Enabling Information Superiority through C4ISR Interoperability

Robin Quinlan
Deputy Director for Systems Interoperability
Office of the Under Secretary of Defense (Acquisition, Technology and Logistics)
3070 Defense, Pentagon Room 3C261
Washington, DC 20301-3070
quinlarl@acq.osd.mil

Gordon Tillery
Science Applications International Corporation
1755 Jefferson Davis Highway, Suite 202
Arlington, VA 22202
tilleryg@saic.com

Keywords:
Interoperability; System of Systems; Collaborative Engineering Environments; Joint Distributed Engineering Plant

ABSTRACT: *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Systems Interoperability is the number one problem in the Defense Department today in joint force operations. Deployed operational forces are joint - a meld of multiple Services and coalition partners, each independently efficient and smoothly operating. The resulting mix of unique systems, operating procedures, protocols and standards, tactics, and languages produces an interoperability quagmire and complicates the full realization of information superiority. Further, new systems and system upgrades are increasingly complex in sophistication of information technology and communications interfaces, and the problems compound. Because of practical limitations on assembling joint forces short of actual operational deployment, modeling and simulation (M&S) is a key to understanding and resolving interoperability problems.*

M&S plays a critical role in system and force evaluation; the Joint Distributed Engineering Plant (JDEP) will provide a test bed for systems to be exercised in a representative joint operational environment. A collaborative engineering environment underpins JDEP, utilizing concepts of Simulation Based Acquisition (SBA).

Individual systems must be "born joint." In addition to optimizing a system's design, in terms of independent performance, the design must include the capability to interoperate with a myriad of other systems. This is in the context of a systems architecture drawn from a joint operational architecture which portrays the user's (theater warfighting Commander-in-Chief) requirements to prosecute operations. M&S used in system development must provide reuse and interoperability of models and data across service and program lines. This is essential to build-in system-of-systems interoperability.

Also critical to the realization of information superiority is the ability to demonstrate a clear, continuous, and complete air, ground, and maritime operating picture to U.S. and allied forces.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2000**	2. REPORT TYPE	3. DATES COVERED **00-00-2000 to 00-00-2000**

4. TITLE AND SUBTITLE
Enabling Information Superiority through C4ISR Interoperability

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Office of the Secretary of Defense,Acquisition, Technology and Logistics,3070 Defense Pentagon Room 3C261,Washington,DC,20301-3070

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**10**	

The ability to provide coalition partners and disadvantaged users with integrated pictures across each of these domains relies upon the ability to adequately operate in a seamless multi-level security (MLS) environment. In the short term, a refinement of tactics, techniques, and procedures (TTP) regarding the processing of various sensitive data (such as raw intelligence, surveillance, and reconnaissance data) must occur. The desired end-state is to reconcile current policy and doctrine, as appropriate, with available MLS technologies to implement effective filtering mechanisms to allow seamless data flow between SCI and GENSER security environments.

It is important to ensure that intelligence data is seamlessly integrated with a picture of the battlespace at all levels of end-use, through each time dimension, and across appropriate security domains. Interoperability must be achieved between the collection, processing, and disseminating systems and the COP/CTP/SIA-G-MP in order to provide the end-user with timely, accurate, and relevant intelligence data.

1. Interoperability is the Number One Problem.

In 1983, United States operation "Urgent Fury" in Grenada witnessed a problem that became a milestone in the recognition of interoperability difficulties in joint operations. Army paratroopers on the ground were totally dependent for fire support upon naval aircraft and naval gunfire. The soldiers discovered that when they needed naval support their radios could not communicate with the ships in the offshore *Independence* battle group. The ground troops - exhibiting the self-reliant, ingenuity so common to the American soldier in our Nation's history - placed a long distance commercial telephone call to their home base at Fort Bragg which relayed by satellite the call-for-fire to the Navy ships off the coast of Grenada. [Reference 1]

Many things have changed, but some have not. Interoperability of joint forces remains today a very big problem.

Lessons learned by our warfighting forces in operations in Kosovo, and the most current issues identified by our nation's nine warfighting Commanders-in-Chief (CINCs) are replete with interoperability problems. The problems range from restrictive policy (such as releasability of classified information to coalition partners); to native language barriers; to training of personnel (to implement joint communication architectures); to design of technical interfaces of tactical data links (limiting exchange of message traffic among joint force systems); to "leakers" in joint force defensive nets and fratricide (system-of-system misidentified targets and uncorrelated target track data resulting from differing message formats, data translation, fire control correlation algorithms, coordinate systems, and ineffective configuration management of software in our deployed systems).

Typically, our weapon systems have been designed against specific performance requirements, but - until very recently - there has been scant emphasis on design for interoperability with other systems, especially other Service or country systems. When you couple this situation with the incessantly fast pace of computer technology evolution, the Revolution in Military Affairs and Joint Vision 2010 (exploiting information technology to increase tempo and precision in military operations), and the expanding sets of coalition partners in a broader range of US military operations, the future presents many challenges for achieving interoperability.

Figure 1. The Future Presents Challenges for Joint Force Interoperability

Interoperability is the number one problem today facing our nations joint forces. Interoperability is neither a new problem, nor is it one for which quick solutions are readily apparent. But top-level Defense leadership interest, focus and commitment to achieving interoperability has arrived – so defining and applying solutions may no longer be a bridge too far.

2. Interoperability Problems

Interoperability in joint force operations, and especially in coalition operations, is a recognized challenge. According to the Secretary of Defense: "…building and maintaining effective coalitions also present significant challenges, from policy coordination at the strategic level to interoperability among diverse military forces at the tactical level. As the U.S. military incorporates new technologies and operational concepts at a pace faster than that of any other military, careful design and collaboration will be needed to ensure the United States and its allies and partners meet new interoperability challenges." [Reference 2]

Recent Kosovo operations illustrate the challenges. The absence of secure voice interoperability led to security breaches during air operations; allied nations found the different levels of electronic sophistication precluded seamless interoperability in joint operations; and increased use of information systems placed severe stress on bandwidth availability that limited deployment of certain assts. [Reference 3] Other examples are abundant; each recurring joint force exercise in the All Service Combat Identification Evaluation Team (ASCIET) series reveals our interoprability issues are not diminishing.

2.1 What is Interoperability?

There are many different definitions for interoperability. Joint Publication 1-02 has two definitions: [Reference 4]
"1. The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.
"2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users."

For the purposes of this paper, I will not consider physical interfaces of services or equipment (such as standard ammunition sizes, or fuel connections), but instead limit the topic to the exchange of information between systems. Simply put, interoperability in this context can be defined as *the exchange of information that preserves the meaning and relationships of the information exchanged*.

Because of the increasingly joint/coalition nature of post-Cold War military operations, interoperability is essential to achieving complete warfighting capability. Being good stewards of defense resources, we should not consider procuring additional systems as a way to make up for interoperability problems degrading force capability. So we must solve the interoperability problems.

There are two classes of interoperability problems: those we currently experience in legacy systems, and those we can avoid in acquisition systems. For legacy systems, the solutions can be introduced in system design changes, different operating tactics/techniques/procedures, and/or improved operator training. For emerging systems, we need to build interoperability in, from system conception.

2.1 From the CINCs Perspective

Reports from the warfighting CINCs, from operational campaigns, and from training exercises are replete with interoperability problems. The problems can be categorized into these general areas:

- **Situational Awareness**
  Real time air/ground/sea display with Combat Identification and Intelligence is incomplete, inconsistent, and often inaccurate
- **Information Management System Processing**
  Bandwidth and system capacities cannot support operational conditions
- **Coalition Interoperability**
  Incomplete sharing of information; incompatible systems; language barriers; no early warning/multi-level security/encryption for coalition partners
- **Incompatible Tactical Data Links (TADIL)**
  Digital data links transmitting messages between various systems not fully interoperable
- **Operator Training**
  Joint communications staff not sufficiently trained in multi-TADIL architectures
- **Joint Distributed Collaborative Planning**
  Several tools exist; need common joint tools and methods
- **Combat Identification & Fratricide Prevention**
  Not integrated for consistent, accurate, reliable targeting decisions
- **Intelligence Processes**
  Need interoperable system to develop & distribute intelligence effectively, including coalition partners

2.2 From a Mission Area Perspective

Work by the Ballistic Missile Defense Organization in designing a family of systems has focused on eliminating "five deadly sins" of interoperability. A significant amount of modeling has been applied to understanding the problems and assessing the design trade space, incorporating known system interoperability issues. These are recognized problems associated with sharing information in a Link-16 based data network to accomplish the Joint Theater Air Missile Defense (JTAMD) mission:

- **Gridlock**
  Need common location reference plane between the sensor and shooter systems
- **Time Synchronization**
  Need common time reference to the milli-second level
- **Data Registration**
  Need consistent location information
- **Characterization**
  Need similarly identified threat targets to allow optimal intercepts
- **Track Correlation Picture**
  Need to match local and remote sensor tracks

2.3 From a System Perspective

System specific interoperability issues have been demonstrated in numerous exercises and operational deployments. Underlying causes are, in most cases, complex and beyond the scope of this paper. These problems are typical of the many which preclude our defense systems from achieving full capability.

- Core battle management systems (e.g., GCCS-M, GCCS-I3, JDISS, ASAS, TBMCS) not fully integrated into the GCCS.
- JTAMD Family-of-Systems use incompatible correlation algorithms to evaluate identical tracks
- Forwarding tactical event data from the ALERT, JTAGS, TACDAR systems onto tactical Datalinks (and GCCS) causes erroneous/multiple tracks
- Time latency and poor correlation contributes to multiple tracks on single targets

3. The Joint Distributed Engineering Plant

A concept has emerged from the Navy's recent efforts in solving interoperability problems in their sea systems. The Navy's Distributed Engineering Plant (DEP) was created to accomplish systems engineering activities using hardware, software, and personnel at geographically dispersed locations linked by telecommunications network technology. The DEP enables the Collaborative Engineering Process. While it does not replicate a Joint Force, the DEP was successfully used by the Navy to resolve critical interoperability problems.

The Navy's DEP includes such facilities as the AEGIS Combat System Engineering Facility. Any of you that have driven Interstate Highway 95 into New Jersey may have noticed it from the highway; some call it "Aegis in a Cornfield." The facility replicates functionality of topside systems for hardware/software/operator in-the-loop assessment across a distributed environment.

Photo courtesy of Lockheed Martin. Used by permission.

Figure 3.1. "Aegis in a Cornfield"

The Joint Distributed Engineering Plant (JDEP) is intended to incorporate the DEP foundation and additional distributed capabilities - such as the Theater Missile Defense System Exerciser. The purposes are: Joint Force interoperability testing of currently fielded systems; Joint Force interoperability engineering of future systems; systems engineering for design and development performance testing and evaluation; and, assessment of Joint Force interoperability requirements.

In addition, the Joint Interoperability Test Command will use the Joint Tactical Data Link Laboratory-based network, with sensor simulation and secure tactical/voice communications, to conduct system interoperability certification testing.

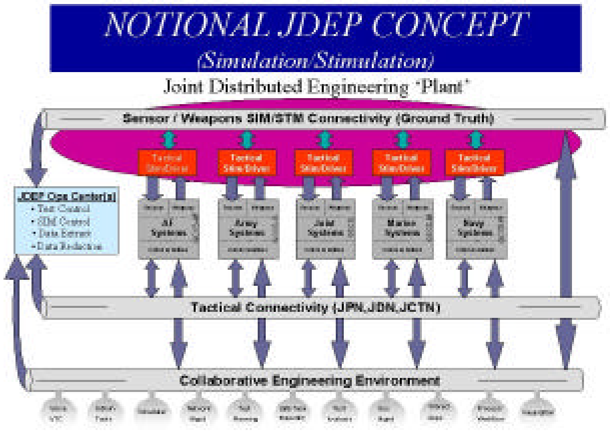


Figure 3.2. Notional JDEP Structure

Note that a Collaborative Engineering Environment underpins JDEP. A Collaborative Environment is an enduring collection of subject matter experts, supported by interoperable tools and data bases, authoritative information resources, and product/process models that are focused on a common domain or set of problems. In JDEP, the collaborative engineering environment will facilitate system-of-system engineering functions based on sharing information, databases, and analytical models across geographically dispersed engineers/engineering teams. [Reference 5]

The JDEP capability is important for many reasons:

- Enables a disciplined systems engineering and testing at the Joint Force-level
- Provides vehicle for requirements engineering and Measures of Performance/Measures of Effectiveness development
- Provides a repeatable "controlled environment" for evaluation of Joint Force-level interoperability problems
- Reveals 'why' vice just replicating interoperability problems
- Contributes to the ability to conduct system-level "fault isolation" of interoperability problems
- Provides controlled environment to evaluate "work-arounds" and "fixes"
- Enables Joint Forces to validate operational Tactics, Techniques and Procedures prior to deployment

By simulating and stimulating the sensor, processing, information exchange, kinematics, dynamics, mechanical, and other characteristics of some particular domain's system (radar, processor, data bus, platform, hull, propulsion system, etc.), engineers can create a multi-disciplinary environment to evaluate a wide range of parameters. Capturing parametric results is the primary reason to include design level models or simulations as well as stimulation's employing tactical hardware/computer programs in the loop. These models or simulations of particular domains (communications, combat systems, safety, platform, infrastructure, etc.) can be integrated at different sites to examine interoperability early in the acquisition life cycle. By exercising these models and simulations (at distributed and possibly redundant sites), interoperability design and development issues can be discovered, addressed, and resolved. [Reference 6]

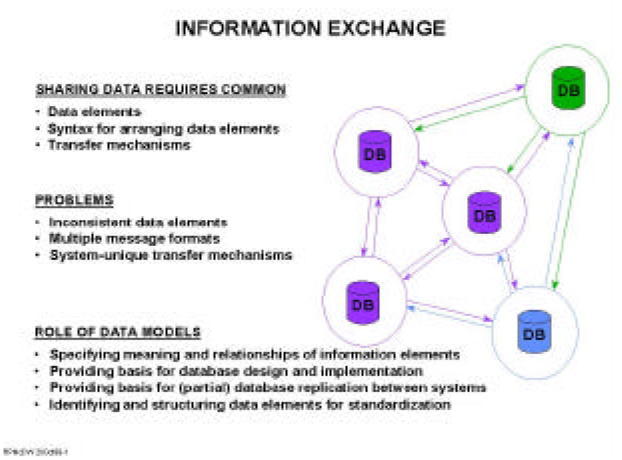
Consensus has been achieved between the Services, the Joint Staff, and OSD in the need to establish a JDEP capability for joint systems development and testing.

4. Modeling & Simulation

M&S is key to understanding and resolving interoperability, to fix existing problems in legacy systems, and to build-in interoperability in acquisition systems.

But the application of M&S must conform to the principles for reuse and interoprability of M&S. Why? Because to achieve joint force system-of-systems interoperability, we must provide reuse and interoperability of models and data across service and program lines. The ability to reuse models and data of other system representations, across services and even national boundaries, is fundamental and essential to achieve interoperability in the context of systems-of-systems joint force operations.

There are basic concepts for assuring data reuse/sharing/exchange.



INFORMATION EXCHANGE

SHARING DATA REQUIRES COMMON
- Data elements
- Syntax for arranging data elements
- Transfer mechanisms

PROBLEMS
- Inconsistent data elements
- Multiple message formats
- System-unique transfer mechanisms

ROLE OF DATA MODELS
- Specifying meaning and relationships of information elements
- Providing basis for database design and implementation
- Providing basis for (partial) database replication between systems
- Identifying and structuring data elements for standardization

Figure 4.1. Basic Concepts for Assuring Data Reuse/Sharing/Exchange

The Army has selected a strategy to assure data is created for use in standard and common software products across all command and control systems. This strategy is called the Joint Common Data Base (JCDB).

Based upon the Joint Technical Architecture (JTA) standard Command and Control Core Data Model (C2CDM), the JCDB is comprised of functional area data utilized by both Army and Joint C2 systems making it extensible and usable as a joint interface for data shared among the various services. JCDB data is intended to be shared through direct 'db-to-db' exchange among LAN based host systems in near real time. [Reference 7]

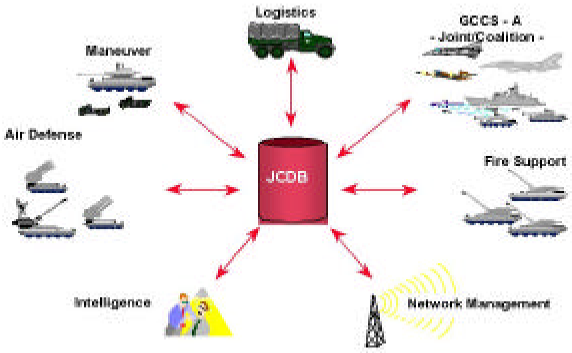
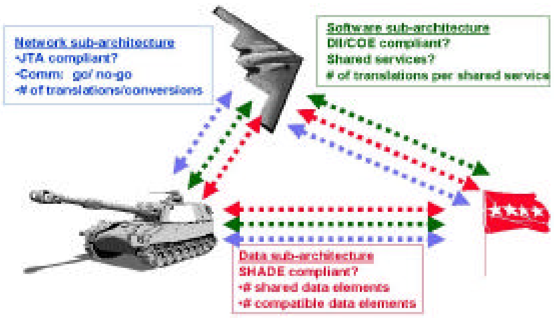


Figure 4.2 Joint Common Data Base Concept

To fully represent joint force operational system employment scenarios, a practical architectural taxonomy for interoperability at the system level is necessary. Consider:

- Interoperability requires specified sub-architectures of a system's architecture.
- This relationship appears more clearly if we consider the Systems Architecture as comprising three sub-architectures: network, data and software.
  - A network architecture that specifies the physical network connectivity and network protocols.
  - A data architecture that answers what data will move across the network.
  - A software architecture that specifies the application interfaces that will use the network and generate data.



Network sub-architecture
-JTA compliant?
-Comm: go/ no-go
-# of translations/conversions

Software sub-architecture
DII/COE compliant?
Shared services?
# of translations per shared service

Data sub-architecture
SHADE compliant?
-# shared data elements
-# compatible data elements

Figure 4.3. Illustration of Taxonomy

Clearly, we must apply the disciplines of the M&S community when considering system data architectures. A suggested set of rules:

- Select Standards Before Implementation
    - Where possible, find minimum set of standards that provide basic interoperability
    - Use commercial technical standards
    - Agree to a common data model for specifying information's meaning and relationships
- Identify Transfer Mechanisms that Exploit DBMS Technology (database-to-database interoperability)
- Identify and Specify Multinational Information Exchange Requirements (IERs)
- Adopt Common Information Products and Exchange Mechanisms
    - Separate protocol and syntax from content
    - Relate each information element to an IER and to a data standard
- Use Data Models to Identify and Structure Data Standards

5. Interoperability is Worked Everywhere

It has been said there are 200 organizations in the DoD community with the word *Interoperability* in their title. I will discuss a few.

5.1 Organizational Efforts

Starting at the top, the Office of the Secretary of Defense has established a Director for Interoperability. The Director reports to the Under Secretary of Defense (Acquisition, Technology and Logistics). The mission is to provide a focus, working with C^3I, the Joint Staff, CINCs, Services, Defense Agencies, and Coalition Forces, to enable the full range of military operations, through Interoperability and Coalition Warfare initiatives. A primary focus is to establish an effective Common Operating Picture (COP), the corresponding Common Tactical Picture (CTP), and Single Integrated Air/Ground and Maritime Pictures (SIAP/SIGP/SIMP).

The Joint Staff has two important activities focusing on interoperability: the Interoperability Joint Warfighting Capabilities Assessment (I-JWCA), and the Military Communications Electronics Board (MCEB). JWCA-I, led by the J-3 staff, focuses Service/Agency responses to CINC interoperability issues. The MCEB, led by the J-6, focuses C4 leadership across DoD on a broad range of issues including interoperability. MCEB has working panels that monitor interoperability testing certification and related matters.

The Assistant Secretary of Defense (Command, Control, computers and Intelligence) is the DoD Chief Information Officer. The staff is organized with responsibility for information assurance and interoperability, and publishes such documentation as the C4ISR Architecture Framework.

Within the last year a joint program office was formed to represent the CINCs in the Service command and control system commands. Each system command (USAF Electronic Systems Command, USN Space and Naval Warfare Systems Command, and USA Communications Electronics Command) has assigned six personnel in its own organization and also six personnel to each of the other two, so that each system command now has 18 personnel functioning as an in-residence, CINC's Interoperability Program Office (CIPO).

5.2 Policy and Guidance

Two instructions have been reissued to emphasize the role of the Joint Staff in assuring interoperability:

- CJCSI 3170.01A, "Requirements Generation System." This instruction requires the J-6 to certify all requirements documentation - regardless of acquisition category level - for conformance with joint policy, technical architecture integrity, and interoperability standards. In addition, Joint Forces Command is designated as the JCS Chairman's advocate for joint warfare interoperability, and thus will play a critical review role in all systems requirements. [Reference 8]
- CJCSI 6212.01B, "Compatibility, Interoperability, Integration and C4 Supportability Certification of Command, Control, Communications, Computers and Weapon Systems." In final drafting, this instruction specifies three interoperability certifications to be accomplished for every C^4I system by the J-6. Additionally, it provides the process and format for developing interoperability Key Performance Parameters and Information Exchange Requirements for system requirements documentation. [Reference 9]

5.3 Experiments and Demonstrations

A number of activities are designed to demonstrate and improve interoperability for joint forces. Several Advanced Concept Technology Demonstrations (ACTD) focus on interoperability. ACTDs typically focus on improvements within a specific problem or mission area. We must also assure that any capability developed in an ACTD is verified for conformance to general interoperability applications. Verification is possible in exercises and demonstrations, such as the Joint Warrior Interoperability Demonstration (JWID), or the ASCIET series of joint force representative trials. Unfortunately, recent ASCIET results have tended to show worsening interoperability – primarily due to bringing more sensors into the mix. Hence, the JDEP concept has merit to assure solutions are engineered within the context of the joint force.

6. Summary

Joint force – and combined (coalition) force – operations are here to stay. Information technology has changed the world, and will continue to change the way our forces conduct military operations. In acquisition, interoperability has been the victim of traditional processes optimized for Service requirements. Our forces have repeatedly experienced severe interoperability problems in operations and exercises. The imperative is to both fix the legacy problems, and build interoperability into future systems. DoD has expanded the emphasis on joint force interoperability, and the requirements process has changed in that regard. Several activities are ongoing to improve legacy systems. The M&S community has much to offer. Concepts such as JDEP rely upon M&S to create system-of-system simulations incorporating hardware, software, and operating personnel in-the-loop to engineer joint systems with interoperability built-in from conception. Interoperability is not a choice; it is the imperative!

7. References

[1] Office of the Chairman of the Joint chiefs of Staff, "Operation Urgent Fury - The Planning and Execution of Joint Operations in Grenada," pp. 52-53, 1997

[2] Secretary of Defense, "Annual Report to the President and the Congress," 1999

[3] Robert Ackerman, "Kosovo Maps the Future of Information Technologies," *Signal* magazine, December 1999 issue

[4] Joint Doctrine Division, J-7, Joint Staff, "DOD Dictionary of Military and Associated Terms," *Joint Publication 1-02*

[5] Acquisition Council, “A Road Map for Simulation Based Acquisition,” pp. 5-2 to 5-10, 9-3, 4 December 1998

[6] Joint Engineering Task Force, “Final Report,” pp. 9-10 Appendix B, November 15, 1999

[7] Robert Carnevale, “The Joint Common Database,” May 18, 1999

[7] CJCSI 3170.01A, Requirements Generation System

[8] CJCSI 6212.01B, Compatibility, Interoperability, Integration and C4 Supportability Certification of Command, Control, Communications, Computers and Weapon Systems

Author Biographies

ROBIN QUINLAN is the Deputy Director for Systems Interoperability in the Office of the Under Secretary of Defense (Acquisition Technology & Logistics).

Ms. Quinlan is a Systems Engineer educated at Pennsylvania State University and the University of Virginia. She is a graduate of the Defense Systems Management College Program Managers Course and is Level III Certified Acquisition Professional for Program Management; Systems Planning Research, Development and Engineering; Computers and Communications Systems; Test and Evaluation; and Production Quality Manufacturing. She is also licensed by the Virginia State Board of Architects and Engineers.

She has worked as an engineer in both industry and government. For IBM she was the Lead Engineer on the SH-60B Helicopter Weapon System/Flight Trainer from 1985-89, until IBM’s Federal Systems Division was disestablished, and she was the Division Head for Systems Integration & Requirements in the Navy’s Tomahawk Program. She also served as a Systems Engineer for the Navy’s Space and Naval Warfare Systems Command.

Since 1995 she has served in the Office of the Secretary of Defense where she served as Special Assistant to the Principal Deputy Under Secretary of Defense (Acquisition & Technology), and a Systems Engineer in the OSD Systems Engineering Directorate until it was disestablished. In that capacity, she led the Simulation Based Acquisition initiative for the DoD under Dr. Patricia Sanders, and formulated DoD policy for M&S in acquisition.

In her present position she is responsible for systems interoperability associated with the Common Operating Picture, the Common Tactical Picture and the Single Integrated Air/Ground/Maritime Pictures.

Gordon Tillery, a Senior Engineer with SAIC and provides systems interoperability technical support to OUSD(AT&L). He holds a Master of Science degree in Industrial Engineering.