



INSTITUTE FOR DEFENSE ANALYSES

CLEARED
For Open Publication

Oct 17, 2023

Department of Defense

OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Joint Interoperability: Resources and Recommendations for Improving DTE&A's Contribution to Assessing Systems

Lance E. Hancock

Kyle A. Morrison

September 2023
IDA Report P-33590
ANDREW 3000674

**Cleared for Public Release by the DoD Office of
Prepublication Review, Case 24-T-0072, 11 October 2023**

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305



The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project AX-1-5169, "Assessments for DTE&A," for the Director, Developmental Test Evaluation and Assessments. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Cleared for Public Release by the DoD Office of Prepublication Review, Case 24-T-0072, 11 October 2023

Acknowledgments

The authors would like to thank the IDA review committee, Dr. Stephen Ouellette (chair), Dr. David Sparrow, Dr. Evan Laprade, and Dr. James Gilmore for providing technical review of this effort.

For More Information

John S. Hong, Project Leader
jhong@ida.org, (703) 845-2564

Stephen M. Ouellette Director, SED
souellet@ida.org, (703) 845-2443

Copyright Notice

© 2023 Institute for Defense Analyses
730 East Glebe Road, Alexandria, Virginia 22305 • (703) 845-2000

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (Feb. 2014).

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document P-33590

Joint Interoperability: Resources and Recommendations for Improving DTE&A's Contribution to Assessing Systems

Lance E. Hancock

Kyle A. Morrison

Executive Summary

The Office of the Executive Director of Developmental Test, Evaluation and Assessments (ED, DTE&A), Office of the Undersecretary of Defense (OUSD) for Research and Engineering (R&E) requested IDA to investigate whether DTE&A Action Officers have access to the necessary data for assessing the interoperability of systems under their oversight. The study was based on phone interviews with 12 DTE&A Action Officers from across the DTE&A warfare areas (Air, Land, Missile Defense, Naval, Space, and Nuclear Command, Control, and Communications (NC3)) and the review of documents provided by Interoperability Steering Group (ISG) members describing the processes related to setting requirements, planning tests, and evaluating systems for Joint Interoperability (JIO).

This report provides a brief overview of the JIO development process, along with interoperability resources and references for Action Officers. It also presents insights from the Action Officers concerning JIO. In general, Action Officers rely on the Joint Interoperability Test Command (JITC) for the compilation and interpretation of JIO test data. Several factors contribute to this reliance. For instance, many Programs do not delve into system interoperability until Operational Test (OT) data are collected for Joint Interoperability Certification (JIC), which occurs late during or after Developmental Test (DT). Additionally, Action Officers often lack the guidance, resources or access needed to gather and analyze DT interoperability data. The insights shared by the Action Officers varied significantly among warfare areas and even among Programs within a given warfare area. These discrepancies can be attributed to differences in how Services and individual Program Managers conduct their operations, as well as the traditional approaches adopted in the development of specific types of systems. It is worth highlighting that Services and Programs employ diverse strategies for achieving interoperable systems. These strategies may include early planning, iterative testing and fixing during integration testing, or an expectation of making necessary fixes during the sustainment phase.

The study found that while there is a well-defined process for systems to achieve JIC through JITC, some Action Officers and Programs may lack familiarity with this process. JITC occasionally engages with Programs at an early stage, during the initial refinement of their Net Ready Key Performance Parameters (NR-KPPs) for the ISG. Nevertheless, even JITC's well-defined process can encounter challenges arising from the practical realities of military acquisition, which may not always readily facilitate interoperability testing. For instance, there may be multiple versions of a given system in the field due to

the time-consuming fielding process. Ideally, interoperability testing should encompass every significant combination of the fielded system versions, which can be impractical.

Contents

1.	Introduction.....	1-1
	A. Purpose and Audience.....	1-1
	B. Report Organization.....	1-1
	C. Methodology.....	1-1
2.	Background.....	2-1
	A. DoD Interoperability Policy.....	2-1
	B. Joint Interoperability Certification.....	2-2
	C. Motivation for Testing Interoperability in DT.....	2-3
	D. Interoperability Testing in DT.....	2-3
	E. Current DTE&A Guidance.....	2-4
3.	DTE&A Action Officer Observations.....	3-1
4.	ISG Observations.....	4-1
5.	The DTE&A Interoperability Evaluation Process and Considerations.....	5-1
	A. Conceptual DTE&A Interoperability Evaluation Process.....	5-1
	1. DTE&A Organization.....	5-1
	2. DTE&A Action Officers.....	5-2
	B. Considerations for DTE&A Interoperability Involvement.....	5-2
6.	Interoperability Resources for DTE&A.....	6-1
	A. Data.....	6-1
	B. Procedures.....	6-4
	1. JITC.....	6-4
	2. Joint Staff.....	6-4
	C. Organizations.....	6-4
7.	Final Thoughts and Future Considerations.....	7-1
	Appendix A. Joint Interoperability Certification Process Details.....	A-1
	Appendix B. Acronym List.....	B-1
	Appendix C. References.....	C-1

(This page is intentionally blank.)

1. Introduction

A. Purpose and Audience

This report is intended for Developmental Test, Evaluation and Assessments (DTE&A) Action Officers to expand their ability to gather and assess information related to the interoperability of systems under their oversight. It also provides recommendations to enhance their collaboration with Programs and partners and to identify opportunities for acquiring improved interoperability information.

B. Report Organization

This report provides background information on interoperability in Chapter 2, information IDA collected from the DTE&A Action Officers in Chapter 3, the information obtained from the Interoperability Steering Group (ISG)¹ in Chapter 4, the DTE&A interoperability process and considerations for improvement in Chapter 5, interoperability resources for Action Officers in Chapter 6, and final thoughts and future considerations in Chapter 7. Appendix A offers additional details on the Joint Interoperability Certification (JIC) process.

C. Methodology

The study began with phone interviews of 12 DTE&A Action Officers spanning various warfare areas (Air, Land, Missile Defense, Naval, Space, and Nuclear Command, Control, and Communications (NC3)) to gain insight into processes and challenges associated with assessing system interoperability. These challenges were then presented to the ISG to explore potential mitigation strategies. The ISG members offered valuable context, guidance, and documentation, which will directly benefit the Action Officers and their assessment of interoperability.

¹ You can find more information on the ISG and its activities on their website:
<https://jitc.fhu.disa.mil/projects/isgsite/pubs.aspx>

(This page is intentionally blank.)

2. Background

A. DoD Interoperability Policy

The Department of Defense Instruction (DoDI) 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS) [1] defines Interoperability to be

The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment in its operational environment including appropriate cybersecurity aspects.

Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions in appropriately stressed operational environments over the system's life-cycle.

Developing interoperable systems within the DoD involves multiple organizations at various levels and necessitates coordination, cooperation, and collaboration. To oversee and facilitate this effort, the ISG was established in accordance with DoDI 8330.01. The ISG is tri-chaired by DoD Chief Information Officer (CIO), USD (A&S), and Joint Staff (JS) J6.

The primary mission of the ISG is to promote interoperability in systems possessing IT/NSS capabilities or those that must function within the defense IT/NSS environment to fulfill the mission-critical requirements of joint and combined operational commanders. The ISG achieves these objectives through a formal process dedicated to identifying and resolving critical IT/NSS interoperability policy and process issues. [2]

Joint Interoperability (JIO) refers to the ability of IT systems used by different Services or Agencies to interoperate effectively, whether they belong to DoD or non-DoD entities. Joint Interoperability Test Command (JITC) serves as the certification authority for JIO of systems, which is integral to the satisfaction of a Net-Ready Key Performance Parameter (NR-KPP).² According to DoDI 8330.01, JIO requirements encompass "any requirement levied on an IT to implement information exchanges to other IT across or beyond a Military Department's (MILDEP's), a Combatant Command's (CCMD's), Defense Agencies' and DoD Field Activities'

² "The Net-Ready KPP assesses the net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. It evaluates information needs, information timeliness, Information Assurance (IA), and net-ready attributes." [3]

(DAFA's), and an OSD Component's boundaries or implement a web service with the explicit or implicit intention to share information with other IT across or beyond their boundaries."³

It is worth noting that, as per the current interpretation, only JIO requirements rise to the level of a KPP, while requirements for other types of interoperability do not.

B. Joint Interoperability Certification

Before a system can be certified as interoperable, it must undergo two crucial certifications. The first is called Net-Ready Certification. It identifies that the system requirements specify JIO (i.e., include a Joint Performance Requirement (JPR)) and therefore demand a KPP, which will encompass all specified and derived JIO requirements encapsulated within the Program's architecture products. This certification process for JIO requirements is overseen by the JS J6, which functions as the Net-Ready Certification Authority as outlined in the Joint Capabilities Integration and Development System (JCIDS) Manual and DoDI 8330.01 for all IT systems with Joint, multinational, or interagency interoperability. The J6 works closely with the Program Manager to ensure all JIO requirements are comprehensively documented, using the various architecture views and products specified in JCIDS (Chairman of the Joint Chiefs of Staff instruction 3170.01) and the JCIDS Manual. [9] The details of the process can be found in the J6 publication *NR-KPP and Interoperability Smart Book*, 13 April, 2023. [4] Within this document, the J6 offers specific guidance on the preparation, format, content, submission timelines, and review procedures related to the Net-Ready (NR) Performance Attribute (PA) and Key Performance Parameter (KPP).

- NR is a mandatory PA, required by both the JCIDS Manual and DoDI 8330.01.
- The NR PA requires interoperability between individually developed and fielded capability solutions.
- If a Program of Record (PoR) has a JPR (i.e., joint interfaces or joint information exchanges with other IT), the PA is elevated to a KPP, through Net Ready Certification.
- NR Certification by the J6 essentially means that the interoperability requirements are sufficiently understood and documented, and that if the system can meet these requirements it will be able to achieve the intended interoperability objectives.
- NR Certification serves as a prerequisite to the Defense Information Systems Agency (DISA) JTC JIC.

³ Of note, this definition does not restrict the requirement to just DoD-only interfaces. This is reflected in the fact the Interoperability Process Guide (IPG) v3 states that "joint interfaces or joint information exchanges with other IT... requires JIC", and "A joint interface is an interface between/among external partners", and defines External Partner as "another DoD Component, U.S. Government Department or Agency (including federal, state, and local), Coalition partners, non-governmental organizations, or any combination thereof that utilize the same interfaces and/or exchange information produced/consumed/shared or distributed by the IT." [5]

The second interoperability certification, JIC, is intended to certify that the system under evaluation/assessment can effectively perform JIO functions in accordance with the NR-KPP. JITC is the designated joint interoperability certification authority for all DoD IT systems with JIO requirements, as specified in DoDI 8330.01. The certification process involves a great deal of planning, testing, and evaluation prior to receiving JIC. The process is described in depth in the *Interoperability Process Guide (IPG) VER 3.0, July 2023*. [5] Additional information on interoperability certification can be found in Appendix A of this report.

C. Motivation for Testing Interoperability in Developmental Test (DT)

The U.S. military must make decisions and act more quickly than its opponents. This demands that its systems and personnel can effectively collaborate to support their missions. This is particularly critical as systems become increasingly automated, requiring thorough checks to ensure that all interactions occur seamlessly.

Interoperability testing has traditionally leaned toward being operationally realistic. This approach is favored because decision-makers want assurance that critical interactions between systems and Services haven't been overlooked during development. It's important to note that simply adhering to a set of standards doesn't guarantee interoperability; it must be meticulously planned and tested to ensure success. It is tempting for developers and Programs to prioritize making their systems functional, but interoperability testing with other systems can easily become an afterthought. Neglecting fundamental design considerations necessary for a system to interoperate with its counterparts can lead to costly redesign efforts, even if detected early in the DT phase.

Interoperability is also challenging to establish because it demands alignment between systems, personnel, Concept of Operations (CONOPS), and Tactics, Techniques, and Procedures (TTPs), all in sync with the intended mission. Furthermore, the multitude of systems in the field that a new system must interoperate with are continually undergoing patches, upgrades, and replacements. This results in a highly heterogeneous environment and numerous opportunities for unplanned configuration inconsistencies. This complexity underscores the risk to interoperability and argues for testing throughout the development process to mitigate unforeseen issues and the associated delays.

D. Interoperability Testing in DT

JITC conducts evaluations of JIO using operationally representative systems in operationally representative environments. Identifying opportunities to collect operational test (OT) interoperability data can be challenging due to limited test asset availability. JITC therefore often must gather data from exercises and other opportunistic events. Typically, this occurs toward the end of DT when more mature and operationally representative test components are available. Since testing in an operational environment is costly, these tests primarily focus on collecting OT JIO data rather than DT data intended for aiding system development. Services are responsible for

gathering intra-Service (non-JIO) interoperability data, but they don't always share the test details with DTE&A Action Officers. JTC has strong partnerships with the Service test agencies that help collect and share the JIO data.

The current approach to interoperability testing, as viewed by the OSD, emphasizes certifying systems as having achieved JIO status. However, before these systems can be certified for JIO, they must undergo design and development phases. The Program Management Office's (PMOs) willingness to share DT interoperability test planning and results is a major factor in DTE&A's Action Officer's ability to assess interoperability progress and risk. Testing system components as they mature during DT is essential to ensure they are ready to support eventual system interoperability. This proactive approach helps guide development for more successful OT outcomes. Similar to cybersecurity, waiting until the design is complete and OT results are available is a costly way to identify and address interoperability issues. Nevertheless, conducting interoperability testing with communicating systems before the fully developed system is available presents practical challenges and may have limited scope.

E. Current DTE&A Guidance

DTE&A Action Officers receive little explicit guidance or formal training for assessing system interoperability. Instead, they rely on a combination of resources, including the language of the KPPs, the overarching process outlined in DoDI 8330.01, any Service-specific guidance, and advice from fellow Action Officers and testers to navigate their interoperability evaluation responsibilities.

3. DTE&A Action Officer Observations

During phone interviews with 12 DTE&A Action Officers, IDA identified several recurring themes. Additionally, IDA gathered observations specific to Action Officers' respective warfare areas (Air, Land, Missile Defense, Naval, Space, and NC3). Many of the Action Officers IDA spoke to had extensive experience in their roles, spanning both DTE&A and prior test and evaluation (T&E) positions. This allowed them to offer insight based on decades of experience, providing a longitudinal perspective on the effectiveness of various aspects of interoperability evaluation. It is crucial to note, however, that these observations are anecdotal and should be seen as indicators of potential issues within the interoperability evaluation process, rather than definitive conclusions.

The main themes highlighted by the Action Officers include:

1. Interoperability testing isn't given high priority by many of the Action Officers, leading to limited involvement in interoperability test planning, test events, or the examination of test data. Instead, the Action Officers depend on JITC-planned testing, and leverage strong relationships and coordination with Director, Operational Test and Evaluation (DOT&E) Action Officers, who have better access to data and ample support. Even if the Action Officers had the time to participate in test planning and execution, approved scenarios and system mission requirements are not always readily available, and interoperability requirements are often ambiguous and lack clarity.
2. Action Officers hold varying understandings of how interoperability should be tested. Some believe that JITC is proficient in its responsibilities and thus the Action Officers should only involve themselves in test details if issues that could impact the schedule arise. Consequently, in certain warfare areas, Action Officers consider "interoperability" to align with JITC's determination, while others equate it primarily with platform integration. A few Action Officers have embraced the notion that interoperability encompasses all aspects necessary to accomplish the mission, while others have not ventured beyond viewing it as ensuring reliable communication pathways. Few differentiate between DT interoperability data, OT interoperability data, and OT JIO data (the focus of JITC assessments).
3. Some Action Officers recognize the value of getting involved earlier in the process to steer Programs in the right direction, and a few manage to find the time to do so. They emphasize that system developers need a deeper understanding of how the system will be utilized, and they stress the importance of securing early feedback from users.

Although some Programs may postpone interoperability testing until integration testing or until the latest system version is available just before OT, those Programs that prioritize it seem to do so due to either Program Executive Office (PEO) enthusiasm or due to interoperability specific system requirements (beyond an NR-KPP). One Action Officer asserted that, unless interoperability testing is deliberately planned and adequately funded in the contract, it is unlikely to be executed effectively.

4. PEOs for various Programs employ different approaches when acquiring different types of systems, each with its unique interoperability considerations. Some Programs prioritize extensive laboratory testing, while others dedicate significant time to field testing. Some choose to integrate already-proven subsystems, while others merge interoperability testing with integration testing. This diverse approach stems from the recognition that the system's mission context plays a crucial role in determining the adequacy of its interoperability. Ultimately, a Program's commitment to ensuring interoperability stands out as the most critical factor in achieving interoperability goals.
5. Action Officers lack compelling success stories to encourage Programs to prioritize interoperability in their designs. This is a challenge because achieving interoperability is more complex than it may initially seem; even when Programs emphasize interoperability as a core system requirement, they often encounter significant difficulties in achieving it. Several Action Officers agreed that achieving interoperability between systems is simply challenging and should be treated as such.
6. There are well-known features of the Acquisition system that contribute to creating interoperability problems.
 - a. Military systems, missions, and environments are constantly changing, with cybersecurity threats and the interoperability landscape evolving at a much faster pace than system development cycles. System requirements are typically not defined to address these rapid changes. As technology advances, missions and systems become increasingly complex, posing challenges for integrating legacy systems that were not originally designed to accommodate the desired level of interoperability. Additionally, our military systems are vast, dispersed, come in various configurations, and cannot be updated simultaneously or quickly. This situation necessitates a significant degree of backward compatibility and makes it challenging to find opportunities for testing these systems outside of exercises.
 - b. Contractors have little incentive to voluntarily disclose details about their products or share test reports unless specified in the contract. This lack of transparency fosters opportunities for misunderstandings and miscommunications between developers, resulting in interoperability issues. Even when two systems are being developed concurrently, interfaces

between them may suffer from what can be likened to a "tragedy of the commons"⁴ if contractors are not adequately motivated to ensure their interfaces work seamlessly. Without a centralized authority overseeing these interfaces, contractors may push the responsibility for making necessary changes. Similarly, Programs may not be incentivized to share valuable lessons learned, even within their own service branches, as any issues may be perceived as detrimental to the PMO's reputation.

- c. Systems are developed at different times and rates, making it challenging to synchronize changes for each interaction. Programs also tend to prioritize "must-have" characteristics, such as performance, effectiveness, and survivability, to secure approval for fielding. This focus on non-negotiable attributes often leaves more flexible characteristics that could be addressed after fielding overlooked.

⁴ A "tragedy of the commons" is a metaphoric label for a concept that is widely discussed in economics, ecology and other sciences. According to the concept, should a number of people enjoy unfettered access to a finite, valuable resource, they will tend to over-use it, and may end up destroying its value altogether. To exercise voluntary restraint is not a rational choice for individuals—if they did, the other users would merely supplant them—yet the predictable result is a tragedy for all. [6]

(This page is intentionally blank.)

4. ISG Observations

The members of the ISG initially did not fully understand why the DTE&A Action Officer's were so interested in the OT JIO test data. Nevertheless, they were highly receptive to involving DTE&A in the JIC process. The ISG staff observed that, even within the JIC process, there was a lack of sufficient visibility with Programs. The ISG staff also noted that Programs often inquired about certification when the DT phase was nearly concluded.

Observations made by the ISG about JIC include:

1. The interoperability definition in DoDI 8330.01 specifies that the mission environment encompasses "appropriate cybersecurity aspects," indicating that operationally representative test environments should likewise be considered. Accordingly, it is vital that tests are planned from an enterprise perspective, aiming to encompass as much of the System-of-Systems (SoS) aspect as possible and striving to assess the interoperability (as well as performance) of as many operationally-representative systems when they are operating together as feasible. Although assembling numerous and disparate systems for testing can be a challenge, it offers a more efficient utilization of range time and provides the best means to observe complex dependencies and failure modes. Naval Sea Systems Command (NAVSEA) is already taking steps to connect laboratories across the country to facilitate interoperability testing in this manner.
 - a. NAVSEA has expressed interest in exploring potential coordination with USS SECURE⁵ to integrate interoperability and cyber testing.
 - b. JITC is increasingly relying on Software Integration Lab (SIL) testing, with more labs becoming available. However, they lack an authoritative directory of SILs and other applicable labs.
 - c. JITC is incentivized to conduct a greater portion of its JIO testing during OT events where cybersecurity red teams are actively operating, making the test environment more representative of operational conditions.
2. JITC provides comments on the Department of Defense Architecture Framework (DoDAF) architecture submitted by a Program to the ISG. This collaborative effort assists JS J6 and the Program in building the KPP table. Similarly, the ISG has the

⁵ "USS SECURE is a multi-enclave test environment that enables the Navy's development, evaluation and testing of cyber security concepts and technologies to defend mission critical systems at sea and ashore." [7]

capability to grant DTE&A early access to Program submissions, allowing for timely input.

- a. The incorporation of practical mission considerations into draft architectures during the early engagement phases with the Program, followed by the dissemination of these architectures to contractors, improves the existing JIC capability to ensure that essential JIO aspects are addressed in JITC testing.
3. JITC faces challenges in being included early in the test planning process, primarily due to their funding structure (cost-reimbursable by PMOs). Moreover, JITC won't complete the JIO test planning until the architectures are finalized and the Program achieves NR Certification, often leading to lengthy delays.
 - a. It would be beneficial for DTE&A Action Officers to gain an understanding of JITC's preliminary interoperability test plans and their perspective on the necessary OT testing for each Program. This way, DTE&A can ensure that the foundations to system interoperability are being developed and validated during the DT phase.
 - b. Successful Programs are able to make rapid revisions to their architectures which allows JITC to initiate JIO test planning even before significant progress is made in the DT phase.
4. Approximately a quarter of the Programs that consult the ISG discovered it through informal channels, such as word-of-mouth, rather than from official Service guidance or checklists.
 - a. It is imperative that each Service designates a responsible party to ensure that engaging with the ISG and initiating the JIC process early becomes an integral part of their standard operating procedures. This practice should be explicitly incorporated into their internal regulations and guidance. The instructions should outline what Programs should anticipate, including typical timelines, and detail what must be submitted to the ISG and JITC to successfully complete the JIC process.
5. It is extremely important to include a clear requirement for achieving JIC using the JIC process within Requests for Proposals (RFPs) and contracts with development contractors. This ensures that JIC is adequately funded and planned for, a practice that is still lacking in many cases, despite the expectation that PMOs should be knowledgeable about the JIC requirement and process.
 - a. Attempts to field a SoS without a comprehensive understanding of their requirements, or without a coherent set of requirements, often encounter interoperability issues.

- b. JITC and the ISG also engage in the JIC process for non-Acquisition Category (ACAT) I Programs and aid Programs lacking a JPR for interoperability testing. For example, many ACAT II and ACAT III Programs do not have OT requirements for interoperability, but JITC will still review test data and certify them at their request.⁶
 - c. Regarding interoperability with foreign and coalition forces, it is rare to encounter a coalition interface that differs from a required U.S. Joint interface already considered in the JIC process. Any explicit JS-certified requirements for an external interface with a foreign system will undergo JITC evaluation, similar to any other JIO requirements.
6. The primary objective of the JIC process is to provide critical information to fielding authorities. However, it appears that the Services and CCMDs are not thoroughly reviewing the caveats in JIC reports and may not fully grasp the level of interoperability to which their systems are certified.
7. Performing interoperability testing during the DT phase holds immense value, as identifying interoperability issues during OT often comes too late and results in substantial costs for remediation. Nevertheless, conducting interoperability testing during DT before the fully developed system is available presents practical challenges and may have limited scope.

The JS and JITC provided documentation to the IDA team outlining their approaches to addressing interoperability T&E (see Chapter 6). These approaches could potentially be adapted for use by DTE&A.

⁶ There are three Acquisition Categories (ACAT): ACAT I, ACAT II, and ACAT III. ACAT I Programs have the highest level of oversight, with ACAT II and ACAT III Programs having decreasing levels of oversight. The difference between each category is dependent on the location of a Program in the Acquisition Process, funding amount for Research, Development, Test and Evaluation (RDT&E), total procurement cost, Milestone Decision Authority (MDA) special interest, and decision authority. [8]

(This page is intentionally blank.)

5. The DTE&A Interoperability Evaluation Process and Considerations

The aforementioned challenges in building and testing interoperability for DoD systems suggest that a substantial, transformative shift may be necessary to ensure interoperable systems right from the outset. The required steps are a topic for another discussion, but there may be some immediate, albeit limited, avenues that DTE&A and the broader T&E community can take to influence and enhance interoperability.

The main approach that DTE&A Action Officers can adopt to foster the development of interoperability is to offer early feedback on derived interoperability requirements and test budgets, ensuring their adequacy. This can be accomplished through direct engagement with Programs and through DTE&A assessments. Additionally, DTE&A can play an important role in guiding DT plans to effectively capture interoperability-related issues and provide timely feedback to contractors and Programs, thus expediting the resolution of interoperability challenges. To that end, a conceptual DTE&A interoperability evaluation process and a set of suggestions and advice for improving this process are provided below.

A. Conceptual DTE&A Interoperability Evaluation Process

The following is a summary of recommended steps that DTE&A could follow to assist in assessing and evaluating system interoperability before OT. Additional details are provided in Appendix A.

1. DTE&A Organization

1. Identify newly initiated Programs under development that are likely to have interoperability requirements.
2. Monitor the ISG discussions and documents to stay informed of when new Programs have started the JIC process.
3. Ensure that Programs with interoperability requirements are promptly assigned to DTE&A Action Officers to oversee interoperability progress and manage associated risks from the outset.

2. DTE&A Action Officers

1. Establish effective working relationships with key PMO personnel, such as the Chief Engineer, Chief Tester, and other team members knowledgeable about interoperability requirements and development progress.
2. Acquire a thorough understanding of the system's mission, design, and interoperability requirements. Review interoperability architecture products as they become available and seek clarity on any unclear requirements in the context of the mission. The JS J6 may be helpful in assisting in this effort.
3. Encourage Programs that are delaying or under-resourcing interoperability testing to allocate sufficient resources for comprehensive interoperability testing.
4. Evaluate the contractors' understanding of both stated and derived interoperability requirements. In cases involving multiple Programs, assess whether contractors from all Programs are collaborating effectively.
5. Review the interoperability data collected during Contractor Testing and DT, if available. Provide constructive recommendations to PMO contacts for potential improvements in interoperability design and test.
6. Keep DTE&A management informed about significant interoperability development challenges identified and recommend strategies to mitigate interoperability Program risks.
7. Elevate the importance of interoperability as a special area of interest during Program reviews, design reviews, Independent Technical Risk Assessments (ITRAs), and all interactions with PMO personnel and contractors. Emphasize that interoperability Program risks can be substantial, warranting special attention.

B. Considerations for DTE&A Interoperability Involvement

The IDA team did not formally prioritize the above steps for potential impact on system interoperability. However, the team suspects that collaborating with Programs early on to derive comprehensive and testable interoperability requirements, which extend beyond JIO and involve DOT&E and JITC, could be one of the most valuable and cost-effective initiatives. Such an effort would naturally lead to considerations of budgeting, test planning, and data sharing. Secondly, actively participating and providing feedback on DT planning could aid in the early detection of interoperability issues. In essence, interoperability should undergo assessment in a manner similar to any other KPP, regardless of whether it is explicitly mentioned.

To gain insights into the challenges faced by Services in ensuring system interoperability, DTE&A could gather data related to the status of JIC. Simplified, easily collectible data could help identify significant disparities in interoperability development among different types of systems,

allowing for trend analysis over time. This information could also pinpoint areas where Action Officers could provide more effective assistance to specific Programs or types of Programs.

For a more comprehensive understanding of the interoperability of the fielded force, additional data elements would be required, including the nature of the systems' missions, interoperability issues discovered during operationally-representative testing, and the Programs' strategies for interoperability development. However, gathering this information for a substantial portion of the fielded force would be time-consuming. To swiftly identify interoperability issues, a more immediate approach would involve systematic engagement with operators and a review of field reports.

(This page is intentionally blank.)

6. Interoperability Resources for DTE&A

This section provides a list of reference materials, each accompanied by a brief description of its contents and often a URL for easy access. This list is intended to serve as a practical desktop reference tool, aiding DTE&A Action Officers in effectively carrying out their oversight and support responsibilities for Programs in development. Action Officers can refer to the resources in this section to enhance their understanding of interoperability processes, roles, and responsibilities. Additionally, these references can provide insights into the progress of Programs in their interoperability development stages.

A. Data

JIT (JITC Industry Toolkit) - <https://jit.fhu.disa.mil>

JITC has accumulated a repository of interoperability issues observed over the years, including those they believe could have been detected during the DT phase. Becoming familiar with these patterns of acquisition failure can prove valuable for identifying or anticipating issues in new systems. The following is the description given for JIT at <https://jitic.fhu.disa.mil/organization/serviceCatalog/tools/index.aspx> : “The JITC Industry Toolkit (JIT) provides high speed access to key interoperability information. The heart of the system is an extensive data repository featuring the JITC Lessons Learned Reports, JITC Test Reports, the North Atlantic Treaty Organization (NATO) Interface Guide, Joint Interoperability Certification Letters, and other interoperability documents and references; as well as a high-speed search engine to quickly access data. This tool gives a quick and easy on-line capability which identifies system/equipment characteristics, tested configurations and practical "how-to" information to facilitate Interoperability.”

Global Information Grid Technical Guidance Federation (GTG-F) Joint Interoperability and Supportability Assessment Module (IAM)

Request GIG-F 1.18.9 access at <https://gtg.csd.disa.mil/>

Request GIG-F 2.0 access at <https://jasm.apps.mil/prweb/PRWebLDAP1/>

Link: https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance/IAM

Programs that follow the Information Support Plan (ISP) process utilize the GTG-F IAM system to share architecture documents that are used to assemble their ISP. Within this framework, JITC personnel and other ISG members use the GTG-F IAM to offer feedback on these documents. It has not been established whether these documents are maintained and updated within the GIG-

F IAM throughout the system's development process, or if the final version of the system architecture is directly supplied to JITC and DOT&E.

For access to a specific Program's ISP documentation, it may be necessary to request access either from JITC or the Service sponsor within the ISG.

**Knowledge Management/Decision Support (KM/DS) system -
<https://jrockmdsbpm.js.smil.mil> (on Secret Internet Protocol Router Network (SIPRNet))**

Programs that follow the JCIDS process use the Knowledge Management/Decision Support (KM/DS) system to share their acquisition documents with the ISG. These documents include the Initial Capabilities Document (ICD), Capability Development Document (CDD), and Capability Production Document (CPD). JITC personnel use the KM/DS system to access and provide feedback on these documents.

To access a specific Program's ISP documentation, it may be necessary to request access directly from the Program.

System Tracking Program (STP) - <https://stp.jitc.disa.mil/>

JITC personnel use STP to store and analyze information concerning the systems, including their interoperability test data. It is not expected that JITC will grant automatic access to Action Officers, so obtaining data from this system will likely require making specific requests to JITC.

Joint Interoperability Certification (JIC) Reports

“JITC distributes interoperability information via the JITC Electronic Report Distribution system.”⁷

JIC reports for similar systems, previous iterations of a system, or systems with which a new system must achieve interoperability can offer valuable insights. This information may include details on interoperability challenges encountered by the system, any limitations noted in the certification process for which mission requirements were not successfully certified, and estimates regarding the timeline for obtaining an Interim Certificate to Operate (ICTO) or full certification.

DAVE (Defense Acquisition Visibility Environment) - <https://dave.acq.osd.mil/> or <https://advana.data.mil/#/> (Advana pulls data from DAVE, and is available to DTE&A)

DAVE (Defense Acquisition Visibility Environment) serves as an extensive repository of acquisition-related information for Programs. Action Officers can also leverage Advana to conduct in-depth analysis of DAVE data. The official description of DAVE, available at <https://www.acq.osd.mil/asda/ae/ada/pd-ada.html>, outlines its significance as follows: “The

⁷ 28 December 2022 JITC Memorandum, at https://jitc.fhu.disa.mil/tssi/cert_pdfs/Aruba_HPE_7000-7200_9000-9200_WLAS-WAB_ArubaOS_8-10_TN1805302_DTR7_22MAR2023.pdf

Defense Acquisition Visibility Environment (DAVE) is the authoritative source for Acquisition Program Baselines, as well as unit cost/schedule/performance/contracts data required for DoD and Congressional insight. DAVE is the central point for Acquisition data for the Department of Defense. Resources available through DAVE include tools for statutory and regulatory reporting, data and capabilities for Program and portfolio analysis, and technical resources for data consumption via application program interfaces. Key capabilities include: ... Program Submissions, ... Acquisition Information Repository, ... Acquisition Data Sets, ... Data Analytics Enablement.”

DOT&E Annual Reports - <http://www.dote.osd.mil/annualreport/>

DOT&E Annual Reports can provide insight into system missions, current status, and developmental challenges. Although interoperability problems are not always explicitly categorized as such, these reports frequently highlight performance and developmental issues that have the potential to lead to interoperability challenges.

ISG Annual Reports - <https://jitc.fhu.disa.mil/projects/isgsite/pubs.aspx>

ISG annual reports serve as valuable resources that identify specific interoperability issues encountered by Programs. They are essential references for current systems in the certification pipeline, previous iterations of those systems, and other systems requiring interoperability with the current one. Additionally, these reports offer detailed descriptions of the JIC and ISG processes.

Selected Acquisition Reports (SARs) - https://www.esd.whs.mil/FOIA/Reading-Room/Reading-Room-List_2/Selected_Acquisition_Reports/

SARs offer insights into the evolving aspects of Major Defense Acquisition Programs (MDAPs), including their cost, schedule, and performance. These reports include essential information such as the system's Mission and Description, Threshold Breaches, Schedule, Performance, Cost and Funding, Production, Foreign Military Sales, and Contracts. Furthermore, SARs provide a comprehensive life cycle cost analysis of the Program and all its increments.

SARs are useful for getting an overview of a Program or assessing the historical performance of similar Programs. Accumulating SARs for systems that must be interoperable with a specific system can assist analysts in determining the most likely timeline for completing interoperability tests and certification.

These reports are issued on an annual basis, with critical updates provided through quarterly "exception" SARs. SAR information can be supplemented with corresponding Defense Acquisition Executive Summary (DAES) reports, which receive monthly updates. Access to SARs and DAES reports is available through DAVE.

B. Procedures

1. JITC

Interoperability Process Guide (IPG) -

https://jitic.fhu.disa.mil/isg/downloads/IPG_Version_3_Final_signed_20230703.pdf

The IPG outlines the overall process used by JITC to certify systems for Authority to Operate (ATO). This documentation includes the involved organizations and their respective information requirements. Recently, Version 2 Change 1 has been replaced by Version 3, which incorporates valuable appendices for further assistance and clarity.

JITC Test and Evaluation Guide: Architectures for Joint Interoperability Test, Evaluation, and Certification - https://jit.fhu.disa.mil/isg/download/TE_Guide-Architectures_for_Joint_Interoperability_FINAL_8_Mar_23_signed.pdf

This JITC Guide describes the DoDAF architectural views that are valuable for test planning and the assessment of system interoperability.

2. Joint Staff

NR-KPP and Interoperability Smart Book -

[https://jitic.fhu.disa.mil/isg/downloads/JS_J6_NR-KPP_and_Interoperability_SMART_BOOK-April_2023_\(final\).pdf](https://jitic.fhu.disa.mil/isg/downloads/JS_J6_NR-KPP_and_Interoperability_SMART_BOOK-April_2023_(final).pdf)

JS J6 has prepared this shareable version of the document used for training NR-KPP assessors responsible for reviewing Program ISPs.

C. Organizations

ISG (Interoperability Steering Group) - <https://jitic.fhu.disa.mil/projects/isgsite/index.aspx>

The ISG plays a vital role in assisting Programs with the identification of JIO test requirements and the issuance of Interim Certificates to Operate (ICTO). The ISG meets regularly, and coordinates with Service representatives serving as the Points of Contact (POCs) for the Programs. The ISG has three Tri-Chairs, from the Office of the Undersecretary of Defense (OUSD) (A&S), DoD CIO, and J6.

The ISG operates in accordance with the documented procedures outlined in the DoD IPG, ensuring the execution and enforcement of DoDI 8330.01. Furthermore, it compiles an Annual Report detailing the ISG's actions over the Fiscal Year, offering an invaluable reference for gaining insight into relevant system interoperability matters.

The ISG Site provides convenient access to various pertinent documents (including those mentioned above), alongside information about ISG actions and meeting details.

JITC (Joint Interoperability Test Command) - <https://jitc.fhu.disa.mil/>

JITC is responsible for certifying systems for JIO, in accordance with DoDI 8330.01. Its personnel assist Programs with devising strategies to gather the requisite interoperability test data from operationally-representative systems and analyzing it to certify systems as compliant with their JIO requirements. They serve as a valuable resource for gaining insights into Programs and to coordinate the collection of DT interoperability data with their OT interoperability data collection efforts to avoid conflicts.

Joint Staff (JS) - <https://www.jcs.mil/Directorates/J6-C4-Cyber/>

The JS sets system requirements through the Joint Requirements Oversight Council (JROC), including for JIO. JS J6 participates in the ISG.

DoD CIO - <https://dodcio.defense.gov/>

The DoD CIO sets relevant interoperability policy and participates in the ISG.

DOT&E - <https://www.dote.osd.mil/>

DOT&E helps JITC plan for collecting the necessary OT interoperability test data.

(This page is intentionally blank.)

7. Final Thoughts and Future Considerations

The focus of this study was the activities of the DTE&A Action Officers and ISG members, primarily centered around JIO. IDA has identified opportunities for improving the evaluation of system interoperability by Action Officers. These include gaining a better understanding of requirements for interoperability, knowing the processes involved in JIC, taking advantage of IOSG engagement with Programs, and becoming more familiar with Service and JITC interoperability test procedures. Such knowledge can enhance Action Officer's ability to understand how particular tests are planned, the availability of the produced data, and the most effective methods of interpretation.

It is evident that interoperability is a context-dependent characteristic, depending greatly on factors such as the availability of other systems for a mission, the CONOPS and TTPs used in mission execution, as well as the broader operational environment in which the mission takes place. This raises important questions about the extent of interoperability required among the systems and personnel involved in a mission to attain the desired level of performance and success.

Furthermore, it leads to consideration of the tradeoffs that need to be made in system design, as opposed to addressing them at the time of the mission. These tradeoffs encompass issues such as system flexibility, cost, speed of operations, information security, and the alignment of operations with mission partners. DoD must consider whether it can afford to wait for the development and testing of such adaptable systems. Additionally, DoD must ponder the degree of flexibility and upgradability required for its systems to maintain interoperability throughout their Service lives, especially within a rapidly changing battlespace where predicting operational environments is fraught with uncertainty.

The nature of the military's expectations regarding system interoperability and the practicality of implementing these expectations warrant discussion with the Services. It is crucial to develop a clear and comprehensive description of system interoperability that addresses the continuum of options for when, where, and to what extent systems can effectively collaborate.

Setting aside larger institutional changes that might be needed, immediate actions that DTE&A could take include:

- Educating the ISG about DTE&A's roles and responsibilities to enhance understanding and collaboration.
- Coordinating with the ISG to ensure that DTE&A Action Officers understand interoperability requirements and certification processes.

- Providing clear guidance to Action Officers on how to prioritize interoperability test planning and assessments.
- Exploring the possibility of establishing an Interoperability and Early DT of Interoperability seminar series or a short course tailored specifically for Action Officers.

These steps could enhance the effectiveness of DTE&A interoperability efforts within the organization and improve overall interoperability outcomes.

Appendix A. Joint Interoperability Certification Process Details

The key stakeholders responsible for defining the requirements, designing, and certifying an IT Program's JIO are the OUSD A&S, the DOD CIO, the PMO, and JITC.

The JS J6 collaborates closely with the Program Manager to ensure that all JIO requirements are comprehensively documented. Detailed procedural information can be found in the J6 publication *NR-KPP and Interoperability Smart Book*. [4] Within this document, the J6 offers specific guidance concerning the preparation, format, content, submission timelines, and review process for the Net-Ready PA and KPP.

Ultimately, the JS J6 serves as the primary advocate for the DoD and its CCMDs in matters related to IT Interoperability. The J6 holds the role of the Net-Ready Certification Authority, as defined in the JCIDS Manual and DODI 8330.01, for all IT systems with Joint, multinational, or interagency interoperability requirements. [9, 1] The J6, OUSD A&S, and DoD CIO jointly chair the ISG, with support from DISA JITC. Additionally, the J6 assists the DoD CIO in ensuring that JIO requirements and related architectures in Information Support Plans (ISPs)⁸ are adequate.

The overarching process can be summarized as follows:

1. A Program identifies the existence of a JIO requirement, often represented as a Net Ready KPP, and initiates contact with the ISG.
2. The ISG advises the Program regarding the interpretation of these requirements.
3. JITC assists the Program in planning ahead for thorough interoperability testing.
4. Both the Program and JITC collaborate to gather the necessary test data.
5. JITC reviews the collected data and certifies whether the system has met the criteria for JIO.
6. The ISG evaluates the JITC certification and, upon approval, grants an ATO to the Program.

⁸ An ISP describes a systems dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The ISP is required for all ACAT Programs that connect in any way to the communications and information infrastructure including both IT and NSS Programs. The ISP is summarized in the Acquisition Strategy and reviewed at Milestones B and C and is prepared concurrently and collaboratively with the CDD or CPD. [10]

This process and additional details are illustrated in Figure 2.3 of JITC's *Interoperability Process Guide*, which is reproduced here, in Figure 1. [5]

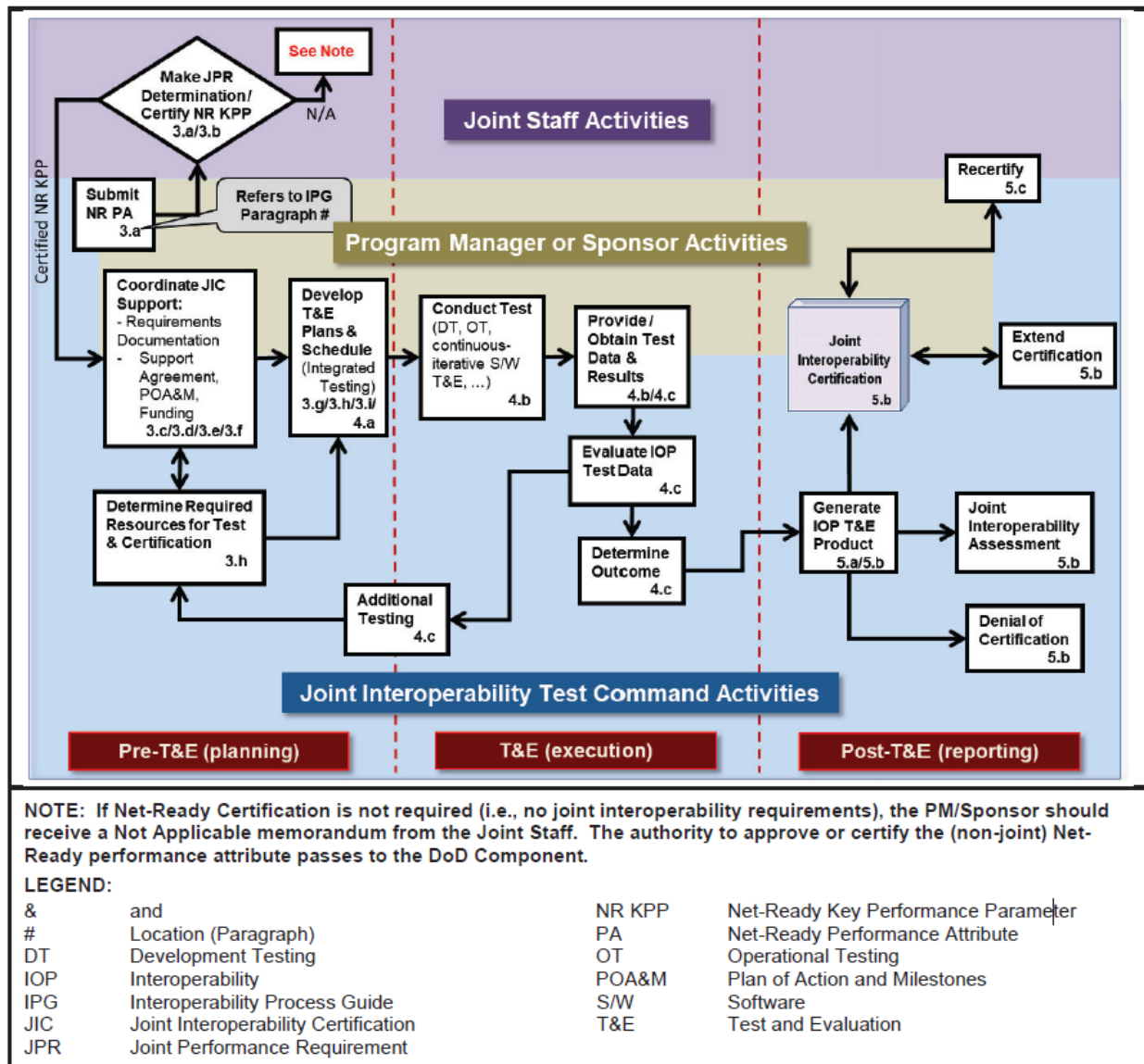


Figure is reproduced from figure 2-3 in [5].

Figure 1. Notional Joint Interoperability Certification Process

Appendix B. Acronym List

ACAT	Acquisition Category
A&S	Acquisition & Sustainment
CCMD	Combatant Command
CIO	Chief Information Officer
CONOPS	Concept of Operations
DAFA	Defense Agencies and DoD Field Activities
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDI	Department of Defense Instruction
DT	Developmental Test
DOT&E	Director, Operational Test and Evaluation
ED, DTE&A	Executive Director, Developmental Test, Evaluation, and Assessments
IA	Information Assurance
ICD	Initial Capabilities Document
ISG	Interoperability Steering Group
IT	Information Technology
ITRA	Independent Technical Risk Assessment
JCIDS	Joint Capabilities Integration and Development System
JIC	Joint Interoperability Certification
JIO	Joint Interoperability
JITC	Joint Interoperability Test Command

JPR	Joint Performance Requirement
JS	Joint Staff
MILDEP	Military Department
NAVSEA	Naval Sea Systems Command
NC3	Nuclear Command, Control, and Communications
NR-KPP	Net Ready Key Performance Parameter
NSS	National Security Systems
OUSD	Office of the Undersecretary of Defense
OT	Operational Test
PA	Performance Attribute
PEO	Program Executive Office
PMO	Program Management Office
POC	Point of Contact
PoR	Program of Record
RDT&E	Research, Development, Test and Evaluation
RFP	Request for Proposals
R&E	Research and Engineering
SIL	Software Integration Lab
SIPRNet	Secret Internet Protocol Router Network
SoS	System-of-Systems
T&E	Test and Evaluation
TTP	Tactics, Techniques, and Procedures

Appendix C. References

- [1] Department of Defense Instruction 8330.01, “Interoperability of Information Technology, Including National Security Systems,” 27 September 2022.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/833001p.pdf?ver=c7Bds_aCFKSe7SK_MiYBIg%3d%3d
https://jitc.fhu.disa.mil/isg/downloads/833001p_Signed_Rewrite_27_SEP_2022.pdf
- [2] Department of Defense Interoperability Steering Group, “FY22 Annual Report,” 5 Jul 2023.
[https://jitc.fhu.disa.mil/isg/downloads/FY22_ISG_Annual_Report_FINAL_\(as_of_05_JUL_2023\).pdf](https://jitc.fhu.disa.mil/isg/downloads/FY22_ISG_Annual_Report_FINAL_(as_of_05_JUL_2023).pdf)
- [3] <https://acqnotes.com/subcategory/jcids-process/page/2>
- [4] Joint Staff, *NR KPP and Interoperability Smart Book*, 13 April 2023.
[https://jitc.fhu.disa.mil/isg/downloads/JS_J6_NR-KPP_and_Interoperability_SMART_BOOK-April_2023_\(final\).pdf](https://jitc.fhu.disa.mil/isg/downloads/JS_J6_NR-KPP_and_Interoperability_SMART_BOOK-April_2023_(final).pdf)
- [5] JITC, *Department of Defense Interoperability Process Guide*, July 2023.
https://jitc.fhu.disa.mil/isg/downloads/IPG_Version_3_Final_signed_20230703.pdf
- [6] https://en.wikipedia.org/wiki/Tragedy_of_the_commons
- [7] <https://www.defense.gov/Multimedia/Photos/igphoto/2002871137/>
- [8] <https://acqnotes.com/acqnote/acquisitions/acquisition-category>
- [9] JCIDS Manual, *Manual for the Operation of the Joint Capabilities Integration and Development System*, 30 October 2021.
<https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Manual%20-%20JCIDS%20Oct%202021.pdf>
- [10] <https://acqnotes.com/acqnote/acquisitions/information-support-plan>

REPORT DOCUMENTATION PAGE**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION**

1. REPORT DATE 07-2023		2. REPORT TYPE Paper		3. DATES COVERED	
				START DATE	END DATE
4. TITLE AND SUBTITLE Joint Interoperability: Resources and Recommendations for Improving DTE&A's Contribution to Assessing Systems					
5a. CONTRACT NUMBER HQ0034-19-D-0001		5b. GRANT NUMBER		5c. PROGRAM ELEMENT NUMBER	
5d. PROJECT NUMBER AX-1-5169		5e. TASK NUMBER		5f. WORK UNIT NUMBER	
6. AUTHOR(S) Hancock, Lance E.; Morrison, Kyle A.					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305				8. PERFORMING ORGANIZATION REPORT NUMBER P-33590 Log H 2023-000266 ANDREW 3000674	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Ms. Sarah M. Standard Cybersecurity/Interoperability OUSD R&E, DTE&A				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER	
12. DISTRIBUTION/AVAILABILITY STATEMENT Cleared for Public Release by the DoD Office of Prepublication Review, Case 24-T-0072, 11 October 2023					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT OUSD R&E DTE&A requested that IDA investigate whether DTE&A Staff Specialists have access to the data they need for assessing the interoperability (IO) of systems in development. IDA held phone interviews with 12 DTE&A Staff Specialists from across the warfare areas (Air, Land, Missiles, Naval, Space, NC3), presented observations to the Interoperability Steering Group, and was provided several documents by ISG members describing the processes involved in setting requirements, planning tests, and evaluating systems for Joint Interoperability (JIO). This report includes an overall description of the Joint Interoperability development process, Lessons Learned from the Staff Specialists, opportunities to improve Staff Specialists' oversight of Joint Interoperability, additional avenues to investigate, and descriptions of resources and references for Staff Specialists.					
15. SUBJECT TERMS Developmental Test; Interoperability; JITC					
16. SECURITY CLASSIFICATION OF:				17. LIMITATION OF ABSTRACT	
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified		SAR	
18. NUMBER OF PAGES					
19a. NAME OF RESPONSIBLE PERSON Dr. John S. Hong, Project Leader				19b. PHONE NUMBER 703-845-2564	

PREVIOUS EDITION IS OBSOLETE.

STANDARD FORM 298 (REV. 5/2020)

Prescribed by ANSI Std. Z39.18