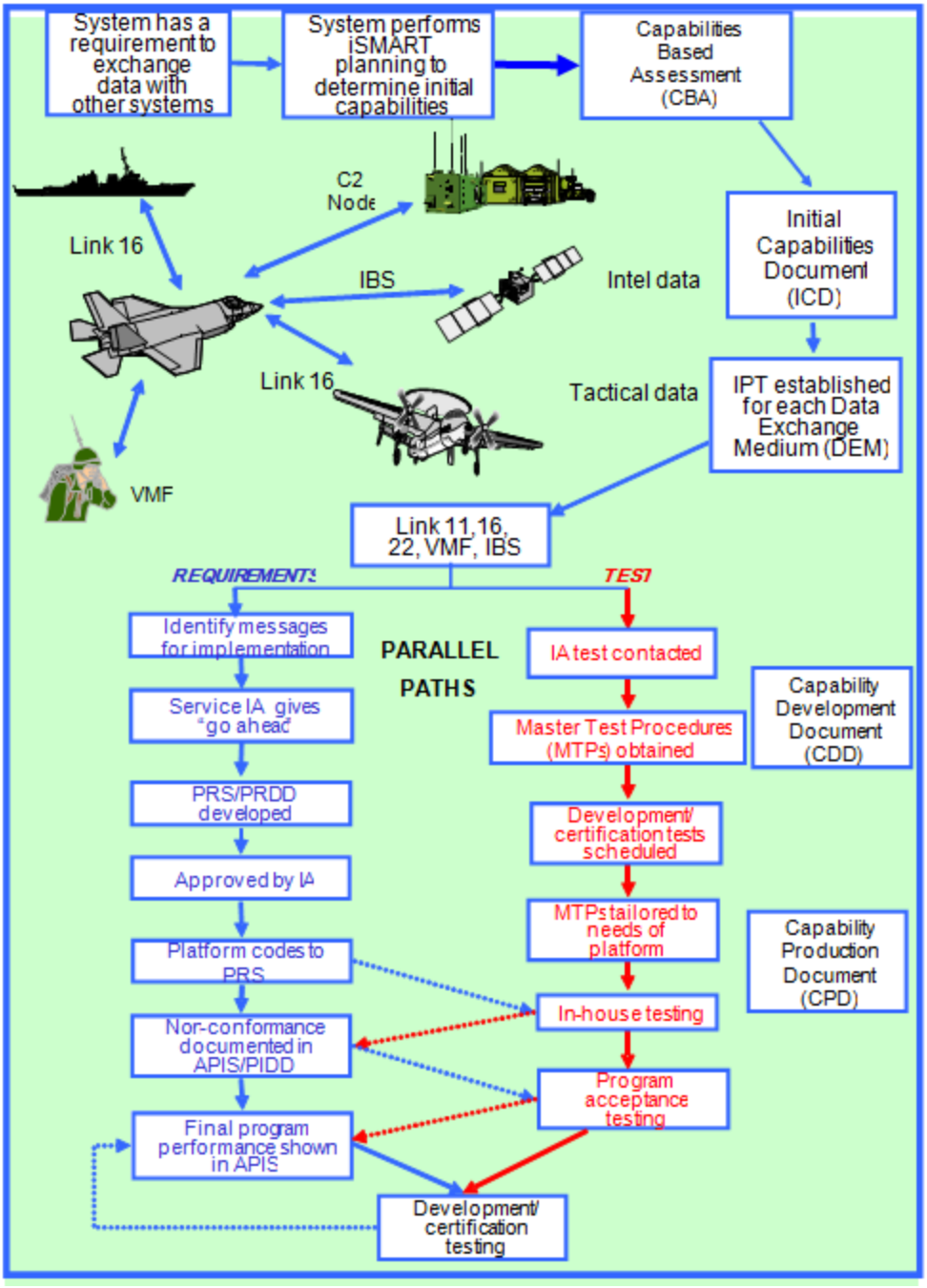

FIGURE 1. Testing and JCIDS Process

5.2. Composition of the IPT

5.2.1. The IPT composed of the PO/PM/PDA determines which messages and protocols will be implemented to support the Information Exchange Requirements (IERs). The IPT is made up of representatives from the PO/PM/PDA, Program Developer, TDES Interoperability Authority and the user community. The participant roles are summarized in TABLE I.

5.2.2. The IPT will assist the PO/PM/PDA in developing:

a. Message implementation that meets the platform's information exchange requirements.

b. Functionality to the user (i.e., operational employment perspectives and Human Machine Interface (HMI) issues).

c. Interoperability certification plans.

5.2.3. Any platform that attempts to enter a network has functionality that must be implemented, regardless of whether that functionality satisfies a platform data exchange requirement. For example, implementation of a capability on Link 16, such as a surveillance function, may require that other capabilities be implemented, such as Identity (ID) Difference Resolution, in order to comply with the interoperability core requirements of the MIL-STD-6016 Link 16 Message Standard.

TABLE I. IPT Participant Roles

Participant	Role
Program Office/Program Manager/ Program Development Agency	Develop ICD for platform. Task the program developer. Adjudicate implementation disagreements within the IPT.
Program Developer	Develop platform hardware/software that meets mission needs and is interoperable. Generate PRS/PRDD/PIDD/APIS/bit-level implementation (platform iSMART documents).
TDES Interoperability Authority	Identify message implementation that meets mission requirements. Identify interoperability issues. Interpret message standard.
User Community	Provides operational perspective on implementation of requirements for platforms operating within the tactical edge networks.

5.2.4. The TDES Interoperability Authority will:

a. Identify that the platform implementation is in accordance with the message standard.

b. Advise when failure to implement a requirement, or incorrect implementation, may adversely impact the probability of platform interoperability certification and/or interoperability within the GIG.

c. Provide interpretation of the standard.

d. Provide advice for mitigating any adverse impact when a compromise is agreed upon by all stakeholders .

e. Assist Program Office/Program Managers by maintaining components of the NR-KPP that are generic to the tactical networks that they have messaging oversight for. This includes application of the DOD Information Enterprise Architecture (IEA), Integrated Architecture Products. Key Interface Profiles (KIPs), and Information Assurance (IA) requirements that are the backbone of successful interoperability assessments.

f. Provide iSMART training as needed to the Service PO//PM/PDA and Program Developers.

5.2.5. The TDES Interoperability Authority to the IPT provides Subject Matter Expert (SME) advice based on:

a. Existing requirements for similar platforms.

b. Requirements of the message standard.

c. Understanding of the platform's capabilities and limitations.

5.3. IPT Decision Making Process

5.3.1. The IPT assists the PO/PM/PDA in determining which Tactical Data Links should be implemented on a platform's particular tactical data link system. The PO/PM/PDA, supported by the IPT, will provide the TDES Interoperability Authority recommended implementation plans for approval. Factors supporting implementation decisions made by the IPT include:

a. Platform missions - The mission areas of the platform are the primary capabilities on what messages and protocols the platform will implement.

b. Platform manning - While much of the functionality of the data link is automated, some actions must be performed by the operator. If the platform is required to implement a capability, but is not manned to provide the required operator interactions, then the platform may have to implement the capability some other way, or not at all.

c. Platform hardware capabilities - Platforms may be limited by the capabilities of their sensors, radios, and other equipment. For example, a platform's Electronic Warfare (EW) sensor suite may not be able to provide bearing accuracy, or detect the presence of jitter. These limitations should be documented in the PRS/PRDD.

d. Schedule - If the platform is using an incremental development process, the IPT should ensure that the functionality implemented in each increment continues to be interoperable with other net-enabled platforms through Interoperability Evaluation (IOE) comparisons and documenting those results in an Interoperability Assessment (IOA).

5.4. Identifying Messages for Implementation

5.4.1. The workflow that best supports the IPT process should be flexible due to the wide range of factors that may influence the decision-making process.

5.4.2. The IPT identifies messages that are required to be implemented to satisfy the platform's IERs, primary missions, and comply with appropriate standards. The Services may establish unique methods for doing this, as described in the Service appendices (A-D).

5.4.3. Once the basic MIP for the platform is determined, it is submitted to the TDES Interoperability Authority for review and approval. This review will verify that the platform is taking the correct approach for its implementation. The Service TDES Interoperability Authority will approve the implementation or recommend changes to satisfy interoperability requirements.

5.4.4. When a platform's message implementation is approved, the TDES Interoperability Authority will formally recommend that the platform continue with development. The recommendation should describe any perceived discrepancies and operational impacts. The TDES Interoperability Authority will post the platform's approved message implementation on the Joint iSMART web site. The Joint Staff and the other Service TDES Interoperability Authorities will be notified of the approval and posting.

5.5. Incremental Development Plans

5.5.1. Many POs/PMs/PDAs take an incremental development approach to fielding a platform. In this approach, a platform is initially fielded with a desired capability identified, an end-state requirement is known and the requirements are met over time through the development of several increments (blocks, versions, etc), each dependent on available mature technology. The IPT should ensure that each increment of the platform contains the functionality that supports the operational capability being fielded and that it is interoperable with other units.

5.6. PRS and PRDD Development

5.6.1. The primary function of the IPT is to develop the PRS and the PRDD using the approved Message Implementation Plan (MIP) (bit-level information). The PRS provides the exact message standard implementation requirements for the platform. The PRDD lists all the

deviations from the message standard, along with a rationale for each. The PRS also includes the MIP requirements for the platform. The iSMART process can apply to any Data Exchange Medium (DEM), the following paragraphs will refer specifically to Link 16 documents for ease of understanding.

5.6.2. FIGURE 2 is an example PRS/PRDD that shows a part of MIL-STD-6016 that will not be implemented by a system, along with the Interoperability Assessment (IOA).

C.0 INTRODUCTION

C.0.1 GENERAL

C.0.1.1 J2.x Precise Participant Location and Identification (PPLI) messages are transmitted by all Joint Tactical Information Distribution System (JTIDS)/MIDS Units (JUs) in a network, on one or more of the PPLI and Status Network Participation Groups (NPGs). The terminal generates the messages and received messages are used within the terminal for synchronization and relative navigation. The message also conveys network participation status, positional, identification and operational information on the transmitting JTIDS/MIDS Unit (JU), which is used to support other link functions.

C.0.1.2 Not Used.

Deviation Index	1	Interoperability (IO) Impact	None
Rationale		SOP Requirement	None
Platform does not have an operational requirement for the capability (platform is not a data forwarder).			

C.0.1.3 J13.x Platform and System Status messages are transmitted by all JUs in a network. The messages are generated by the host system. J13.x Platform and System Status messages are used by command authorities, weapons controllers, and the other members of a non-C2 JU's flight to support weapons coordination and management.

FIGURE 2. Sample PRDD/PRS in Word Format.

5.6.3. To develop the PRS/PRDD, the IPT should establish a review schedule for the sections and appendices of the latest version of MIL-STD-6016 with any changes as of the date the systems documents are developed. This order will vary depending on the platform capabilities and Service priorities. Service appendices to this Handbook may document a specific order for reviewing.

One example for reviewing MIL-STD-6016 is shown in

TABLE II. Within each priority level, sections are listed in alphanumeric order; no sub-priority is implied. Numerals shown in parentheses indicate review items that are not applicable to all platforms. For example, review of MIL-STD-6016 Section 4.17 is only required if the platform implements ballistic missile surveillance.

TABLE II. MIL-STD-6016 Review Order.

Priority	Section	Importance
1	3.1, 3.2, 3.5	Provides IPT members with background for Link 16 and answers to potential questions.
1	4.2, 4.3	Platforms must be aware early on of the data registration and Track Number (TN) management requirements.
1	App C	Transmitting and receiving PPLI messages is required before any other function can be implemented.
2	4.7, 4.8, 4.11, 4.15, App D	It is assumed that the platform will be reporting some type of surveillance entity. All platforms will receive surveillance entities. Special consideration must be paid to what Point Type/Point Amps will be implemented in the J3.0.
2	4.4, 4.5, 4.14, App P, App U	Any platform that performs surveillance is required to perform the necessary track management and correlation functions.
(2)	4.17	This is required for systems implementing ballistic missile surveillance.
2	Section 5-4	Transmit Tables

TABLE II. MIL-STD-6016 Review Order – Continued.

2	Section 5-5	Receive Tables
3	App E	Any platform that transmits surveillance entities is also required to implement the J7.1.
3	App K	All platforms will implement some aspects of App K. At a minimum, all platforms shall receive the J10.2.
(3)	App L, App M	Controlling and controlled units will implement much of L and M. However, it is possible for a platform to be neither a controlled nor a controlling unit.
3	App V	Network Management - the terminal automatically provides most of the functionality.
4	App G	At a minimum, platforms should receive the J3.7 for situational awareness. Additional EW requirements are platform-dependent.
(4)	App I	This is applicable to platforms capable of intercepting ballistic missiles.
(4)	App O	This is applicable to platforms with Anti-Submarine Warfare (ASW) sensors.
4	App F, App H, App N, App T	This is applicable to supporting messages, some of which are required, but which are less critical than messages in other appendices.
5	App Q, App R, App S	Supporting messages - review as required.
5	App J	Voice – Most of the functionally is automatically provided with the terminal.
5	App Z	National/Service Proprietary Annexes - review as required.

5.6.4. Generally, the program developer is tasked with developing drafts of each section/appendix; including the relevant transmit/receive tables, which are then presented to the IPT for review. Developing only a few documents at a time is recommended, so that lessons learned can be incorporated into succeeding documents.

5.6.5. The PRS provides the exact protocol implementation requirements for the platform. All parts of the message standard that do not apply to that platform will annotated as "Not Used", all special requirements will be added and all tailored requirements will be modified. However, the development of the PRS is more complicated than simply annotating the message standard. Because the PRS is a historical document, every decision made with respect to a non-implementation or modification of a requirement should be documented. This supports future program development, testing, and interoperability planning for other platforms. Decisions are documented in the PRDD.

5.6.6. The PRDD specifies deviations from a requirement of the MIL-STD and provides explanatory information. The PRDD is a collection of forms, similar to Trouble Reports (TRs), documenting every instance that the platform deviates from the joint requirements of the MIL-STD. Most deviations are allowable and correct, e.g., for a Link 16 implementation, numerous paragraphs of MIL-STD-6016 can be deleted based on whether the platform is a C2 unit or Non-C2.

5.6.7. The Service appendices will provide specific instruction for developing the PRS and PRDD.

5.6.8. When comments are reviewed at the IPT meeting, the PO/PM/PDA is responsible for adjudicating conflicts that are not resolved through consensus; however, failure to follow TDES Interoperability Authority recommendations could result in a platform unable to pass certification.

5.6.9. Regardless of the process used to develop the deviation descriptions for the platform, each deviation should include the information listed below:

a. The MIL-STD-6016 paragraph to which the deviation applies.

b. The instructions for incorporating the deviation (add, delete or modify).

c. The text of the deviation (if required).

d. The rationale for the deviation.

e. The interoperability impact of the deviation.

f. Whether or not changes to Concepts of Operations (CONOPS), Standard Operating Procedures (SOP) or TTPs are required.

5.6.10. The rationale for the deviation explains why the paragraph was added, deleted or modified. Rationales should be standardized as much as possible to facilitate cross-platform comparisons. TABLE III presents a list of common rationales and the circumstances under which they might be used. Platforms should only create a unique rationale as a last resort. Platforms may always add explanatory text following the main rationale.

TABLE III. Standard PRDD Rationales.

Rationale	***Cases Where Used***
Platform is a C2 unit and requirement is for a non-C2 unit.	Self-explanatory.
Platform is a non-C2 unit and requirement is for a C2 unit.	Self-explanatory.
Platform does not perform ballistic missile defense.	Used for platforms that cannot track ballistic missiles and are not required to implement functionality related to tracking and engaging ballistic missiles.
Platform does not have underwater sensors.	Used primarily for airborne or land C2 Link 16 unit that does not have ASW sensors and is not required to transmit the J3.4 message or implement the J5.4 message.
Platform equipment does not support this capability.	Used for non-implementation of requirements that are part of an implemented functional area, but which cannot be supported because the platform does not have the appropriate equipment.
Platform does not have an operational requirement for the capability.	Used when a functional area is not implemented, such as Image Exchange, because the platform does not have an operational requirement for the function.
Platform equipment cannot provide the data to support this capability.	Used in transmit tables when a platform implements a word for transmission, but is unable to transmit a field or data item because onboard equipment does not support it. For example, an EW sensor that does not detect jitter.
Platform equipment is not integrated with the data link.	Used in the transmit tables for the J13.x messages when a platform has a piece of equipment but is unable to report the status because the equipment is not integrated with the host system.

TABLE III. Standard PRDD Rationales – Continued.

Platform cannot control other JUs.	Used for C2 JUs that do not have an operational requirement to control other JUs via the control NPG.
Platform cannot command other JUs.	Used for C2 JUs that do not have an operational requirement to command other C2 JUs.
Platform has no weapons or only self-defense weapons.	Used for C2 JUs that do not have tactical weapons, e.g., weapons for which the status is reported on the data link.
Platform does not perform inter-flight air control.	Used for non-C2 JUs that do not have an operational requirement to control other non-C2 JUs on Network Participation Group (NPG 9).
Not applicable to own unit environment.	Used primarily in Appendix C when deleting requirements for JUs of other environments.
Platform unable to meet requirement, with acceptable work around.	Used for deviations when the platform does not implement the exact requirement, but does provide functionality that adequately meets the intent of the requirement. Note that platforms may still receive a Trouble Report (TR). Work-arounds must be approved by the TDES Interoperability Authority.
Platform unable to meet requirement, dispensation granted.	Used when a platform fails to meet a requirement, but because of extenuating circumstances, the platform has been relieved of the requirement. Exemption may only be granted by the TDES Interoperability Authority. Platforms may receive a TR.
Platform unable to meet requirement, no work around.	Used for a deviation where the platform fails to meet a requirement for unspecified reasons. This kind of deviation will merit a TR.
Additional capability unique to platform.	Used when adding additional text to the PRS to document a capability of the platform not covered by the MIL-STD.
Editorial.	Used when an error has been found in the MIL-STD and corrected in the PRS. This can also be used when personalizing the platform's PRS, e.g., changing "a C2 unit shall" to "JSF shall."

5.6.11. There is no rationale that states "platform unable to implement because of time/budget constraints." The platform has a requirement to implement a capability regardless whether it has the budget to do so. In these cases, the requirement stays in the PRS, but would be modified or deleted in the APIS and the deviation would be included in the PIDD with a rationale explaining the time/budget constraint.

5.6.12. The interoperability impact of the deviation is determined by the IPT, and represents the best estimate of the effect of the deviation on interoperability with other platforms. The interoperability impact may be updated at any time during or after the program's development based on a number of factors. For example, following posting to the Joint iSMART web site and initial joint mission area interoperability assessments, additional entries that are coordinated with the joint community may be posted by the TDES Interoperability Authority.

5.7. Special Cases

5.7.1. MIL-STD-6016 appendices all contain a Section 0. Section 0 contains introductory and descriptive information regarding the subject of the appendix. Many appendices also use Section 0 to document rules and protocols that do not fit easily into a transactional format (as used in Section 1 and greater in the appendices). Therefore, when developing a PRS, Section 0 of an appendix may not be for information only. Each Section 0 should be individually evaluated.

5.7.2. When a paragraph is informational only, it is recommended that it be retained in the platform PRS. If the paragraph provides information on a function that is not implemented by the platform, it is recommended that it be deleted from the platform PRS.

5.8. Developing the Actual Platform Implementation Specification/Platform Implementation Difference Document APIS/PIDD

5.8.1. The approved PRS defines the baseline requirements of a platform and does not change. The PRDD format is used to explain the differences between the MIL-STD and the PRS. The APIS defines the program's actual performance, and the PIDD format is used to explain the differences between the baseline standard and the APIS. The APIS can change often, as problems are discovered and fixed.

For example, after the baseline requirements of a platform have been implemented and tested, it is discovered that the platform did not correctly implement required track correlation protocols; the information is removed from the APIS by filling out a PIDD form. The PRS is the required implementation document, whereas the APIS is the actual implementation document. The PRS will be documented as a new baseline when capabilities, mission areas or incremental improvements are implemented by the platform/link. The APIS is more dynamic and is changed as implementation errors or inconsistencies are found and/or corrected.

5.8.2. The procedures for completing PIDD forms and developing the APIS are similar to completing a PRDD form for the PRS.

5.8.3. Initial PRDD entries are transitioned to the PIDD document.

5.8.4. The rationales used in creating a new PIDD forms are standardized. New PIDD forms may have different rationales from the standardized PRDD rationales. TABLE IV shows acceptable PIDD rationales and FIGURE 3 shows an example of a PIDD/APIS entry. Platforms should only create a unique rationale as a last resort. Platforms may always add explanatory text following the main rationale. Each PIDD deviation should include a priority for correction in following baselines.

TABLE IV. Standardized New PIDD Rationales.

Rationale	Cases Where Used
Requirement incorrectly implemented (discovered during _____ testing).	Used when a required protocol was incorrectly implemented in the program code. This is usually discovered during testing. The rationale should include the type of test. Generally, these will also be documented in trouble reports. If possible, the TR# should be referenced. The changed text of the PIDD entry should describe the program's actual behavior.
Program unable to implement requirement.	Used during development when the platform determines that it is unable to implement a requirement. This could be because of time, cost, unanticipated complexity or similar reasons.
Requirement determined to not apply to platform.	Used when it is determined that a requirement does not actually apply to the program. Such deviations should be approved by the TDES Interoperability Authority.

D.1.1.19 Periodically, for each local track, as follows:

a. 12 seconds for a real-time Air Track, real-time Surface Track, real-time Ballistic Missile Track with Lost Track Indicator = 0 (Tracking) and Subsurface Track (Identity = 6 (Hostile)).

b. 48 seconds for a non real-time Air Track, non real-time Surface, real-time Ballistic Missile Track with the Lost Track Indicator = 1 (Lost Track), non real-time Ballistic Missile Track, Land Track and Subsurface Track (Identity is other than 6 (Hostile)).

Deviation Index	1	Interoperability (IO) Impact	None
Rationale	TR 33	SOP Requirement	None
Requirement incorrectly implemented (discovered) during Service Certification (Oct 2011) Testing.			

D.1.1.2 C^2 Track Transmission Preparation Constraints

FIGURE 3. Sample PIDD/APIS in Word Format.

5.9. Preparing the Actual Implementation

5.9.1. The platform will provide the required and the actual bit-level implementation. Following the IPT process, the required bit-level implementation should be presented, along with the PRS/PRDD, to the Service Interoperability Authority. The actual bit-level implementation contained in the APIS shows the deviations from the required implementation plan detailed in the PRS/PRDD and implementation differences documented in the PIDD. This bit-level implementation should be provided after the platform's program has been implemented and tested, but before it is submitted for Joint certification testing. The procedures governing the development of the required implementation are the same as that of the actual implementation.

5.10. TDES Interoperability Authority Review and Approval

5.10.1. The final PRS and data item implementation are presented to the TDES Interoperability Authority for formal approval. TDES Interoperability Authority approval is required before the platform can submit a request for Service and Joint interoperability certification testing. The TDES Interoperability Authority's primary approval or disapproval criteria is based on whether the platform implementation meets its stated operational requirements and meets the standards of interoperability dictated by the appropriate TDL MIL-STD or other governing documents.

5.10.2. Upon approval of the PRS, the TDES Interoperability Authority will formally approve the deviations documented in the PRDD. Platforms will have a PRDD that contains

deviations that are approved by the Service (see Appendices A-D) TDES Interoperability Authority. By approving a platform's PRS/PRDD that includes deviations against Service requirements, the TDES Interoperability Authority has confirmed that the platform satisfactorily meets its operational and interoperability requirements, despite the required deviations. FIGURE 4 illustrates platform tracking through the iSMART process.

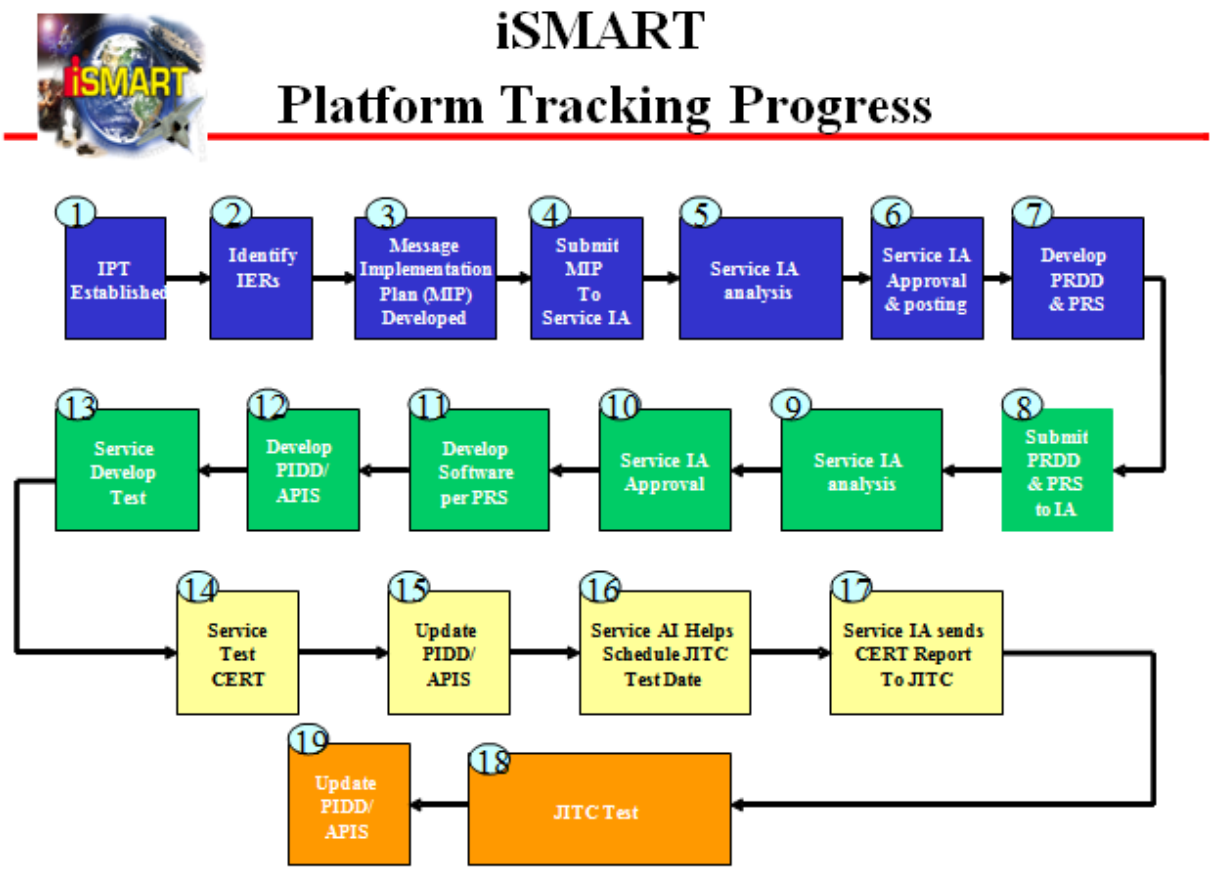

FIGURE 4. iSMART Platform Tracking.

5.11. Life Cycle iSMART Support

5.11.1. When a new software discrepancy is discovered through testing or operational feedback, the APIS would be updated to remove the requirement from the platform implementation specification. The removed requirement would be documented in the PIDD. When the requirement discrepancy has been corrected, it would be removed from the PIDD and the requirement would be documented in the APIS. APIS/PIDD updates for each fielded baseline should be published and updated as required by the Services.

5.11.2. When the message standard changes, it affects all the iSMART documentation. The platform requirements should be analyzed with every new, changed or deleted requirement to determine if the platform is affected. No changes are made to the platform's baseline PRS as it represents the approved requirements for the platform when it was developed.

An exception can be made if the PRS itself is still in development; in this case, the PO/PM/PDA and the developer, advised by the TDES Interoperability Authority, should determine which new requirements should be entered into the PRS baseline. When the PRS has been finalized, new requirements cannot be retroactively added to the platform's requirement specification.

5.12. Software Development

5.12.1. The PRS is the approved TDL implementation requirements for the platform that the program developer uses to develop the software.

During software development, it may be discovered that certain PRS requirements cannot be met. In this case, the deviation from the requirements is noted in the PIDD. The PIDD is a collection of all required and non-required deviation descriptions from the baseline standard that are fielded/actually implemented, similar to the PRDD.

The deviations may be the result of a number of factors, but generally, deviations are the result of a failure to meet a requirement in the PRS. When program development is complete, an APIS is developed to maintain a platform's actual software performance, rather than the requirements shown in the PRS. Programs may develop interim documentation during the course of development, but the final APIS and actual bit-level implementation data will be used for interoperability comparisons later in the iSMART process.

5.12.2. Any in-house testing and software changes the program developer performs prior to delivery to the program office are documented in the APIS, PIDD and actual bit-level implementation data. In-house testing may include testing of capabilities that are currently outside the scope of Service data link certification testing (example; such as Wide Area Network (WAN) or Information Assurance (IA) testing)).

The PIDD and the APIS provides a tool for the PO/PM to evaluate contract performance. A system's actual bit-level implementation data is used by external users when conducting system to system IOE comparisons. These results are documented in an IOA in which Services may utilize to improve future system development or incremental builds. Results of in-house testing should be provided to TDES Interoperability Authority and Joint-level certification authorities, to support a system's certification testing. For any requirement identified in the PRS/PRDD and MIP, a corresponding APIS /PIDD and actual bit-level implementation data is created.

5.12.3. The APIS and PIDD are living documents, that are constantly being updated through its life cycle to facilitate iSMART analyses that support own unit and all other units. When a deficiency is identified it is removed from the APIS and documented in the PIDD. When a deficiency has been corrected it is removed from the PIDD and documented in the APIS. The various events that trigger a document update and the resulting action are depicted in FIGURE 5.

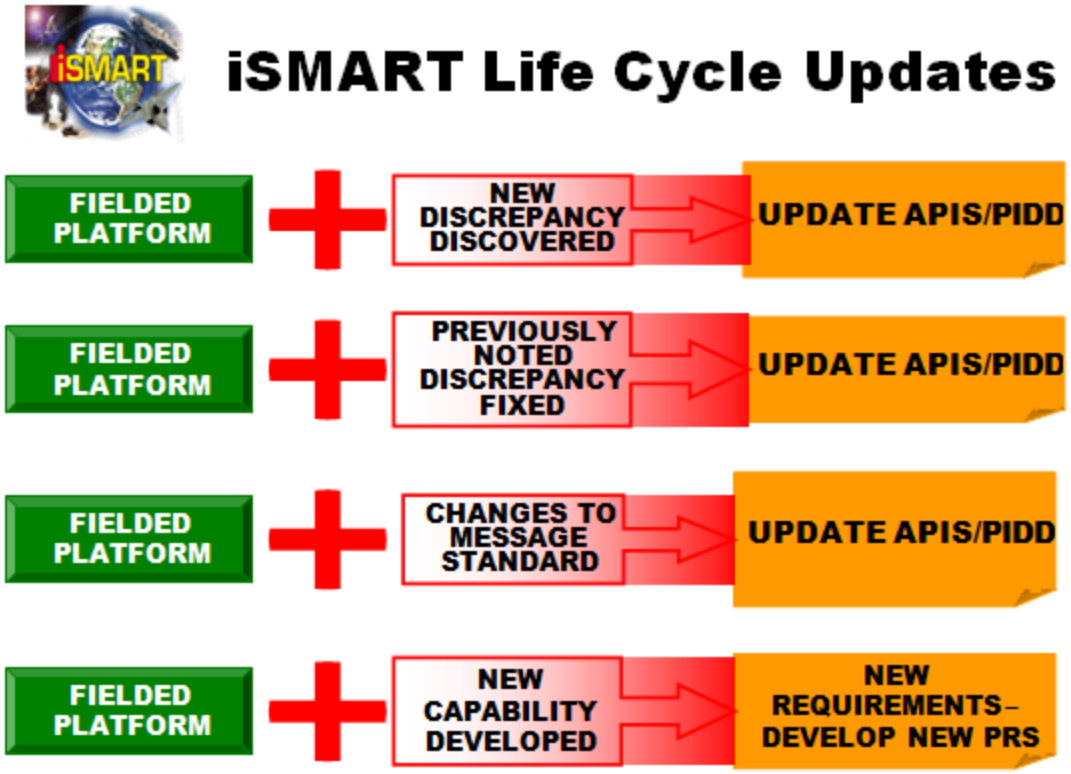

FIGURE 5. iSMART Life Cycle Updates.

5.13. iSMART Terms and Products

5.13.1. FIGURE 6 and TABLE V are provided as a summary of the terms and products that have been discussed. It provides a sequential, building block approach of how these products are developed and how they interact with each other.

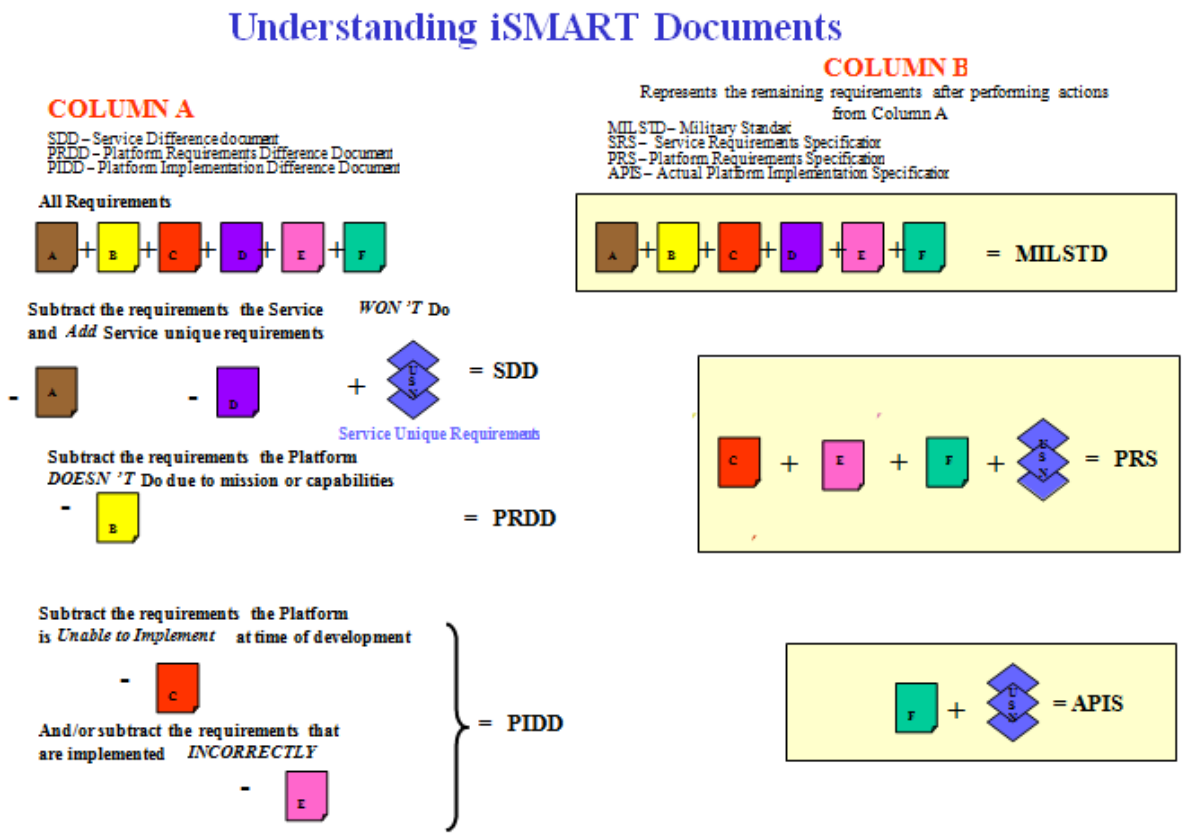

FIGURE 6. iSMART Documents.

TABLE V. iSMART Terms and Products.

TERMINOLOGY	*DEFINITION/PRODUCT*
Military Standard (MIL-STD)	Contains the complete interoperability specification.
National Difference Document (NDD)	Contains the deviations approved by national authorities (i.e. Multi-TDL CCB) for all systems from that country. The US has not implemented a Link 16 NDD, currently using MIL-STD 6016 as the baseline.
Service Difference Document (SDD)	Contains the deviations submitted by the Services' and approved by the Multi-TDL CCB. Maintained by TDES Interoperability Authority.

TABLE V. iSMART Terms and Products - Continued.

Platform Requirements Specification (PRS)	A platform specific version of the MIL-STD requirements and a complete definition of the platform data (DFI, DUI, and DI) exchange requirements.
Platform Requirements Difference Document (PRDD)	Defines the differences between the MIL-STD and those required of the specific platform. The PRDD includes a complete definition of the platform data (DFI, DUI, and DI) exchange requirements.
Actual Program Implementation Specification (APIS)	A platform specific version of the platform's implementation. (i.e. PRS as modified by the PIDD) and a complete definition of the platform's data exchange. Also includes the actual bit-level implementation data derived from the MIP. .
Platform Implementation Difference Document (PIDD)	Defines the differences between the platform specific requirements (PRS) and those implemented by the platform.

5.13.2. Terms.

a. Specification. This is the requirement that should be met and is the objective end state. A specification is often included in a contractual document as a Service Requirements Specification (SRS) or Platform Requirements Specification (PRS). It is also called "the Standard" and may be used synonymously with the applicable MIL-STD.

b. Differences. Recognizing that technical requirements cannot always be met, they are documented in Difference Documents. Differences can be intended deviations such as Service or National Difference Documents, or unintended deviations that are discovered during developmental activities.

   1. National Difference Documents (NDD) – Defines the differences between a standard and a specific nation's Configuration Management (CM) requirements to fulfill that nation's data link philosophy and operational needs.

   2. Service Difference Document (SDD) – Defines the difference between the MIL-STD and NDD requirements, and a specific Service's CM requirements to fulfill that Service's data link

c. The association of the MIL-STD, NDD and SDD are depicted in

FIGURE 7.

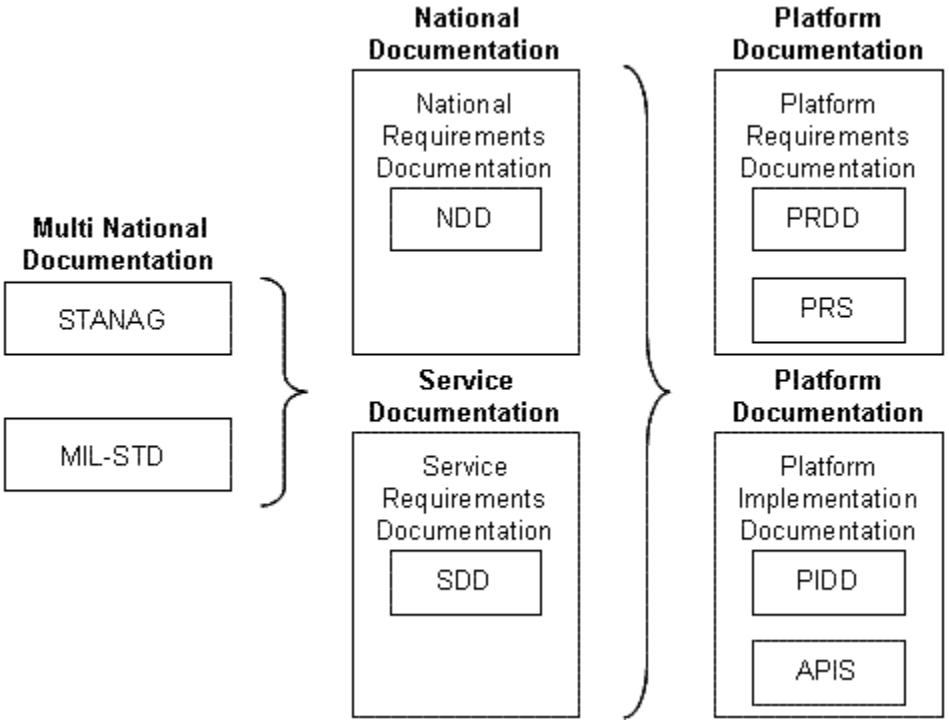

FIGURE 7. MIL-STD/NDD/SDD Association.

This Page Intentionally Left Blank

6. JCIDS, INTEROPERABILITY, AND iSMART

6.1. Introduction

6.1.1. This Paragraph provides a high-level discussion of the relationship between the JCIDS, Information Technology (IT) and National Security Systems (NSS) and the iSMART process. It was written primarily in response to requests by Program Managers to understand the relationship between these processes, understanding that iSMART is a life cycle process, while the JCIDS, IT and NSS are of limited duration.

6.1.2. The CJCSI/M 3170.01series, the Instruction/Manual for JCIDS, prescribes policy and procedures for the JCIDS. The JCIDS supports the CJCS and the JROC in identifying, assessing and prioritizing joint military capability needs. The JCIDS provides the CJCS advice and assessment for acquisition programs in support of the Defense Acquisition Process. Joint Staff J6 performs review, certification and validation of interoperability and supportability of JCIDS documents for acquisition programs supporting milestone decisions (ICD/CDD/CPD) and other programs as required/requested through the JCIDS process.

6.1.3. CJCSI 6212.01, the Instruction for Interoperability and Supportability of IT and NSS, establishes policies and procedures for the interoperability and supportability certification and validation of JCIDS Acquisition Category (ACAT) programs and for all non-ACAT and fielded systems. It also provides guidance for development and assessment of the Net-Ready Key Performance Parameter (NR-KPP). It requires systems that implement TDLs to identify bit-level data prior to Milestone C.

6.1.4. Department of Defense Instruction (DODI) 4630.8 series, Procedures for Interoperability and Supportability of IT and NSS, issues the DOD policy and responsibilities for interoperability and supportability of IT and NSS. This instruction governs the format for Information Support Plans (ISP).

6.1.5. iSMART supports the above policies and requirements in that data link implementation is designed and engineered to support the platform's information exchange requirements. The JCIDS process is applicable at the system acquisition level. Through the iSMART process, the PO/PM ensures that its platform satisfies joint requirements for military capabilities. iSMART also provides clarity at the required level of detail for CJCSI 6212.01 series and supports the JCIDS and IT/NSS requirements.

6.1.6. The following paragraphs are intended to show the linkages between CJCSI 3170.01 series and CJCSI 6212.01series IT/NSS policy and requirements, and iSMART. Readers are encouraged to read those documents in their entirety, as only that information relevant to iSMART is represented herein.

6.1.6.1. POs/PMs/PDAs should also be familiar with these references when preparing JCIDS documents:

d. Department of Defense Document (DODD) 4630.05 series, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

e. Department of Defense Directive (DODD) 8320.02, series Data Sharing in a Net-Centric Department of Defense

f. Department of Defense Instruction (DODI) 4630.8 series, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

g. Joint Requirements Oversight Council Memo(JROCM 261-06), Cost Performance and Interdependency Chart Implementing Directive

h. Department of Defense Information Enterprise Architecture (IEA), Version 1.2

i. Global Information Grid (GIG) Technical Guidance (GTG), GIG Joint Tactical Edge Service Guidance

j. Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01 series, Joint Capabilities Integration and Development System (JCIDS)

k. Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01 series, Interoperability and Supportability of Information Technology and National Security Systems

6.1.6.2. The JCIDS process in CJCSI/M 3170.01 series supports the concept of design tradeoffs in order to support earlier fielding of required systems. Through the manipulation of threshold and objective values for each KPP, systems that are less than ideal are fielded, as long as they bring needed capability to the warfighter.

Similarly, the iSMART process ensures that design tradeoffs do not result in a platform being unable to meet its threshold operation requirements. The iSMART process also ensures that platforms using an incremental (blocks, versions, etc) development plan, which is an evolutionary acquisition strategy, are interoperable at each level of development. This acquisition strategy provides needed capabilities that are interoperable within the GIG at the earliest opportunity.

6.1.7. JCIDS process in CJCSI/M 3170.01 series supports the concept of design tradeoffs in order to support earlier fielding of required systems. Through the manipulation of threshold and objective values for each KPP, systems that are less than ideal are fielded, as long as they bring needed capability to the warfighter.

Similarly, the iSMART process ensures that design tradeoffs do not result in a platform being unable to meet its threshold operational requirements. The iSMART process also ensures that platforms using an incremental (blocks, builds, versions, variants, flights, updates, new baselines) development plan, which is an evolutionary acquisition strategy, are interoperable at each level of development. This acquisition strategy provides needed capabilities that are interoperable within the GIG at the earliest opportunity.

6.1.8. The iSMART product development sequence is similar to the JCIDS product development process and is depicted in FIGURE 8, in relation to JCIDS and IT/NSS milestones.

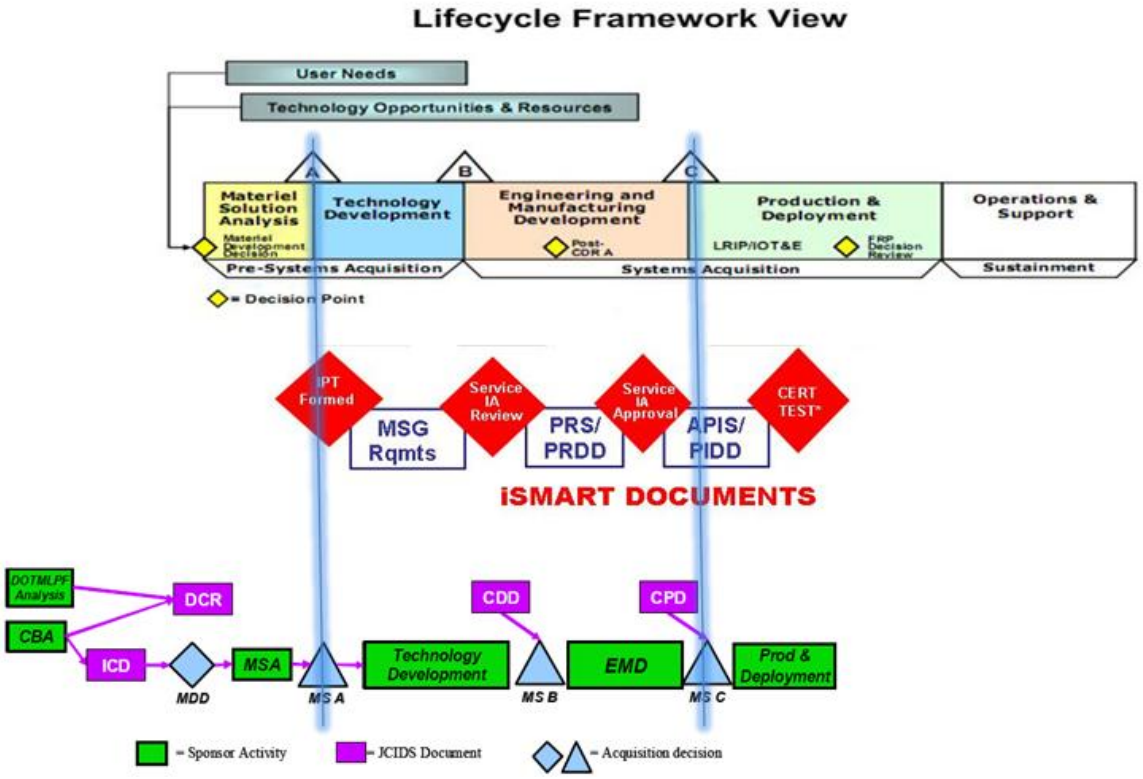

FIGURE 8. iSMART, JCIDS, IT & NSS Lifecycle.

6.1.9. TABLE VI identifies iSMART, JCIDS and IT documents and their functions. iSMART documents are designed to support a rigorous engineering process based on the same policies as the JCIDS documentation and will complement the overarching JCIDS process. JCIDS requires that all DOD acquisition programs be capabilities based. The iSMART process steps are performed in coordination with the JCIDS process as follows:

TABLE VI. iSMART, JCIDS, NR-KPP and ISP Functions.

iSMART	CJCSI/M 3170.01 (JCIDS)	CJCSI 6212.01 (NR-KPP) DODI 4630.8 (ISP)	Function
	Capabilities-Based Assessment (CBA)		Identify existing System of System operational requirements. Determine data exchanges that support operational requirements. Prioritized list of capabilities are the basis forintegrated architectures .
	CBA		Defines new capability required. States data exchange requirements nonspecific to a particular link. Define/ refine architectures.
Identify requirements to implement a data link.	CBA		Identifies capability needs in data exchange, and possible risks .
Establish IPT. Identify which data links to implement.	Initial Capabilities Document (ICD)		iSMART identifies Information Exchange Requirements (IERs) specific to each data link derived from proposed architectures. Supports Milestone (MS) A decision.
Define TDL messages to be implemented.	Capability Development Document (CDD).	NR-KPP ISP	iSMART data link message requirements support CDD and utilize common architecture products in NR-KPP. Supports MS B decision.
PRS/PRDD APIS/PIDD	Capability Production Document (CPD)	NR-KPP and ISP. Identify bit-level implementation.	PRS/PRDD state specific data link implementation and meet CJCSI 6212.01 requirements to identify bit-level. Supports MS C decision.

6.2. Capabilities-Based Assessment (CBA)

6.2.1. The CBA is the Joint Capabilities Integration and Development System analysis process. It answers several key questions for the validation authority prior to their approval: define the mission; identify capabilities required; determine the attributes/standards of the capabilities; identify gaps; assess operational risk associated with the gaps; prioritize the gaps; identify and assess potential non-materiel solutions; provide recommendations for addressing the gaps.

6.3. Initial Capabilities Document (ICD)

6.3.1. The ICD documents the JCIDS process analyses that describe the capability gaps and identifies potential non-materiel and materiel approaches to addressing those gaps. The approaches identified should cover the Joint spectrum of possibilities. The result should not be a stove-piped approach to a gap. The ICD primarily supports the System Requirements Review (SRR) and development of a Milestone A acquisition decision, integrated architectures, and updating of capability roadmaps.

6.3.1.1. Types of capability gaps:

a. Functional Areas

b. Relevant range of military operations

c. Desired effects

d. Time and Doctrine

e. Organization

f. Training

g. Material

h. Leadership and Education

i. Personnel

6.3.2. The iSMART process continues beyond the Capabilities Based Assessment (CBA) with the development of an ICD within the iSMART process. The iSMART IPT should be established as discussed in Paragraph 5. The participants will assist with identifying the most appropriate Data Exchange Medium (DEM) material solution. This will include the specific data to be exchanged, the operational facility with which the data is exchanged, by what medium, and in support of what operational activity.

The process by which the ICD is developed ensures that the program office addresses data link implementation across the entire spectrum of requirements. The identification of capability gaps ensures that the platform does not unknowingly implement a DEM that does not support the system's requirements, and allows early planning to fill capability gaps that can be corrected. The ICD should be provided to the program developer (or included in the Request for Proposal (RFP), if applicable)) so that informed cost estimates can be made.

6.4. Capability Development Document (CDD)

6.4.1. The CDD specifies the attributes of a system in development. These will provide or contribute to the operational capabilities that are inserted into the performance section of the acquisition strategy. The CDD is the sponsor's primary means of defining authoritative, measurable and testable capabilities in the form of Key Performance Parameters (KPPs) needed

by the warfighters to support the System Development and Demonstration (SDD) phase of an acquisition program.

The development of the CCD consists of the Integrated Architectures, applicable Joint Capability Documents (JCDs), the ICD, the Analysis of Alternatives (AoA) and the technology development strategy guide. The CDD captures the information necessary to deliver an affordable and supportable capability using mature technology within a specific increment of an acquisition strategy. The CDD will be validated and approved before Preliminary Design Review (PDR) and Milestone B within the JCIDS process.

6.4.1. Initial Information Support Plan (ISP). All systems that exchange information with external systems will be, tested, evaluated, and certified for Interoperability and Supportability (I&S). For the CDD, this is called the Initial ISP and is governed by the CJCSI 6212.01 series and DODI 4630.8 series. The I&S process consists of integrating the four steps of the NR-KPP process, Mission Analysis, Information Analysis, Systems Engineering, and Documentation. The CDD is the first JCIDS document required to contain the NR-KPP. Their relationship to the iSMART products is summarized below:

6.4.1.1. Compliance with the DOD Information Enterprise Architecture (IEA) and CJCSI 6212.01 series. The IEA serves as a common, enterprise-level, reference model for the DOD's Net-Centric Data/Services, solution architectures and information assurance elements. for current and future acquisition programs to use in focusing and achieving net-centric operational support through the GIG.

Appendix F of IEA maps the DOD IEA activities to the Net-Centric Operations and Warfare Reference Model (NCOW RM) activities which were used to develop some legacy systems and provides a transition bridge to the IEA.

6.4.1.2. Integrated Architecture Products. CJCSI 6212.01series defines the CDD Department of Defense Architecture Framework (DODAF) architectural views to be included in the JCIDS ICD, CDD and CPD. The products consist of Operational, Systems and Standards views for platforms that implement data links. The Operational View (OV-3), Operational Resource Flow Matrix, and IERs are a product of the iSMART IPT. They are used to define the specific data link messages to be implemented.

This allows the initial development of the PRS/PRDD to begin. Although the OV-3 is no longer required with the NR-KPP, it is the basis for the Systems View (SV-6), Systems Resource Flow Matrix that is one of the NR-KPP required views. The Standards View (StdV-1) Profile defines the technical, operational, and business standards, guidance, and policy applicable to the architecture being described. Other required architecture products have similar iSMART and JCIDS relationships.

6.4.1.3. Compliance with Applicable GIG Technical Profiles (GTPs). The purpose of a GTP is to identify an interface to the GIG in accordance with (IAW) the GIG Technical Guidance (GTG). The TDES Interoperability Authorities have available the applicable GTPs

originally developed as KIPs to support data links. The iSMART process supports standards compliance, an important element of the NR-KPP, the DOD IEA and the GTPs applicable to a platform.

6.4.1.4. Compliance with DOD Information Assurance Requirements. The CDD will describe how a system will implement Information Assurance policies and procedures. During the development, design and testing of the fielded data links these requirements have been taken into account and Information Assurance is an important requirement for legacy data links. The TDES Interoperability Authorities and capability / requirements generation offices have available documentation from previously approved systems that will assist in fulfilling this requirement.

6.4.2. During CDD development, the iSMART IPT will assist the PO/PM in defining and scheduling the Service and joint interoperability evaluation and certification

6.5. Capability Production Document (CPD)

6.5.1. The CPD is the sponsor's primary means of providing authoritative, testable capabilities for the Production and Deployment phase vice the CDD SDD phase of an acquisition program. A CPD is finalized after a design readiness review and is validated and approved before the Critical Design Review (CDR) and Milestone C acquisition decision within the JCIDS process. The development of the CPD is guided by the integrated architectures; applicable JCDs, ICDs and CDD; AoA and/or supporting analytical results; developmental and operational test results; and the design readiness review.

As the CPD is finalized after a design readiness review and after the majority of capability development, it is normally not appropriate to introduce new requirements at this point. The CPD captures the information necessary to support production, testing and deployment of an affordable and supportable increment within an acquisition strategy. The CPD refines the threshold and objective values for performance attributes and KPPs that were validated in the CDD for the production increment. The refinement of performance attributes and KPPs is the most significant difference between the CDD and the CPD.

6.5.2. Revised ISP. All CDDs for systems that exchange information with external systems will be evaluated and certified for Interoperability and Supportability. This is called the Revised ISP review. It will include a more detailed inspection of the Initial ISP that was delivered with the CDD and described in 6.6.2. Any missing or incorrect product elements should be completed and included with the CPD, to include all components of the NR-KPP.

6.5.3. PRS/PRDD. The IPT assists the PO/PM in the development of the PRS/PRDD. The MIP available in the PRS/PRDD meets the new requirements of CJCSI 6212.01 series and is a pre-requisite for CPD approval. The PRS/PRDD is a component of the ISP.

6.5.4. Interoperability Evaluation. The PO/PM approved MIP and the developers implementation differences are identified to the bit-level when the APIS and PIDD are provided to the TDES Interoperability Authority. The TDES Interoperability Authority will conduct

interoperability evaluations with the PO/PM as contract deliverables are provided for the emerging system.

This is a continuing process to assist the PO/PM on delivering capabilities based on the best balance of resources. When the TDES Interoperability Authority validates the program's bit-level data (PRS/PRDD/APIS/PIDD) and posts these documents to the Joint iSMART database, the Services and joint community can conduct cross platform and mission area assessments.

6.5.5. Interoperability Certification. The IPT will assist the PO/PM/PDA in identifying the timeline and process to complete Service and joint interoperability certification. This is explained in more detail in Paragraph 8, Service Appendices and Service documents.

7. JOINT IMPLEMENTATION OF iSMART

7.1. Joint iSMART Databases

7.1.1. Service approved iSMART products are maintained by the individual TDES Interoperability Authorities. The Service iSMART data base procedures are coordinated with their respective POs/PMs/PDAs. The procedures for Service approval process of the initial iSMART documentation (PRS/PRDD) are described in Paragraph 5 and modified as necessary in the appropriate Service appendix.

iSMART is used throughout the life cycle of a system. The Services and POs/PMs/PDAs will have a process for the iSMART documentation to remain current while program changes and improvements are implemented following Initial Operating Capability (IOC).

7.1.2. The purpose of the Joint iSMART databases is to facilitate cross platform interoperability assessments and Joint Mission Area assessments by utilizing the iSMART tools, which are discussed in more detail in Paragraph 9. The concept is that the TDES Interoperability Authority will post to the Joint iSMART database of approved iSMART documents. The other TDES Interoperability Authorities and joint users will be notified when changes are posted.

7.2. Interoperability Enhancement Process (IEP)

7.2.1. The objectives of the Interoperability Enhancement Process (IEP) are to:

a. Improve Joint warfighting by developing and providing critical capabilities supporting Joint Mission Thread (JMT) interoperability assessments early in a program's life cycle.

b. Offer Joint planners and operational users' lessons learned with systems interacting in Joint and coalition networks.

c. Provide technical work-arounds addressing current platform interoperability deficiencies that will contribute to a clearer Common Tactical Picture (CTP).

7.2.2. The IEP will assist in the realization and maintenance of interoperable net-centric weapons, sensors and C2 systems at the tactical edge. The IEP will identify interoperability gaps based on weapon, sensor or C2 system demonstrated information exchange capabilities analyzed with respect to the current policies, doctrines, architectures, operational employment concepts, standards, roadmaps, and the JMTs that collectively form the standard view of the TDES Architecture for tactical data link related/dependent systems.

For emerging systems, the IEP will be conducted prior to Milestone C of the platform. The IEP is a collaborative process with Defense Information Systems Agency (DISA), Joint Staff, TDES Interoperability Authorities and the selected POs/PMs.

7.2.3. The IEP consists of two components: Joint iSMART and Joint Capabilities and Limitations (JC&L). JC&L provides warfighters in operational terms how net-enabled platforms interoperate. The goal of the IEP is to enhance and synchronize current Service iSMART and JC&L capabilities. The IEP will provide a path to implement the digital bit-level documentation requirements in CJCSI 6212.01 series and the mission area assessment that supports JMTs in CJCSI 6610.01 series

7.2.4. CJCSI 6610.01series requires the Joint Staff to review the platform's PRS and PRDD during the iSMART process to conduct initial joint mission area interoperability assessments. These assessments are intended to work in conjunction with the IEP.

7.2.5. Service POs/PMs/PDAs fulfill the requirement of CJCSI 6212.01 series to identify platform TDL implementation details at the bit-level by populating the PRS and PRDD prior to Milestone C. The Service populated Joint iSMART database is the source to conduct joint mission area assessments. The common format and bit-level detail are made available to the interoperability community by TDES Interoperability Authorities and POs/PMs/PDAs. The implementation of the iSMART process is the cornerstone which determines a platform's ability to participate in joint mission areas.

7.3. Joint Capabilities and Limitations (JC&L)

7.3.1. The objective JC&L will provide the Joint Data Network Officer (JDNO), Joint Interface Control Officer (JICO) and TDL users a reliable, up to date product that assists them in planning, analyzing, and optimizing Multi-TDL Architectures. JC&L will contain a comprehensive assessment of the overall capabilities of net-enabled platforms operating in a joint environment.

The objective JC&L will consist of an architecture that permits access to Service validated operational impact assessments on how specific platforms function together in their primary networks. JC&L will be available to the operational community 24/7 to assist in all phases of Joint Task Force missions.

7.3.2. Capabilities and Limitations (C&L) currently exist as Service efforts that provide various levels of support to joint warfighters. It is envisioned that the Service C&L efforts will migrate to a common JC&L. JC&L includes numerous inputs, including the TDL aspects that have been defined by the Services, Lessons Learned, Joint exercises, feedback from technical SMEs and the operational community. A common starting point for developing JC&L will be selected data from iSMART databases and potentially use some of the iSMART tools.

7.4. Continuing Challenges

7.4.1. The use of common databases and tools are the essential elements to leverage the technical interoperability views that the iSMART process provides. Recognizing that iSMART implementation by the Services and joint community is not yet fully synchronized, there are issues that have to be resolved and will take a dedicated effort by the interoperability community. Some of these issues require resolution to fully realize the potential of the Joint iSMART process. They include, but are not limited to:

a. Configuration control and management procedures for the Joint Enhanced iSMART (eSMART) databases to support data sharing between the Services and timely certification testing.

b. Configuration control and management of the Joint eSMART tools.

c. Relationship and interaction of eSMART data and tools with JC&L.

7.4.2. Future versions of this Handbook will update the eSMART analysis process, products and reference data as these evolve.

This Page Intentionally Left Blank

8. JOINT CERTIFICATION PROCESS

8.1. Background

8.1.1. JITC, conducts Joint Interoperability Testing (JIT). Enclosure F to CJCSI 6212.01series describes the Joint Interoperability Testing and Certification process. All National Security Systems must be evaluated and certified by the JITC. All systems (Acquisition Category (ACAT), non-ACAT and fielded systems) must be evaluated and certified prior to fielding, and periodically, every four years, during their entire life, as outlined in the JCIDS process.

Following the iSMART process will assist a PO in developing the documentation required to demonstrate that platform data link implementation fulfills the JCIDS process requirements. See the current version of CJCSI 6212.01 series for full interoperability testing requirements in order for a system to be certified for interoperability IAW the NR-KPP.

8.2. Joint Certification Process

8.2.1. The following is a brief summary of the joint certification process:

a. Collect the approved requirements and capabilities identified by the iSMART process:

   1. Systems must successfully complete Service Level Testing (SLT) prior to participating in JIT testing.

   2. All systems will contact Service Participating Test Unit Coordinator (PTUC) for test scheduling and any coordination with JITC.

   3. All systems participating in a JIT, as a System Under Test (SUT) or a participant, will provide their Service PTUC the latest actual bit-level baseline implementation document.

b. Test and evaluation:

   1. JIT involves multiple test events of system capabilities and functional areas. Testing is conducted at various test facilities with representatives from all the Services participating.

   2. Evaluation provides conclusive results representing the entire range of operational uses, configurations and conditions.

   3. Provides assessment of expected operational impact for any discrepancies.

c. Certification and other status reporting:

1. Standards Conformance Certification. Is issued after the technical testing of the systems critical threshold requirements against published standards has been completed. (e.g., conformance to MIL-STD-6016).

2. Joint Interoperability Test Certification. Is issued when all critical threshold requirements for a specific increment has adequately demonstrated Joint interoperability with other systems. This system certification attests that the system's interoperability is sufficient to support a fielding decision.

3. Special Interoperability Test Certification. Issued for systems or system components that require interoperability test certification but are not subject to the JCIDS process, and generally do not individually need requirements certified by the Joint Staff.

4. Limited Joint Interoperability Test Certification. Is issued when a subset of systems interoperability requirements has been adequately demonstrated with other systems. A "limited" certification may not be sufficient to allow fielding.

5. Non-Certification. If system is fielded, critical operational impacts are expected. This provides a warning to the warfighter

.

9. iSMART TOOLS AND THEIR PRODUCTS

9.1. Tools/Products

Various tools exist or are in development that may aid the execution of the iSMART process. The process itself is founded in basic systems engineering principles and does not require any special tools to succeed. Some tools are limited to Link 16 only, or are not suitable for some developers. These tools and their products are explained below.

9.2. iSMART Toolset

9.2.1. The iSMART toolset consist of the following functions.

a. Documenting detailed platform/system tactical data link implementation requirements and actual developed implementation required to perform the iSMART process.

b. Conducting interoperability analysis of the detailed platform documentation in accordance with the iSMART process.

c. Developing detailed reports of documented platform requirements or implementation data and reports of the analysis.

9.2.1.1. Systems will have to determine the level of data they can provide in accordance with the iSMART process. At a minimum, a bit-level implementation on currently fielded systems should be developed. This bit-level implementation can be used to identify future requirements as well as detailed platform requirements specifications that should be used for future upgrades to the system. iSMART toolset functions are described in more detail below.

9.2.2. Documenting and Analyzing Information Exchange Requirements (IERs). The iSMART tool has the capability to document and analyze IERs between platforms/systems utilizing a common set of reference data called Information Definitions. This allows systems being developed to conduct IER analysis prior to developing detailed communication medium requirements specifications.

This consists of analyzing a subject platform/system's bit-level implementation against bit-level implementation of objective systems; the subject platform/system is required to exchange data with. This analysis can identify capabilities gaps, requirements shortfalls, interoperability issues between platforms and/or the need for gateways.

9.2.2.1. The iSMART tool contains capabilities for generation, storage and maintenance of platform requirements and platform implementation specification documentation. Documentation produced includes the PRS, PRDD, PIDD and the APIS.

a. The PRS specifies platform requirements based on a reference standard (e.g. MIL-STD or other Standard).

b. The APIS documents are the fielded or actual implementation data of that platform referenced to the baseline standard.

9.2.2.2. The iSMART tool provides the capability to perform analysis of the system requirements or implementation specifications:

a. The analysis function of the iSMART tool contains comparison features which enables the comparison of two or more documents against the message standards and against each other.

   Comparison can be done by viewing the full text of the message standard document with deviations from the other selected platform documentation highlighted next to the relevant paragraph. The selected documents also can be viewed side-by-side in table view with the deviations color-coded.

b. Interoperability Analysis (IOA) – compares the messages being transmitted by one system against the reception capability of other systems. This analysis is used to determine message level interoperability of one system transmitting data on the network against other network participants.

   For example, analyzing a C2 System transmitting surveillance data and Non-C2 systems receiving surveillance data to determine what data will be lost by the Non-C2 systems and the impact of that loss on the mission. FIGURE 9 is an example of an IOA.

TDL interoperability Assessment							
Serial No	US5	User App	Operator Level A	Release Level:	1	IOM Q No.	50
Originator	SSCPAC 59	Source	IOM				
Op Summary	(U) It is not possible to exchange imagery data between US Navy surface units and F/A-18 aircraft.						
Functional Area	Imagery Date: 22/09/11						
Platform Combinations	DDG 53 / F/A-18 CVN 75 F/A-18						
Op Detail	(U) Navy surface units do not transmit or receive imagery data (J16.0). When operating with the F/A-18 and surface units, the imagery message should not be used.						
Technical Detail	(U) United States Navy (USN) surface units do not implement the J16.0 Imagery message						
Further Action	(U) None						

FIGURE 9. Example of a Link 16 IOA.

c. Generic IO Analysis – compares the system's transmit and receive capability against the transmit and receive capability of another system. For example, a system's transmit and receive fielded capability can be compared against its required transmit and receive capability to determine what needs to be completed to meet the systems requirements.

This Page Intentionally Left Blank

10. NOTES

10.1. Intended use. The contents of this handbook are intended to serve as a guide to the use of tactical data links and message formatting in systems used for military applications.

10.2. Supersession data. There is no supersession data as this is the first submittal of this document.

10.3. Subject term (key word) listing.

- Tactical datalinks
- Message formatting
- Message transmission
- Interoperability of DoD IT systems

10.4. Changes from previous issue. There are no changes from the previous issue as this is the first submittal of this document.

This Page Intentionally Left Blank

US AIR FORCE

A.1. INTRODUCTION

A.1.1. This appendix to the iSMART Military Handbook

a. Defines United States Air Force (USAF) specific procedures

b. Defines the USAF process for developing required iSMART documentation

c. Defines how to access the USAF approved iSMART tools.

d. Provides links to the USAF resources for more information regarding the USAF's iSMART process.

A.2. CLARIFICATIONS TO THE JOINT HANDBOOK

A.2.1. The AF Command and Control Integration Center (AFC2IC) is the USAF's Tactical Data Enterprise Services (TDES) Representative. For further detail on the USAF's iSMART program please see the contact at the end of this appendix.

A.2.2. The USAF does not implement formal Integrated Process Teams (IPTs) for the implementation of the iSMART program. The normal procedure is for Platform Program Offices at the Major Commands (MAJCOMs) to engage the AFC2IC for support during the platform's Tactical Data Link development requirements phase. The MAJCOMs also work with the platform's System Program Offices (SPO) to coordinate iSMART activities.

A.2.3. AFC2IC will support the development of the PRS, which platform requirements baselined on reference standard (e.g. platform requirements from MIL-STD 6016C Ch1).

A.2.4. AFC2IC has a detailed Service level iSMART program overview available to USAF and supported joint system users that further clarifies details unique to the Air Force program. This guidance can be obtained by contacting the AFC2IC iSMART team.

A.3. Developing the USAF Platform Implementations

A.3.1. The USAF iSMART process utilizes Information Exchange Requirements (IERs) analysis by aligning platform specific IERs to a common set of reference data called Information Definitions. This allows program offices to document a system's information exchanges and analyze them against a common reference set. This analysis determines the TDL Communications Media that will satisfy the required information exchanges.

A.3.2. Another means of developing platform requirement specifications is to utilize the functional Implementation Requirements defined in the TDL MIL-STDs. AFC2IC has developed generic template iSMART products for each functional area (consisting of iSMART

Difference Documents and detailed bit-level message implementations) that, using the iSMART Toolset, can be combined to support the development of various types of platforms.

A.3.3. All platform requirement documents are benchmarked in the USAF. Using the iSMART tools, systems can select iSMART products that are closest to that type of system and further develop it to meet their requirements. For example, a new Fighter/Attack aircraft could utilize the F-16 Platform Requirements Specification as the starting point for development of a new PRS.

A.4. US AIR FORCE TEST AND CERTIFICATION

A.4.1. Currently there is no enterprise level requirement for programs in the USAF to implement the iSMART process, however USAF interoperability test and certification organizations (Operational/Development testing, Standards Compliance testing) require programs provide implementation data prior to testing. The required data is the APIS which is the actual implementation requirements specification and a detailed bit-level message implementation. The test organizations have requested that programs provide this data in the iSMART Toolset format.

A.5. US iSMART Toolset

A.5.1. The USAF has developed the iSMART Toolset that is used for documentation and analysis of iSMART products. The iSMART Toolset can be accessed by two methods, either online via the AFC2IC SIPRNET domain or via a stand-alone version that can be downloaded from the USAF's AFC2IC.org Webpage. The web based version is the preferred access method as this gives the user access to the centralized platform data repository hosted by the AFC2IC. Please use the USAF contact information in this appendix for more information.

A.6. AIR FORCE iSMART POINTS OF CONTACT

Mr. David Sprott
AFC2IC/C2II
Air Force Command and Control Integration Center
DSN 575-3567
COMM 757-225-3567
e-mail: david.sprott@langley.af.mil

AFC2IC/C2II
Air Force Command and Control Integration Center DSN 575-5500
COMM 757-225-5500
e-mail: afc2isrc.ismart@langley.af.mil

US NAVY

B.1. Introduction

B.1.1. This is an appendix to the iSMART Military Handbook.

a. Clarifies United States Navy (USN) specific procedures.

b. Notes USN exceptions to the iSMART Military Handbook.

c. Introduces USN procedures for developing platform implementation, including the MIP.

B.2. Clarifications to the Joint Handbook

B.2.1. The USN TDES Interoperability Authority (IA) is SPAWAR Systems Center, Pacific (SSC PAC) Code 591. The Navy has established procedures for developing the iSMART documentation. Paragraph 5 of the main body describes the role of the Integrated Process Team (IPT) in developing the platform's implementation. The paragraphs below provide USN clarifications.

B.2.2. Each Program Office establishes an Integrated Process Team (IPT) to develop the message exchange requirements for each identified DEM/capability set. The IPT consists of the Program Office, Program Developer, and the TDES Interoperability Authority. The IPT will:

B.2.3. Determine the high-level message implementation requirements for the platform to include message, word, and action value implementation. This is called the Message Implementation Plan (MIP). The MIP is submitted to SSC PAC, Code 591 as early in the development cycle as possible. SSC PAC Code 591, as the TDES IA for the U.S. Navy, will review the MIP and determine if the platform's implementation is considered interoperable with other fielded systems.

If not, comments are provided to the Program Developer for their review and update. Once the MIP is accepted, it is then presented to Navy Cyber Forces (CYBERFOR) for concurrence prior to development of the PRS. Program Developers should contact SSC PAC Code 591 for additional details on the MIP.

B.2.4. Develop the precise protocol and data item level implementation for the platform, from the high level implementation. These are documented in the PRS and PRDD for the platform. The PRS shows the exact Link 16 requirements and data item level implementation of the platform. The PRDD documents the deviations from the requirements and provides justification for the deviations.

B.3. Developing the USN Platform Implementations

B.3.1. Paragraph 5.4 of the main body describes how the IPT determines the messages required for implementation by the platform. The paragraphs below provide USN clarifications.

B.3.2. Identifying Messages for Implementation

B.3.3. The workflow that best supports the IPT process should be flexible due to the wide range of factors that may influence the decision-making process.

B.3.4. The IPT identifies message implementation to satisfy the platform's IERs and comply with appropriate standards. The MIP contains the data link implementation at the message, word, and action value required to support the platform's data exchange requirements.

B.3.5. After analysis and recommendation by SSC PAC, the PRS/PRDD are submitted to CYBERFOR for final approval of the platform's implementation. This review will determine if the platform is taking the correct approach for its implementation. CYBERFOR will approve the MIP or recommend changes before approval. Platforms that do not receive CYBERFOR approval will not be eligible for Service or Joint level certification.

B.3.6. Upon approval of the MIP, CYBERFOR will release a message providing a recommendation to continue with platform development. The message will describe discrepancies and operational impacts, and whether a failure to correct will prevent the platform from receiving final approval. The TDES Interoperability Authority will post the platform's approved message implementation on the Joint iSMART web site, when established..The Navy TDES IA will then notify the other TDES Interoperability Authorities and the Joint Staff J8 DDC4 (Deputy Director for C4, Data and Services Division) of the MIP approval and posting.

B.4. DOD IEA and DODAF Artifacts

B.4.1. Paragraph 6.6 of the main body describes the role of the Tactical Data Enterprise Service (TDES) Interoperability Authority in developing IEA and DODAF artifacts. The paragraphs below provide USN clarifications.

B.4.2. Compliance with the DOD IEA. The IEA serves as a common, enterprise-level, reference model for the DOD's Net-Centric Data/Services , solution architectures and information assurance elements for current and future acquisition programs to use in focusing and achieving net-centric operational support through the GIG. Appendix F of IEA maps the DOD IEA activities to the Net-Centric Operations and Warfare Reference Model (NCOW RM) activities which were used to develop some legacy systems and provides a transition bridge to the IEA.

B.4.3. Integrated Architecture Products. CJCSI 6212.01series defines the DODAF architectural views to be included in the JCIDS ICD, CDD and CPD. The products consist of operational, systems and standards views (OV, SV, and StdV) for platforms that implement data links.

B.4.4. Compliance with GTPs. The purpose of a GTP is to identify an interface to the GIG. The iSMART process supports standards compliance, an important element of the NR-KPP, the DOD IEA and the GIG GTPs s which are applicable to a platform.

B.5. USN Procedures for Developing, Approving and Certifying Platform Implementation

B.5.1. Specific USN procedures are provided in the USN iSMART Handbook. These procedures will be used by USN program offices seeking system/platform certification, and are available from SSC PAC Code 591 (see contact information below).

B.5.2. Information about which Navy platforms use the benefits of the iSMART process to enhance systems engineering and interoperability is posted on the DISA and SSC PAC iSMART websites.

B.6. US Navy iSMART Points of Contact

Jay Fernandez
SSC PAC 59112
Standards Management
DSN : 553-0567
COMM : (619) 553-0567
FAX: (619) 553-7526
e-mail: jay.fernandez@navy.mil

Rodney L. Lee
SSC PAC 59112
Standards Management
DSN : 553-7316
COMM : (619) 553-7316
FAX : (619) 553-7526
e-mail : rodney.l.lee@navy.mil

Dan Stigall
SSC PAC Code 59141
Interoperability Testing
DSN : 553-0374
COMM : (619) 553-0374
FAX: (619) 553-9789
e-mail: dannie.stigall@navy.mil

This Page Intentionally Left Blank

US ARMY

C.1. Introduction

C.1.1. This is an appendix to the iSMART Military Handbook

a. Clarifies United States Army (USA) specific procedures.

b. Provides the status of iSMART implementation in the USA.

C.2. Clarifications to the Joint Handbook

C.2.1. Currently, there is no recognized requirement in the USA to implement iSMART process. Some Program Managers have informally applied the iSMART process and utilized the eSMART tools to assist in meeting interoperability requirements. Their experience to date has been positive.

C.2.2. The USA TDES IA is US Army CIO G6 (SAIS AOJ) as the interoperability authority for the Army

C.2.3. US Army Communications and Electronics Command (CECOM) SEC* is the Army's VMF and associated Combat Net Radio (CNR) applications iSMART Subject Matter Expert (SME). Their Points of Contact (POCs) are listed below.

C.2.4. Aviation and Missile Research Development, and Engineering Center (AMRDEC), Software Engineering Directorate (SED) is the Army's Link 16, Link 11, JREAP iSMART SME and their POCs are listed below.

C.2.5. Emerging systems that implement data links are encouraged to consider implementation of the iSMART process. Contact the appropriate POCs at the earliest opportunity.

C.3. US Army iSMART Points of Contact

Victoria H. Moore
HQDA, CIO/G6 SAIS-AOJ
DSN: 332-6593
COMM: (703) 602-6593
e-mail: victoria.moore@us.army.mil

Deborah A. Barclay
HQDA CIO/G6 SAIS-AOJ
DSN: 865-1481
COMM: (703) 545-1481
e-mail: deborah.a.barclay.ctr@mail.mil

Gerald L. Cantrell
AMRDEC/SED (RDMR-BAC)
DSN: 746-0849
COMM: (256) 876-0849
e-mail: gerald.l.cantrell@us.army.mil

APPENDIX D

US MARINE CORPS

D.1. Introduction

D.1.1. This is an appendix to the iSMART Military Handbook

a. Clarifies United States Marine Corps (USMC) specific procedures.

b. Provides status of iSMART implementation.

D.2. Clarifications to the Joint Handbook

D.2.1. The USMC Tactical Data Enterprise System Interoperability Authority is the Marine Corps Tactical Systems Support Activity (MCTSSA). The Integrated Process Team functions will be coordinated and administered by the Program Managers of Marine Corps Tactical Data Link capable systems.

D.2.2. There is not a USMC directive that mandates implementation of iSMART. Selected programs of record are being loaded into the iSMART application.

D.2.3. MCTSSA coordinates all data link interoperability issues, including Link 11, Link 16, VMF, and associated Combat Net Radio applications, and provides guidance to the Program Managers regarding implementation of applicable Military Standards.

D.3. U.S. Marine Corps iSMART Points of Contact

Marine Corps Tactical Systems Support Activity (MCTSSA)

Mr. Earl (Buck) Connally
MCTSSA Interoperability Branch Head
e-mail: Earl.connally@usmc.mil

Mr. James Wells
MCTSSA Standards Management
DSN : 365-2965
COMM : (760) 725-2965
e-mail: james.a.wells@usmc.mil

Ms. Julie Goodrich
MCTSSA TCG IOB (TCG-04)
DSN : 365-2165
COMM : (760) 725-2165
e-mail: julie.goodrich@usmc.mil

This Page Intentionally Left Blank

OTHER POINTS OF CONTACT

E.1. DOD/Agency/Joint iSMART Points of Contact

Office of Assistant Secretary of Defense (OASD)
Networks and Information Integration (NII)
Command, Control, Communications, Space and Spectrum

Mr. David Narkevicius
OASD (NII)
COMM: (703) 607-0259
e-mail: david.narkevicius@osd.mil

Joint Staff

Lt Col Sam Helwig
Joint Staff/J-65A
Aerial Networks 1C1042
DSN: 222-04
COMM: (703) 692-0904
e-mail: samantha.helwig@js.smil.mil
samantha.helwig@js.pentagon.mil

JICO/Tactical Interoperability Standards
Joint Staff, J8 Deputy Director for C4, Data and Services Division

LCDR Chris Schreiner, J684
DSN: 836-8285
COMM : (757) 836-8285
e-mail: chris.schreiner@hr.js.mil

Defense Information Systems Agency (DISA)
Standards Management Branch (EE32)Mr. Ed Marston
DSN: 375-7519
COMM: (301)225-7519
e-mail: edwin.marston@disa.mil

Joint Interoperability Testing Command (JITC)

Robin S. Murray
JITC
DSN: 879-5139
COMM: (520) 538-5139
FAX: (520) 538-4375
e-mail: robin.murray@disa.mil
robin.murray@fhu.disa.smil.mil

Missile Defense Agency (MDA) BC Command and Control, Battle Management and Communications (C2BMC)
Program Directorate
Mr. Chico Menendez
DSN: 224-6750
COMM: (703) 614-6750
e-mail: Arsenio.Menendez.ctr@mda.mil

PROCESSING

F.1. Services iSMART processing

F.1.1. To receive a list of programs that are utilizing the iSMART process, contact the respective Service POCs listed in Appendices A-E.

This Page Intentionally Left Blank

CONCLUDING MATERIAL.

Custodians:
Navy - EC

Preparing Activity:
Navy – EC
(Project 5895-2009-001)

Review Agencies:
Marine Corps - MC

Agent:
DLA – GS

Civil Agencies:
TBD

The activities listed above were interested in this document as of the date of this document. Since organizations and responsibilities can change, you should verify the currency of the information above using the ASSIST Online database at https://assist.dla.mil.