CLEARED
For Open Publication

Feb 10, 2020 5

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Defense Modeling and Simulation Reference Architecture

Version 1.0

Defense Modeling and Simulation Coordination Office
4800 Mark Center Drive
Mailbox 46
Alexandria, Virginia 22350-3600
https://www.msco.mil

"The Defense Office of Prepublication and Security Review (DOPSR) has cleared this document for public release (Distribution A) (Case No. 20-S-0717)."

Contents

Table of Figures 3
INTRODUCTION 4
Scope 4
DMSRA in Relation to Other Reference Architectures 5
STRATEGIC PURPOSE 8
AV-1 Overview & Summary Information 8
Assumptions & Constraints 8
OV-1 High–Level Operational View (OV) Graphic Concept 8
Business Goals and Objectives: 9
CV-1 Vision 10
CV-2 Capability Taxonomy 11
CV-4 Capability Dependencies 14
PRINCIPLES 15
Mapping of Principles to Technical Capabilities 15
TECHNICAL POSITIONS AND POLICIES 18
Technical Position for M&S Standards in StdV-2 19
ARCHITECTURAL PATTERNS 19
Enterprise Architecture Migration 19
Current Architecture 19
Composable M&S Enterprise Architecture 21
Intermediate M&S Enterprise Architecture 22
Composable Architecture and Migration Patterns 23
Cloud Migration – Appendix D 23
Decomposition of Simulations into Modular Components – Appendix E 23
Verification and Validation of Modular Components- Appendix F 23
Documentation – Appendix G 23
SOA Primer - Appendix H 24
Remote Execution - Assessing Feasibility - Appendix I 24
Data - Appendix J 24
Accommodating Occasional / Sporadic Connectivity - Appendix K 24
Cross Domain Solutions - Appendix L 24
Distributed Simulation/ Federation Engineering - Appendix M 24
Enterprise Services - Appendix N 24
Gaming Architectures - Appendix O 24
VOCABULARY 25
Glossary 25
Acronyms 26
REFERENCES 28
APPENDIX A: DMSRA Principles and Rules 29
APPENDIX B: Standards Viewpoint 1 (StdV-1) 42
APPENDIX C: Standards Viewpoint 2 (StdV-2) 60
APPENDIX D: Cloud Migration 61

APPENDIX E: Decomposition of Simulations into Modular Components 62
APPENDIX F: Verification and Validation of Modular Components 63
APPENDIX G: Documentation 64
APPENDIX H: SOA Primer 65
APPENDIX I: Remote Execution 66
APPENDIX J: Data 67
APPENDIX K: Accommodating Occasional / Sporadic Connectivity 68
APPENDIX L: Cross Domain Solutions 69
APPENDIX M: Distributed Simulation/ Federation Engineering 70
APPENDIX N: Enterprise Services 71
APPENDIX O: Gaming Architectures 72

Table of Figures

FIGURE 1. INTENDED USE OF THE DMSRA 5
FIGURE 2. ALIGNMENT WITH OTHER STAKEHOLDER IT ARCHITECTURES 6
FIGURE 3. OV-1 HIGH-LEVEL OPERATIONAL GRAPHIC CONCEPT 9
FIGURE 4. CURRENT EA 20
FIGURE 5. COMPOSABLE EA 22
FIGURE 6. INTERMEDIATE EA 23

TABLE 1. APPLICABLE DODAF VIEWS 7
TABLE 2. CV-1 VISION 10
TABLE 3. CV-2 CAPABILITY TAXONOMY 13
TABLE 4. CV-4 CAPABILITY DEPENDENCIES 14
TABLE 5. ADVANTAGES AND CHALLENGES OF CURRENT EA 21
TABLE 6. ADVANTAGES AND DISADVANTAGES OF COMPOSABLE EA 22

INTRODUCTION

The Department of Defense (DoD) employs modeling and simulation (M&S) to enhance training, warfighting, and materiel acquisition. The Defense Modeling and Simulation Coordination Office (DMSCO) developed this Defense Modeling and Simulation Reference Architecture (DMSRA) to enhance DoD M&S contributions to fielding a lethal, resilient, and rapidly adapting Joint Force. The DMRSA guides M&S capability development and leverages advances in information technology (IT). This guidance will discuss approaches to:

- Leverage DoD IT, enterprise services, and technologies such as cloud computing and Service-Oriented Architectures (SOA)
- Develop simulations that take advantage of emerging technologies and enterprise services
- Adopt DoD M&S enterprise standards to facilitate sharing of M&S services

Recent technology advances have spurred changes in commercial IT. Commercial industry is aggressively adopting cloud computing and SOA to reduce costs and increase flexibility. The Federal Government and the DoD are following suit with their Cloud Computing Strategy [1] and DoD Information Enterprise Architecture (IEA) [2]. Additional DoD strategies and initiatives include Cloud First [3] and the Joint Information Environment (JIE) [4]. The Services are also implementing and expanding upon these strategies.

The DMSRA supplements existing policy and guidance, preparing the Defense M&S community for these major enterprise IT advances. DMSRA will enable DoD to take advantage of new technologies and opportunities. For many M&S applications, a well-planned move to cloud computing and SOA can improve accessibility and agility while reducing operating and other lifecycle costs. For example, training simulations can be rapidly configured for specific missions and delivered on station with minimal operator involvement. Cloud/SOA-enabled decision support tools can provide highly accurate real-time results to commanders in the field.

By coordinating technology implementation such as cloud computing and SOA across the DoD M&S enterprise, we can develop and adopt standards that facilitate model and simulation reuse at the modular component level. Achieving this goal will require facilitating M&S data, tool, and/or service reuse. M&S assets may have capability or content useful beyond their original application. Examples include the data, tools, or services that facilitate the execution of the entire simulation environment life cycle. Efficient reuse will result in reduced development time and cost for new simulations and solution architectures [12]. As individual programs focus development on a smaller set of reusable authoritative modular components, there should be a net improvement in simulation performance without increased cost. The transition to a distributed or cloud environment also creates some risks. Cybersecurity is paramount for any simulations the Department employs in a distributed or cloud environment.

Scope

The DMSRA provides best practices to guide and align DoD Component M&S activities:

- Where doing so provides greater value to the DoD
- Where inter-modular component interoperability is required
- When a common capability (service) is desired

M&S activities include the development of models, simulations, and pre- or post-simulation event services (e.g. scenario builders, after action reporting tools, etc.). The DMSRA is written to be broadly applicable across programs and technologies, but it may not apply to every specific case. Examples of where it may not apply include:

- Specialized capabilities with little potential for M&S reuse
- Systems requiring specialized or stand-alone hardware
- Low-cost models and simulations (e.g. Excel spreadsheet models or Matlab scripts)

Figure 1 illustrates the DMRSA. It serves as the enterprise-level guidance for the development of M&S solution architectures, designs, and products. The DMSRA provides principles, standards, patterns, and best practices for DoD organizations to apply when architecting, developing, operating and maintaining models and simulations. Intended DMSRA outcomes and outputs are:

- **Reducing the cost and improve the performance** of Defense M&S capabilities;
- **Producing technical capabilities** that **leverage the DoD IT infrastructure and architectures (**in accordance with DoD policy**)**.

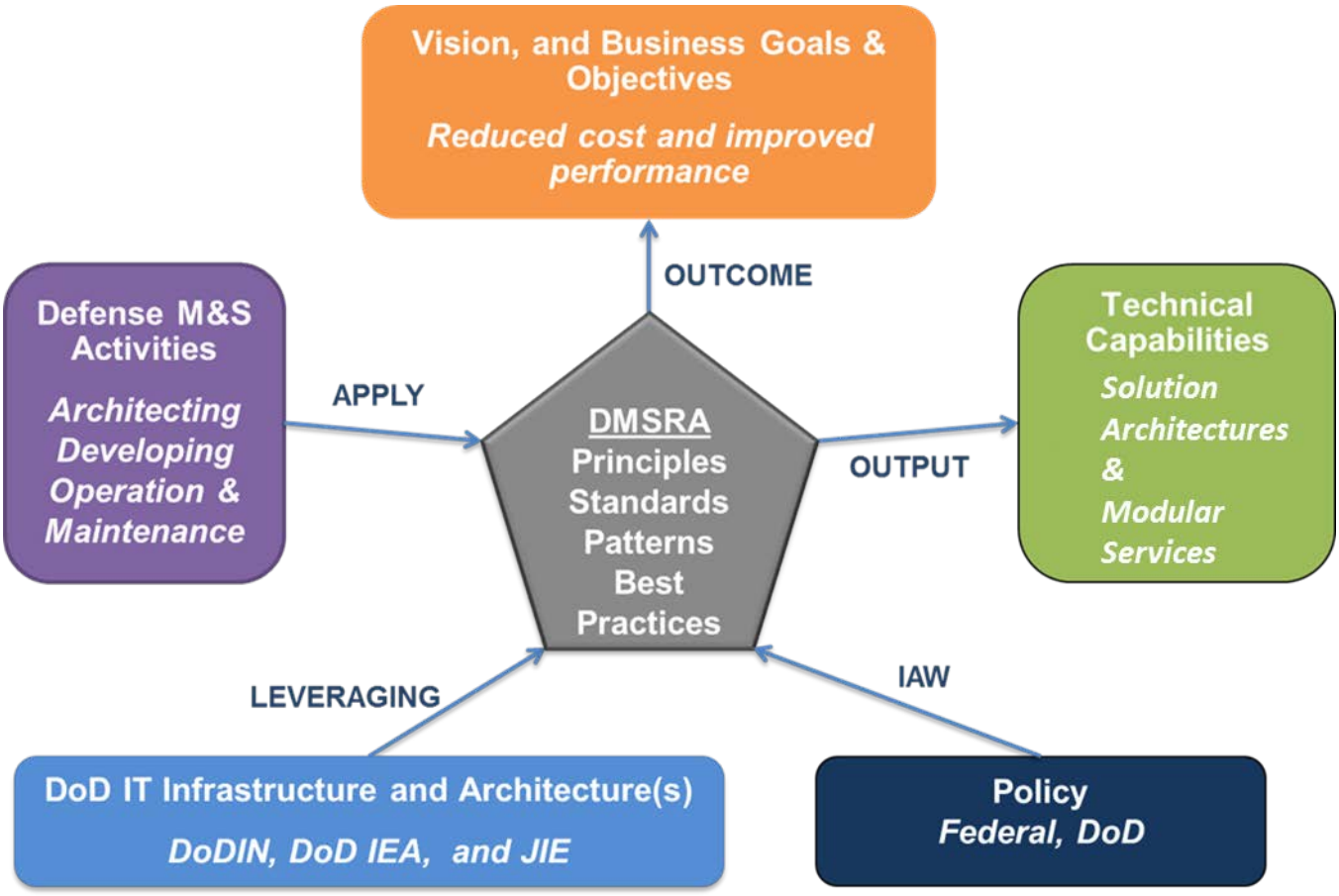

Figure 1. Intended Use of the DMSRA

DMSRA in Relation to Other Reference Architectures

Figure 2 illustrates DMSRA alignment with other DoD IT architectures. The DoD Chief Information Officer (CIO) controls the DoD Information Enterprise Architecture (IEA), the top-level guidance for DoD IT capabilities. The DMSRA falls under the DoD IEA along with other Reference Architectures (RAs) such as the Active Directory Optimization RA (ADORA) [5]. In turn, the DMSRA provides guidance for domain and Service Component RAs and may be used in conjunction with other RAs.

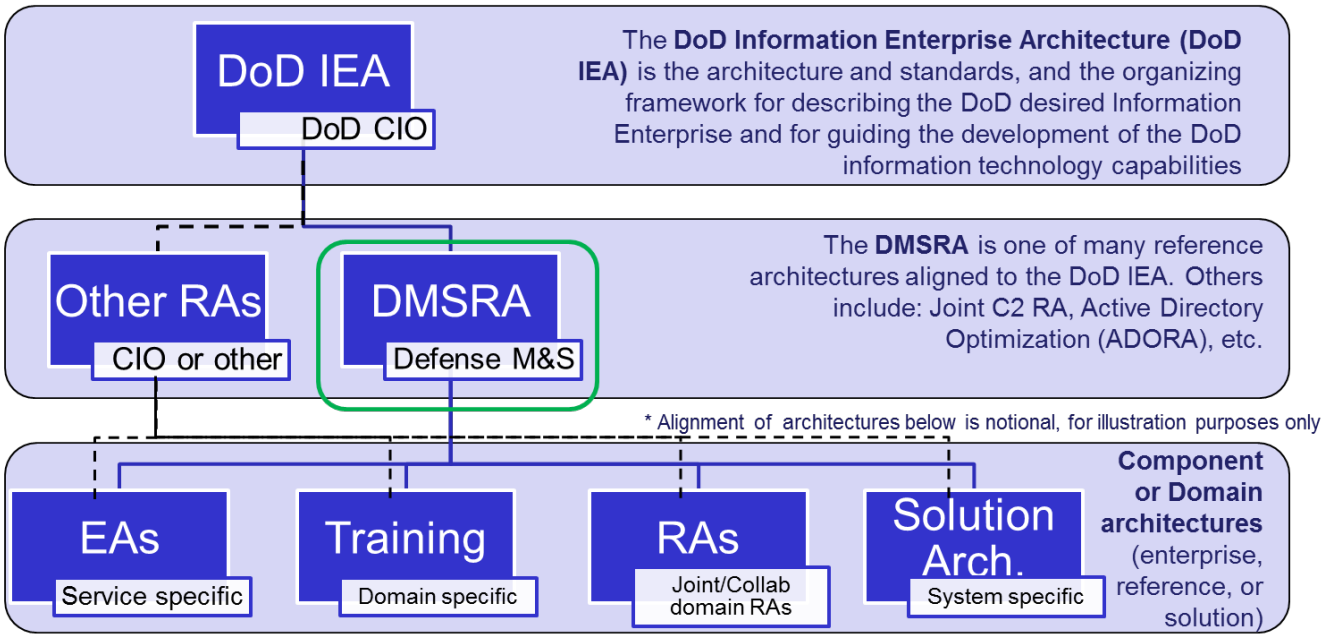

Figure 2. Alignment with Other Stakeholder IT Architectures

The DMSRA follows standard DoD Architecture Framework (DoDAF) v2.02 [6] practices and conventions. It also conforms to DoD IEA compliance requirements and the DoD Reference Architecture Description document. The DMSRA is consistent with the JIE capabilities for the future DoD computing infrastructure. The DoD IEA and related RAs provide additional guidance including architectures, Concepts of Operation (CONOPs), transition plans, and technical direction addressing areas such as cloud computing, virtualization, and tactical/mobile computing.

The DMSRA includes the following elements:

a. **Strategic Purpose** – Goals and objectives of the DMSRA; specific purpose of and the problem(s) to be addressed by the DMSRA.
b. **Principles –** High-level foundational statements of stakeholders, rules, and values that drive technical positions and patterns.
c. **Technical Positions** – Technical guidance and standards, based on specified principles that need to be followed and implemented as part of the solution.
d. **Patterns** (Templates) – Generalized architecture representations (viewpoints, graphical/textual models, diagrams, etc.) that show relationships between elements and artifacts specified by the technical positions and encourage adherence to common standards, specifications, and patterns.
e. **Vocabulary** – Acronyms, terms, and definitions used in the DMSRA and relevant to architectures and solutions that are guided and constrained by the DMSRA.

Table 1 lists DoDAF v2.02 views and models used in the DMSRA. DoDAF defines the following: AV-All Viewpoint; OV-Operational Viewpoint; CV-Capability Viewpoint; Std V-Standards Viewpoint

Table 1. Applicable DoDAF Views

Content	DoDAF 2.02 Views/Models
Strategic Purpose: introduction, overview, context, scope, goals, purpose, why needed, and when and how used	• **AV-1 Overview & Summary Information** - project's vision, goals, and objectives • **OV-1 High Level Operational Concept Graphic –** executive operational summary level of what solution architectures are intended to do and how they should do it • **CV-1 Vision –** overall strategic concept and high level scope • **CV-2 Capability Taxonomy** – hierarchy of capability requirements • **CV-4 Capability Dependencies** – dependencies between planned capabilities and logical groupings of capabilities
Principles: foundational organizational rules, culture, and values that drive technical positions and patterns	• **OV-4 Organizational Relationships Chart –** architectural stakeholders • **Operational and Service Rules and Principles –** identifies rules and principles that constrain operations of the architecture; a combination of the types of rules found in the OV-6a (Operational Rules Model) and SvcV-10a (Services Rules Model)
Technical Positions: technical guidance and standards	• **StdV-1 Standards Profile** – standards, specifications, guidance and policy applying to elements of the solution architectures • **StdV-2 Standards Forecast** – expected changes in technology-related standards, operational standards, or business standards and conventions; includes standards developed, but not yet adopted, and significant standards gaps
Architectural Patterns: generalized patterns of activities, service functionality and system functionality.	• Guidance and best practices for the implementation of the Operational and Service Rules and Principles. Because the architecture is not fully mature and some of the capabilities are still in development, some best practices may only partially realize the principle or rule they address, but they represent the best existing resource.
Vocabulary: acronyms, terms, and definitions	• **AV-2 Integrated Dictionary –** definitions of terms used throughout the architecture

The DMSRA provides an objective M&S reference architecture for the future. Some of the capabilities required and described in this document are not fully mature. These capabilities will require further research and development to achieve. Even though such an architecture is not fully realizable now, M&S capability developers can begin to prioritize, delegate, and resource the technical and programmatic changes to implement enhanced, composable simulation architectures. This document serves to help guide and prioritize research and development to support the vision.

STRATEGIC PURPOSE

The DMSRA is a vision for developing robust M&S solution architectures that:

- Support the full spectrum of DoD activities
- Are delivered to the point of need
- Fall within current fiscal constraints, managing schedules and risk
- Are enabled by agile composition

AV-1 Overview & Summary Information

The AV-1 describes a project's visions, goals, objectives, plans, activities, events, conditions, measured effects, and produced objects.

Assumptions & Constraints

Key assumptions and constraints of DMSRA Version 1.0:

- DoD direction on data and information sharing, architecture management, data center consolidation, cloud computing, and server virtualization is evolving.
- The DMSRA will be developed iteratively with each successive version incorporating new or matured guidance
- The DMSRA points the reader to the approved DoD Cloud Computing Strategy – it does not establish the basis for adoption of cloud computing in DoD
- The DMSRA is a supplement to a larger set of guidance that will guide the DoD to reach the JIE target state.
- The DMSRA serves as enterprise-level guidance for the development of solution architectures, domain- and Service-specific reference architectures, engineering designs, acquisitions, and related programs

This version of the DMSRA will not address:

- Requirements/standards for stand-alone, non-reusable, or simple (i.e., basic spreadsheet models) models and simulations
- JIE governance, CONOPs, performance management, or implementation of the target state environment
- Engineering or solution level technical guidance
- Requirements for M&S operator or maintainer training
- Individual enterprise services or service delivery details

OV-1 High–Level Operational View (OV) Graphic Concept

The OV-1 (Figure 3) is an executive operational summary level of what solution architectures are intended to do and how they should do it

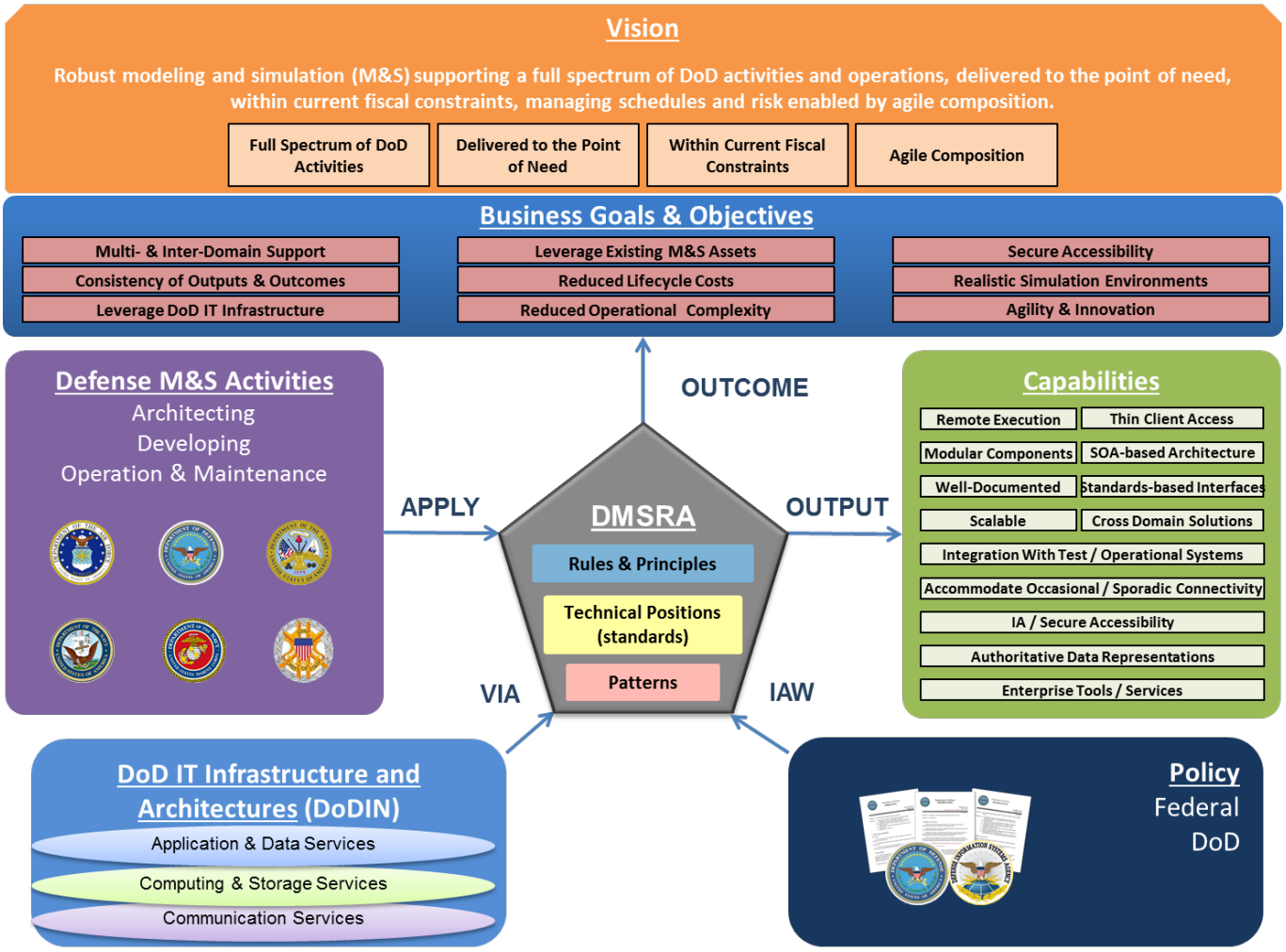

Figure 3. OV-1 High-Level Operational Graphic Concept

DoD M&S activities apply DMSRA principles, standards, patterns, and best practices. DoD applies this guidance during M&S architecture, development, operation, and maintenance activities. DMSRA is aligned with current policy and leverages the DoD IT Infrastructure (the Department of Defense Information Networks (DODIN)) and architectures. The resulting M&S architecture and asset technical capabilities should have the characteristics described in the "Capabilities" box on the right in the OV-1.

Business Goals and Objectives:

Multi- and Inter-Domain Support: Defense M&S assets that serve multiple domains (e.g., acquisition, test, training) or enable interoperability and sharing of data, information, or services between domains. [Ref: M&S Enterprise Goals]
Consistency of Outputs and Outcomes: Credible and trustworthy results from models, simulations, and composed services.

Leverage DoD IT Infrastructure: Reliance on enterprise IT services and assets for the background infrastructure so resources may be realigned toward improving quality of M&S solutions, providing Defense M&S assets that are accessible world-wide via DoD networks and information environments. [Ref: SOA RA (Alignment)]

***Leverage Existing M&S Assets**:* Deliberate integration and transition "to a more organized and integrated set of coexisting systems," reducing the "physical number of systems and enable(-ing) consolidation of platforms." [Ref: SOA RA (Consolidation), and the LVCAR precepts]

***Reduced Lifecycle Costs**:* Reuse of modular components, and decreased cost of modification by consolidating redundant functionality, reducing integration errors, and decoupling functionality from obsolete and increasingly costly applications while leveraging existing investments. [Ref: SOA RA and LS TTE EA]

Reduced Operational Complexity: Reduced preparation, operation, and maintenance cycle time through continuous improvement practices and use of proven processes, services, and assets.

***Secure Accessibility**:* Defense M&S solution availability, integrity, authentication, confidentiality, and nonrepudiation, and efficient cybersecurity accreditation, through adoption of proven and approved cybersecurity technologies and processes early in the development lifecycle. [Ref: DODI 8500.01 (definition of cybersecurity)]

***Realistic Simulation Environments**:* Synthetic representations of the operational environment, including the representations of entities, behaviors, environmental effects, and interactions with the operational environment, that are operationally-valid and at the appropriate resolution for the intended use.

***Agility and Innovation**:* M&S solutions designed for modularity and composability, producing solutions based on a set of loosely-coupled services facilitating rapid restructuring and reconfiguration, and enabling use of existing capabilities in new and innovative ways.

CV-1 Vision

The CV-1 depicts the overall strategic concept and scope. **Table 2** maps business goals and objectives to the vision statement elements, creating a more detailed picture of the vision and its scope. This mapping recognizes some business goals and objectives provide secondary support to the vision statement elements beyond the primary ones identified in the OV-1 section above.

Table 2. CV-1 Vision

	Vision Statements			
Enterprise Goals	Support full spectrum of DoD activities	Delivered to the point of need	Within current fiscal constraints, managing schedules and risk	Enabled by agile composition
Multi- & Inter-Domain Support	X			
Realistic Simulation Environments	X			X
Consistency of Outputs & Outcomes	X			
Leverage DoD IT Infrastructure		X	X	
Leverage Existing M&S Assets	X	X	X	X
Reduced Lifecycle Costs			X	

Reduced Operational Complexity			X	
Secure Accessibility	X	X		
Agility & Innovation			X	X

CV-2 Capability Taxonomy

The CV-2 provides a hierarchy of capability requirements. DoD M&S activities should include the following capabilities:

- **Remote execution** – the ability to run a simulation on a computer, geographically separated from the user over a network connection, such as in a data center.
- **Thin client access** – the ability to access a simulation over the network running remotely from a machine with minimal computational capability. This may be extended to include mobile devices such as tablets and cellphones.
- **Modular components** – distinct simulation functions are contained in separate software modules designed to facilitate reuse.
- **SOA-based architecture** – functionality is encapsulated in discrete services. Services are loosely coupled. Services may be dependent on other services and organized in a layered hierarchy.
- **Standards-based interfaces** – Application Programming Interfaces (APIs) are based on established industry or DoD standards to facilitate interoperability and composability. Examples of industry interface standards are Simple Object Access Protocol (SOAP) and Representational State Transfer (REST)[1].
- **Well documented** – information about the operation, function, and underlying assumptions of a model or simulation is recorded outside of the code itself and in sufficient detail to aid in its discovery, composability, and verification and validation (V&V).
- **Accommodate occasional / sporadic connectivity** – the ability to support the mission when network connectivity is lost or degraded. For example, remote execution and thin client access rely on network connectivity to operate which may be degraded in an operational environment.
- **Scalable** – the ability of the simulation to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. For example, the ability to add users or increase the number of entities without user intervention, e.g. to add computer hardware.
- **Cross-domain solutions** – a form of controlled interface that provides the ability to manually and / or automatically access and / or transfer information between two or more different security domains.
- **Cybersecurity conformant** – simulations, services, and data repositories must be designed and constructed in a way that ensures that data is secure, allows access to only authorized users, and complies with applicable policy and guidance.
- **Authoritative data representations** – databases produced and validated by officially recognized organizations and processes.
- **Integration with test / operational systems** – ability to send and receive data between simulation systems, and existing and future test equipment and operational systems. For example, a simulation may be used to simulate a missile seeker in a test rig in order to evaluate a missile guidance system or the simulation may send and receive messages from an operational mission command system as part of an LVC command exercise.

[1] See Appendix B: StdV-1.

- **M&S Enterprise tools and services -** tools and / or applications that provide common services or capabilities. An enterprise M&S tool / service is available for DoD-wide use and serves more than one domain/community or Component.

Table 3 depicts the DMSRA CV-2 Capability Taxonomy. This view aligns the technical capabilities with the business goals and objectives in the CV-1. The CV-2 is represented in a cross-reference table because the DMSRA CV-2 has multiple inheritances, not single inheritance (i.e. technical capabilities support multiple business goals and objectives).

Table 3. CV-2 Capability Taxonomy

	Business Goals & Objectives								
Capabilities	Multi- & Inter-Domain Support	Realistic Simulation Environments	Consistency of Outputs & Outcomes	Leverage DoD IT Infrastructure	Leverage Existing M&S Assets	Reduced Lifecycle Costs	Reduced Operational Complexity	Secure Accessibility	Agility & Innovation
Remote execution				X		X			
Thin client access				X		X			
Modular components		X	X			X			X
SOA-based architecture				X		X			X
Standards based interfaces	X		X		X	X			X
Well documented	X					X		X	X
Accommodate occasional / sporadic connectivity				X	X		X	X	
Scalable					X	X	X		X
Cross domain solutions				X	X		X	X	X
IA / Secure Accessibility				X	X		X	X	
Authoritative data representations		X	X					X	
Integration with test / operational systems	X	X			X				
M&S Enterprise Tools/Services			X		X			X	

CV-4 Capability Dependencies

The CV-4 defines dependencies among planned capabilities and logical groupings of capabilities.

Table 4 provides the dependencies between the technical capabilities described in the CV-2. An X in a cell indicates that the capability in the row depends upon the capability in the column, i.e. the capability in the column is necessary to the capability in the row. An S in a cell indicates that the capability in the row is supported by the capability in the column, i.e. it will aid in implementation, but is not necessary.

The first three columns of the CV-4 group the individual capabilities into broader categories of capabilities, all three of which are necessary to a functional M&S system. On one end of the spectrum, for a small standalone model, data / information and services may be completely integrated, and run on a single computer. On the other end of the spectrum, a large distributed exercise (in the future) may pull from multiple data sources, implement dozens of inter-related services, and run across a worldwide network, e.g. JIE implemented.

Table 4. CV-4 Capability Dependencies

Data / Information	**Services**	**Infrastructure / Environment**	**Capabilities**	Remote execution	Thin client access	Modular components	SOA-based architecture	Standards based interfaces	Well documented	Accommodate occasional / sporadic connectivity	Scalable	Cross domain solutions	IA / Secure accessibility	Authoritative data representations	Integration with test / operational systems	M&S Enterprise Tools/Services
		X	Remote execution		S		S						X			
		X	Thin client access	X			S	X					X			
		X	Modular components				S	X	X				S	S		S
		X	SOA-based architecture		S	S		X			S		X			
		X	Standards based interfaces											S		X
X	X		Well documented													S
	X	X	Accommodate occasional / sporadic connectivity												S	
	X	X	Scalable	S		S	S						X			
		X	Cross domain solutions										X			
	X	X	IA / Secure accessibility						S					S		
X			Authoritative data representations													S
		X	Integration with test / operational systems					X		X		X	X	X		
	X		M&S Enterprise Tools/Services	S	S					S			X	S		

PRINCIPLES

This section provides the high-level foundational statements of principles, rules, and values that drive technical positions and patterns. The DMSRA principles are derived from both the DMSRA goals and objectives, and DoD IEA principles. Each DMSRA rule is derived from exactly one DMSRA principle. For rules that are applicable to multiple principles, we selected the most relevant principle.

The DMSRA is not a policy statement. The principles and rules of the DMSRA use the term "should" to mean a course of action that is recommended unless inappropriate for a particular circumstance. All DoD IEA principles have been included for completeness and context.

Appendix A lists the DMSRA Principles and Rules in the DoDAF Services Rules Model (SvcV-10a) format. The principles and rules of the Joint C2 (JC2) RA have been incorporated into the DMSRA principles and rules below when JC2 architecture design principles and rules are shared by Defense M&S or vital for C2 / simulation interoperability. Cross-references to the JC2 RA and other source documents are listed in the Notes column.

Mapping of Principles to Technical Capabilities

Table 5 maps DoD IEA and DMSRA principles to the technical capabilities described in the Strategic Purpose section. The DMSRA principles guide architecture and M&S asset design and development using the desired characteristics defined by the technical capabilities.

Table 5. Mapping of Principles to Technical Capabilites

Principle#	Remote execution	Thin client access	Modular components	SOA-based architecture	Standards based interfaces	Well documented	Accommodate occasional / sporadic connectivity	Scalable	Cross domain solutions	Cybersecurity conformant	Authoritative data representations	Integration with test / operational systems	M&S Enterprise Tools/Services
GP 01	x	x	x	x	x	x	x	x	x	x	x	x	x
GP 02			x	x	x				x			x	x
GP 03						x			x				x
GP 04			x	x	x	x		x					
GP 04.1			x	x	x	x		x					
GP 05	x	x		x	x	x			x	x			
GP 05.1	x	x							x	x			
GP05.2				x	x	x							
GP 06			x	x									

Principle#	Remote execution	Thin client access	Modular components	SOA-based architecture	Standards based interfaces	Well documented	Accommodate occasional / sporadic connectivity	Scalable	Cross domain solutions	Cybersecurity conformant	Authoritative data representations	Integration with test / operational systems	M&S Enterprise Tools/Services
GP 06.1			x	x									
DSDP01			x	x							x		x
DSDP01.1			x	x							x		x
DSDP02	x		x	x	x	x		x				x	
DSDP02.1	x			x									
DSDP02.2					x							x	
DSDP02.3	x	x		x				x					
DSDP02.4			x	x	x	x						x	
DSDP03	x		x	x	x						x		
DSDP03.1			x	x	x						x		
DSDP03.2	x		x	x	x								
DSDP03.3											x		
DSDP04			x			x							
DSDP04.1			x			x							
DSDP04.2			x			x							
DSDP05	x	x	x	x	x	x	x				x	x	x
DSDP05.1							x				x		
DSDP05.2											x		
DSDP05.3				x		x							
DSDP05.4											x		
DSDP05.5	x	x											
DSDP05.6	x		x	x		x							
DSDP05.7	x		x	x		x							
DSDP05.8				x		x					x		
DSDP05.9	x	x					x						
DSDP05.10				x									x
DSDP05.11												x	

Principle#	Remote execution	Thin client access	Modular components	SOA-based architecture	Standards based interfaces	Well documented	Accommodate occasional / sporadic connectivity	Scalable	Cross domain solutions	Cybersecurity conformant	Authoritative data representations	Integration with test / operational systems	M&S Enterprise Tools/Services
SAP01							x		x	x			
SAP01.1							x		x	x			
SAP01.2							x		x	x			
SAP02							x			x			
SAP02.1							x			x			
SAP03										x			
SAP04									x	x			
SAP04.1									x	x			
SAP04.2										x			
SIP01							x						
SIP02							x						
SIP03								x					
CIRP01	x	x					x	x					
CIRP02	x	x			x		x			x		x	
CIRP02.1	x	x			x		x			x		x	
CIRP03										x			
CIRP04	x	x					x	x					
CIRP04.1	x	x					x	x					

TECHNICAL POSITIONS AND POLICIES

This section describes the Technical Positions for standards in the DMSRA. The standards are recommended for solution architectures in Defense M&S within the scope of this document. The selected standards are based on current M&S assets, evolving technologies, and gaps in Defense M&S standards, and the architecture approach formulated in the DMSRA. The Defense M&S standardization goal is improving interoperability and supportability while reducing total ownership costs of M&S assets through common processes, standard practices, open systems, and optimized systems engineering. The selected standards are based on current M&S assets, evolving technologies, and gaps in Defense M&S standards, and the architecture approach formulated in the DMSRA.

There are a many standardization documents for Defense M&S. These documents are maintained and registered in several locations. Where applicable, the profile includes the Defense Information Technology Standards Registry (DISR) [7] and/or the Acquisition Streamlining and Standardization Information System (ASSIST) [8] identifiers, and status (e.g., mandated or emerging etc.).

The DMSRA standards in this document are Defense M&S-specific or critical for Defense model, simulation, and M&S service development. To facilitate M&S integration into operational or other domain-specific systems/applications, developers should consult additional standards. For example, a Service's M&S program that interfaces with Joint C2 systems should consult the applicable RA and standards profile. That RA and profile may include guidance and standards that apply to the program but are outside the scope of the DMSRA.

Of note, adopting new standards can drive additional costs during new system development or when updating legacy systems to maintain interoperability. Program managers must balance the decision to standardize against specific interoperability and mission requirements, technology growth desires, and cost effectiveness. This reference architecture and the associated standards profile can help program managers make informed standardization decision.

Technical Positions for M&S Standards in StdV-1

The M&S Standards Viewpoint 1(StdV-1) in Appendix B, provides a summary of adopted standards listed in the Defense M&S Related Standards and Best Practices Guide, and corresponds to the Defense M&S Standards Profile. The use of standards in this section helps enable interoperability across Defense M&S capabilities, including interoperability with legacy systems. The purpose of the Defense M&S StdV-1 is to support interoperability with legacy systems, while new technologies and standards are developed, identified, and implemented to achieve the DMSRA vision and goals.

DISR use is mandated for developing and acquiring new or modified fielded IT systems throughout the DoD, but a Defense M&S capability need not implement all the mandated standards in the DISR. However, if a mandated or emerging standard applies to that capability, use of a competing standard requires justification per the Department of Defense Instruction 8310.01, "Information Technology Standards in the DoD" [9].

Technical Position for M&S Standards in StdV-2

Application of standards in the Defense M&S StdV-1 alone will not achieve the DMSRA vision. The Defense M&S Standards Viewpoint (StdV-2) in Appendix C, serves as a placeholder for emerging standards and gaps in standards needed to fulfill the DMSRA vision and enable transition to a more modular, service-oriented, and cloud-based architecture. Some standards are independent of this transition. Regular updates and emerging successor standards may be included.

ARCHITECTURAL PATTERNS

This section provides guidance and best practices for implementing operational and service principles and rules. It is comprised of two parts. The first part provides an "enterprise-level" description of architectural states during the migration to a composable enterprise architecture. The second part provides a series of patterns. Patterns document best practices and references/resources for applying the principles documented above. [12]

Enterprise Architecture Migration

This section describes three architectural states- the "as-is" M&S architecture, the "to-be" composable M&S enterprise architecture, and the transitional intermediate architecture which will exist during migration between the first two.

<u>Current Architecture</u>

In today's "as-is" Enterprise Architecture (EA), Figure 4, developers create simulations to support one or more missions. Each simulation uses various models necessary to satisfy mission requirements. These models may have been developed as part of the simulation program. More likely however, these models resulted from separate efforts in government, academia, and industry. These models are only common among simulations at the algorithm level. This commonality is typically captured in documentation. Based upon that simulation's specifications, developers code each of the models for each simulation individually. In some cases, where no single simulation is sufficient to meet mission requirements, developers may use a simulation federation. In a federation, multiple simulations interoperate to fulfill the mission requirements. It is common for different simulations in the same federation to have different implementations of same model. Advantages and disadvantages of the current EA are listed in **Table 5**.

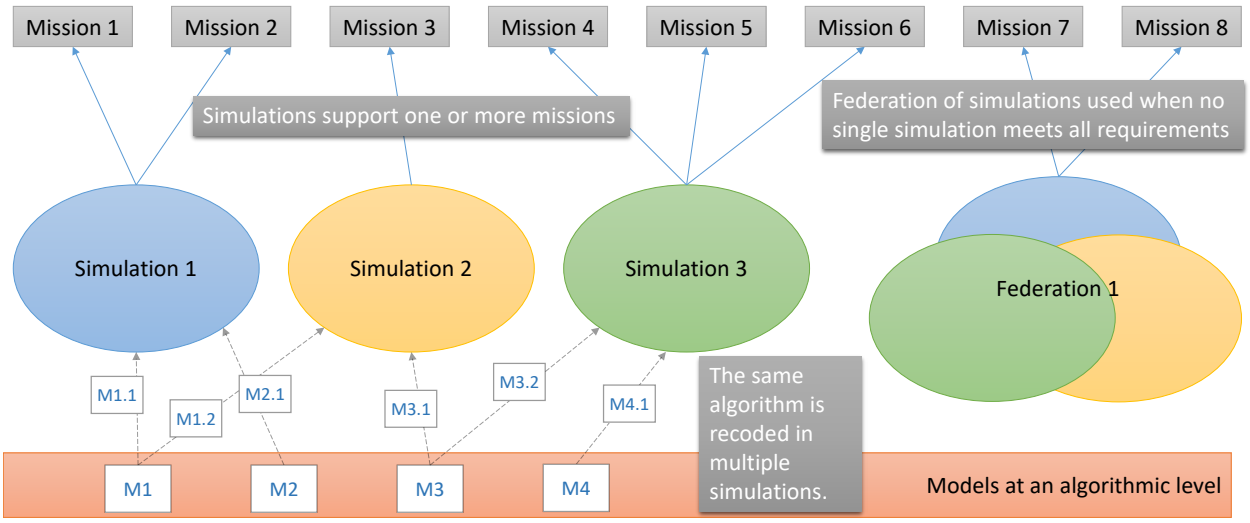

Figure 4. Current EA

Table 5. Advantages and Challenges of Current EA

Advantages	Disadvantages
• Models can be optimized for use within the simulation and for any simulation specific hardware. • Coding the models gives simulation developers a better appreciation of the models. • Simulation programs can be tightly coupled to their mission. • Governance, including funding, structures exist and have grown up around this EA.	• Models are coded multiple times. This increases development time and cost and introduces more opportunities for coding errors to slip through. • If a model is updated, there is no easy way to implement that change in all simulations using that model. • This can lead to larger simulations. Larger simulations typically cost more to use and maintain. • Every simulation is a unique development project where interoperability is typically not a primary design factor resulting in high integration costs.

Composable M&S Enterprise Architecture

The long-term objective is a composable EA, shown in **Figure 5**. Models are coded once into reusable modules. Individual simulations reuse these modules along with simulation-unique code to satisfy their individual missions. Combining reusable models (composing) to form a simulation is the core concept of composability. Composability should result in quicker, cheaper, and more robust simulation development. Tailored simulations would be created for individual missions and federations would not be necessary. Instead of creating a federation to meet specific mission needs, a new simulation would be composed utilizing a common framework. By creating a new, tailored simulation, the user eliminates the non-mission-related code that existing simulations retain. This extra code adds to maintenance costs and inhibits interoperability. Both technical and governance challenges currently exist to implement a composable EA. **Table 6** identifies some advantages and disadvantages of the composable EA.

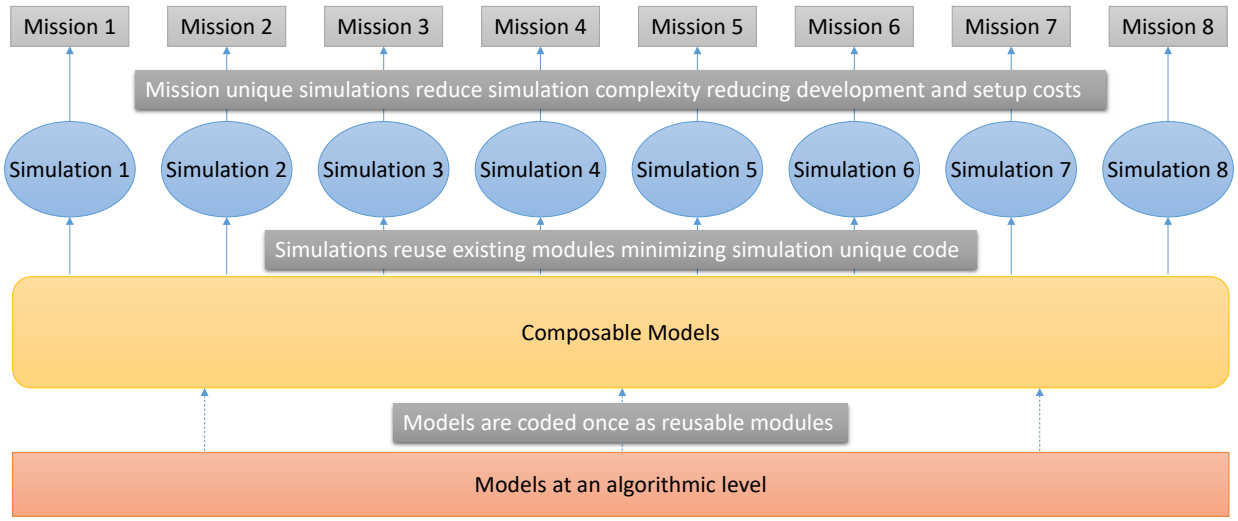

Figure 5. Composable EA

Table 6. Advantages and Disadvantages of Composable EA

Advantages	Disadvantages
• Models are coded once, reducing development time and cost. • Easy to replace models with newer versions that use the same interface. • Smaller simulations should lead to easier use and reduced maintenance costs. • Conducive to cloud computing infrastructure.	• Existing simulation base would need to be rewritten or adapted to the composable framework. • Simulation developers are dependent on model developers that may not be in their program chain. This will require simulation program managers to accept some risk. • New governance structures required. • New standards required to facilitate composability of models.

Intermediate M&S Enterprise Architecture

Figure 6 represents an intermediate step between the current EA and the composable EA, where only some programs have adopted a composable or composable-like architecture. This is the likely near future direction since several DoD organizations/programs are planning to implement composable architectures. This EA may be a natural evolution from today's as-is EA to a composable architecture.

Reducing the cost of compatibility will require coordination and joint decision-making during this transition period. The DMSRA is one means to affect that coordination. Failure to coordinate will almost certainly result in non-compatible architectures that will take large investments in the future to harmonize. This is the case today where simulations have been written to support various interoperability protocols and require significant efforts to federate. In any case, it is likely that non-composable simulations and federations will continue to exist for a significant time if they fulfill a need and there is no compelling reason to change.

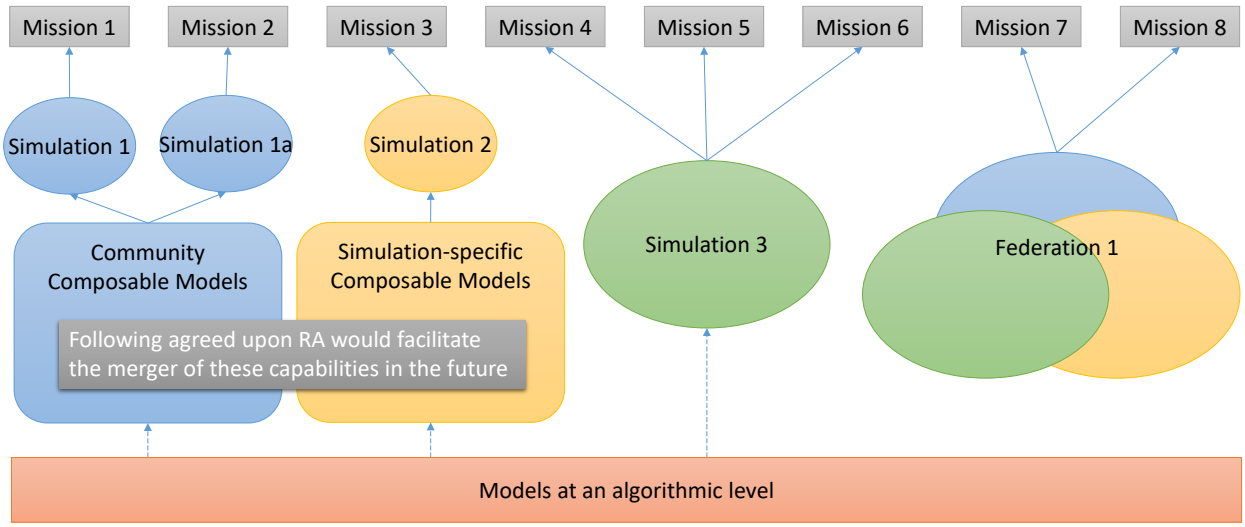

Figure 6. Intermediate EA

Composable Architecture and Migration Patterns

This section describes the DMSRA patterns addressing migration to a composable architecture. These patterns are each mapped to the applicable standards and DMSRA principles and rules. Since some of the desired capabilities are still in development, some standards and best practices may only partially realize the principle or rule they address. Where time and resources were not available to complete a pattern for this DMSRA release, a title and brief description of the need is provided. Once completed, these patterns will be included in Appendices D through N.

<u>Cloud Migration – Appendix D</u>
Cloud computing has been widely accepted as the preferred IT business model within the Federal Government and DoD moving forward. This pattern guides the user to:

- Determine the suitability of an organizational capability for migration to the cloud
- Identify the appropriate cloud service and deployment models
- Formulate a quantitative framework for identifying a suitable cloud service provider (CSP)

<u>Decomposition of Simulations into Modular Components – Appendix E</u>
Modular components are self-contained functions, often dependent on other components to provide a capability. These components can be in the form of services which are loosely coupled and composable. This pattern guides the user to determine the suitability of a simulation for decomposition into modular components.

<u>Verification and Validation of Modular Components- Appendix F</u>
Verification and Validation (V&V) are processes used to build trust and credibility in a component. V&V of modular components and composed simulations requires additional considerations. This pattern guides the user to:

- Identify and describe the intended use for a modular component or composed simulation
- Identify V&V limitations
- Assess risk of using component
- Based on the intended use and risk associated with use of a component, or composed simulation, formulate a V&V plan.

<u>Documentation – Appendix G</u>

Documentation is key to using and reusing all the technical capabilities defined in the DMSRA. Without technically accurate, correctly formatted, discoverable documentation, technical capabilities cannot be used and reused. This pattern guides the user to:

- Identify the types of documentation necessary to achieve the DMSRA vision
- Identify the documentation formats relevant to specific types of capabilities
- Identify potential venues for hosting documentation to make it broadly available

SOA Primer - Appendix H

This pattern will introduce SOA, providing standards, resources and best practices to guide the user in application of DMSRA Principle DSDP02.1, “Create a SOA”.

Remote Execution - Assessing Feasibility - Appendix I

This pattern will guide the user through assessing the feasibility of remote execution for services and composed simulations.

Data - Appendix J

This pattern will guide the user through considerations for how data is managed (e.g. stored, accessed, secured) in a SOA or cloud-based architecture by modular components.

Accommodating Occasional / Sporadic Connectivity - Appendix K

This pattern will help the user address occasional or sporadic connectivity issues in architecture and component design.

Cross Domain Solutions - Appendix L

This pattern will guide the user through considerations for selection of a cross domain solution.

Distributed Simulation/ Federation Engineering - Appendix M

This pattern will guide the user through federation engineering and distributed simulation considerations.

Enterprise Services - Appendix N

This pattern will guide the user on use of enterprise services and a description of services available.

Gaming Architectures - Appendix O

This pattern will guide the user on use of commercial gaming and game technologies, architectures, and the latest innovations in network protocols, cloud computing, and graphics processing - to build massively scalable, connected, immersive worlds for individual and collaborative purposes. The DoD M&S community can in some cases take advantage of these commercial advances for entity level simulations.

VOCABULARY

Glossary

Application - a set of computer programs designed to permit the user to perform a group of coordinated functions, tasks, or activities. [10]

Architecture Pattern - Patterns are models of architecture representations at a level of generality that provides some degree of reuse.[12]

Cloud Computing - Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." [11]

Infrastructure as a Service - the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls) [11].

Platform as a Service - the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations [11].

Reference Architecture – an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions [12].

Service Oriented Architecture - an architectural style that supports a logical representation of a repeatable business activity that has a specified outcome [13].

Software as a Service - the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [11].

Solution Architecture – A Solution Architecture is a framework or structure that portrays the relationships among all the elements of something that answers a problem. It describes the fundamental organization of a system, embodied in its components, their relationships with each other and the environment, and the principles governing its design and evolution.[12]

Acronyms

ADORA	Active Directory Optimization Reference Architecture
API	Application Programming Interface
ASSIST	Acquisition Streamlining and Standardization Information System
BOM	Base Object Model
C2	Command and Control
C2IEDM	Command and Control Information Exchange Data Model
C-BML	Coalition Battle Management Language
CDPE	Common Data Production Environment
CIO	Chief Information Officer
COI	Community of Interest
CONOPS	Concept of Operations
COTS	Commercial-off-the-Shelf
DDMS	Department of Defense Discovery Metadata Specification
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISR	Defense IT Standards Registry
DMSCO	Defense Modeling & Simulation Coordination Office
DMSRA	Defense Modeling & Simulation Reference Architecture
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DODIN	Department of Defense Information Networks
DSE	Data Services Environment
DSEEP	Distributed Simulation Engineering and Execution Process
DTED	Digital Terrain Elevation Data
EA	Enterprise Architecture
EDS	Enterprise Data Services
EMBR	Enterprise Metacard Builder Resource
FEAT	Federation Engineering Agreements Template
FEDEP	Federation Engineering and Development Process
FedRAMP	Federal Risk and Authorization Management Program
FOM	Federation Object Model
GeoTIFF	Geographic Tagged Image File Format
GML	Geography Markup Language
HLA	High Level Architecture
IEA	Information Enterprise Architecture
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information Technology
JC3IEDM	Joint Command, Control and Consultation Information Exchange Data Model

JIE	Joint Information Environment
KML	Keyhole Markup Language
M&S	Modeling and Simulation
MODAF	Ministry of Defence Architecture Framework
MSDL	Military Scenario Definition Language
NATO	North Atlantic Treaty Organization
NEC	NSG Entity Catalog
NFDD	NSG Feature Data Dictionary
NSG	National System for Geospatial-Intelligence
O&S	Operations & Sustainment
OGC	Open Geospatial Consortium
OMG	Object Management Group
OMT	Object Model Template
PaaS	Platform as a Service
RA	Reference Architecture
RPG	Recommended Practices Guide
SaaS	Software as a Service
SCORM	Sharable Content Object Reference Model
SEDRIS	Synthetic Environment Data Representation and Interchange Specification
SIMPLE	Standard Interface for Multiple Platform Link Evaluation
SISO	Simulation Interoperability Standards Organization
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SRM	Spatial Reference Model
STANAG	(NATO) Standards Agreements
SysML	Systems Modeling Language
T&E	Test and Evaluations
TDS	Topographic Data Store
TIFF	Tagged Image File Format
TDL	Tactical Data Link
TSPI	Time-Space-Position Information
UI	User Interface
UML	Unified Modeling Language
V&V	Verification and Validation
VDT	VV&A Documentation Tool
VMF	Variable Message Format
VV&A	Verification, Validation, and Accreditation

REFERENCES

[1] Federal Cloud Computing Strategy, U.S. Chief Information Officer, 8 Feb 2011. https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf

[2] DoD Information Enterprise Architecture v2.0, DoD Chief Information Officer, July 2012. http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2%200_Volume%20II7 %20Document_Final_20120806.pdf

[3] Cloud Computing Strategy, DoD Chief Information Officer, 5 Jul 2012. http://www.defense.gov/news/DoDCloudComputingStrategy.pdf

[4] Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS), Defense Information Systems Agency, 25 Jan 2013.

[5] Active Directory Optimization Reference Architecture, version 1.0, December 15, 2010 http://dodcio.defense.gov/Portals/0/Documents/DIEA/ADORA_Final_v1_20101215.pdf

[6] The Department of Defense Architecture Framework (DoDAF) Version 2.02. 3 March 2011. http://cio-nii.defense.gov/sites/dodaf20/index.html

[7] Defense IT Standards Registry, https://gtg.csd.disa.mil/disr

[8] Acquisition Streamlining and Standardization Information System (ASSIST) data base, https://assist.dla.mil/online/start/

[9] DODI 8310.01, "Information Technology Standards in the DoD," February 2, 2015

[10] Definition: Application Software, https://en.wikipedia.org/wiki/Application_software

[11] NIST SP 800-145, "The NIST Definition of Cloud Computing," Version 15; www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

[12] Reference Architecture Description http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf

[13] The Open Group Standard for SOA Reference Architecture (SOA RA). December 2011. https://www2.opengroup.org/ogsys/catalog/C119

[14] "The SOA Source Book" http://www.opengroup.org/soa/source-book/soa/soa.htm

[15] DoD VV&A Recommend Practices Guide, http://msco.mil/vva_rpg.html

[16] VV&A Documentation Tool (VDT), http://vdt.msco.mil/

[17] DoD M&S Catalog, http://mscatalog.msco.mil/

APPENDIX A: DMSRA Principles and Rules

Structure of DMSRA principles and rules: The DoD IEA Principles numeric identifiers have been retained and are the basis for DMSRA Principle identifiers. The DMSRA principles have been mapped to the DoD IEA Principles and are annotated according to the DoD IEA parent principle and a sequential decimal. For example, DMSRA Principle GP04.1, builds upon and provides M&S specific guidance related to DoD IEA Principle GP04. DMSRA rules are aligned to DMSRA principles and are annotated by their associated DMSRA Principle and a sequential numeric identifier. For example, DMSRA Rule GP04.1 01 is the first rule aligned to DMSRA Principle GP04.1. The sequence of principles and rules does not indicate importance or priority.

DMSRA Principles and Rules (SvcV-10a)

Principle#	Rule#	Simple Statement	Notes
GP 01		Department of Defense Chief Information Officer (DoD CIO)-governed resources are conceived, designed, operated, and managed to address the mission needs of the DoD.	This principle is the basis from which all following principles are derived.
GP 02		Interoperability is a DoD strategic goal. All parts of the Global Information Grid (GIG) must work together to achieve this goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. The DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance.	
GP 03		Data assets, services, and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.	
GP 04		DoD CIO services shall advertise service-level agreements (SLAs) that document their performance and shall be operated to meet that agreement.	
GP 04.1		Defense M&S services should be operated in accordance with service level agreements (SLAs).	
	GP04.1 01	M&S services should advertise service level agreements (SLAs)	In the future, services or an enterprise catalog or repository is envisioned for publishing SLAs, metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts.
	GP04.1 02	SLAs should include M&S service's performance and minimum up time; to support monitoring, failover, and load balancing.	Performance and minimum up time information are considered by consumers when making decisions, including those regarding service selection, scope of use, and appropriate redundancy or backup configurations.

GP 05		The GIG will provide a secure environment for collaborative sharing of information assets (information, services, and policies) with DoD's external partners, including other Federal Departments and Communities of Interest (e.g., Department of Homeland Security, the Intelligence Community), state and local governments, allied, coalition, non-governmental organizations (NGOs), academic, research, and business partners.	
GP 05.1		M&S capabilities must comply with cybersecurity policies and guidance for cross domain information sharing.	The policy includes: - CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities* - DODI 8540.01, *Cross Domain (CD) Policy* - DODI 8500.01, *Cybersecurity* - DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations* - DODM 5200.01 Vol1, *DoD Information Security Program: Overview, Classification, and Declassification* - DODM 5200.01 Vol2, *DoD Information Security Program: Marking of Classified Information* - DODM 5200.01 Vol3, *DoD Information Security Program: Protection of Classified Information* - DODM 5200.01 Vol4, *DoD Information Security Program: Controlled Unclassified Information* For more information, see http://iase.disa.mil/cdes/Pages/index.aspx
	GP05.1 01	If an M&S capability requires cross domain information flows, the capability developer should contact and work with the appropriate cross domain support element (CDSE) to address its requirements.	Adapted from: JC2 RA A132r1
	GP05.1 02	M&S capabilities that enable the sharing or transfer of information across multiple security levels should use Enterprise Cross Domain Services (ECDSs) if the services meet their needs.	See note above. Adapted from: JC2 RA A364

GP05.2		Agreements among interoperable/federated simulations are used to define common design, execution, management, data, infrastructure, and modeling agreements.	Adapted from: JC2 RA GP05.2
GP 06		The DIE will include global access to common DoD-wide capabilities and services that enable access to people and information resources from any computer in the world. To the extent possible, services shall be developed for global use. The use of these globally accessible services will improve warfighting effectiveness, and interoperability, while reducing cost.	
GP 06.1		Modular frameworks are used to allow incremental development (including requirements), more manageable development and fielding, and continuous user inputs with capability demonstrations.	
DSDP01		Data, services, and applications belong to the enterprise. Information is a strategic asset that cannot be denied to the people who need it to make decisions.	
DSDP01.1		Existing enterprise data, services, and end-user interfaces are used whenever possible, practical, and appropriate, instead of re-creating those assets.	
DSDP02		Data, services, and applications should be loosely coupled to one another. The interfaces for mission services that an organization provides should be independent of the underlying implementation. Likewise, data has much greater value if it is visible, accessible, and understandable outside of the applications that might handle it.	
DSDP02.1		Create a SOA.	Adapted from: JC2 RA DSDP 02.1
	DSDP02.1 01	A service-oriented environment should provide a user interface for rapid composition of reusable modular services to perform a task.	Improves flexibility and enables reuse.

	DSDP02.1 02	Defense M&S capabilities should be made available to the enterprise comprised of network-based services with published, well-defined interfaces.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts.
	DSDP02.1 03	Data, services, and applications should be loosely coupled to one another. The interfaces for services that an organization provides should be independent of the underlying implementation.	New M&S services should be designed to be modular, adhering to the tenets of high cohesion and low coupling.
DSDP02.2		Solution architectures give preference to standards and technologies that support interoperability with other DoD Components.	
	DSDP02.2 01	M&S capability interfaces should be compliant with adopted standards.	
	DSDP02.2 02	When a standard that is not currently adopted is selected, the standard should be proposed for adoption.	
DSDP02.3		Modular components of a Defense M&S Capability comply with the same design and interoperability standards.	Adapted from: JC2 GP 04.1
	DSDP02.3 01	Defense M&S capabilities should include an interface description document that describes the interface of the capability in enough detail to enable connectivity to each of the capabilities services.	A capability developer should be able to read this document and figure out how to connect to the service without further technical support. Adapted from: JC2 RA A032
	DSDP02.3 02	The capability interface description document should include at least one example of how to connect to each service.	Adapted from: JC2 RA A198
DSDP03		Only handle information once (the OHIO principle). Information that exists should be reused rather than recreated.	
DSDP03.1		Defense M&S services should use standardized data management technologies (e.g. XML, JSON, and NIEM) to improve flexibility for processing and mediating data.	Adopted from: JC2 RA DSDP 03.4
DSDP03.2		Data services enable access to information by a variety of consumers.	Adopted from: JC2 RA DSDP 03.2

DSDP03.3		Defense M&S data providers assign unique identifiers to data/information resources to support external access	Adapted from: JC2 RA DSDP 03.3
DSDP04		Semantics and syntax for data sharing should be defined on a community basis. Information sharing problems exist within communities; the solutions must come from within those communities.	
DSDP04.1		Vocabularies are reused to define common concepts and extend them for community needs.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adopted from: JC2 RA DSDP04.1
	DSDP04.1 01	M&S asset developers should develop, adopt, and register taxonomies, controlled vocabularies, and ontologies of common concepts for discovery content and message content in a namespace governed by a Community of Interest (COI) prior to deploying assets.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA A314
	DSDP04.1 02	DoD adopted data format standards should be used to improve the exchange and accuracy of data and improve compatibility between services.	
DSDP04.2		Semantic technologies enable taxonomical classifications for information resources and definition of controlled vocabularies.	Adopted from: JC2 RA DSDP04.6
DSDP05		Data, services, and applications must be visible, accessible, understandable, and trusted by “the unanticipated user”. All needs can never be fully anticipated. There will inevitably be unanticipated situations, unanticipated processes, and unanticipated partners. By building capabilities designed to support users outside of the expected set, the Department can achieve a measure of agility as a competitive advantage over our adversaries.	

DSDP05.1		Authoritative data in legacy M&S capabilities is made available by data services whenever possible, practical, and appropriate.	Adapted from: JC2 RA DSDP 05.1
DSDP05.2		Model and simulation services and applications use authoritative data assets whenever available and appropriate.	Adapted from: JC2 RA DSDP 05.2
DSDP05.3		XML artifacts and service interface documentation are published.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA DSDP 05.3
	DSDP05.3 01	M&S developers should publish and update XML artifacts prior to deploying and updating capabilities.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA A049 and A051
	DSDP05.3 02	M&S developers should upload technical documentation for the service interface as part of the service registration activities.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Derived from: JC2 RA A054
	DSDP05.3 03	M&S developers should assert the relationship between an older and a new version of an XML artifact when the new artifact is published.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA A055
DSDP05.4		M&S authoritative data producers describe and advertise data assets and capabilities.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, interface documentation, validation information, and contracts. Adapted from: JC2 RA DSDP 05.5
DSDP05.5		Host M&S capabilities so they are accessible across the relevant network(s).	Adapted from: JC2 RA DSDP 05.6

DSDP05.6		M&S services purpose and capabilities should be documented, including information about applicability, level of trust and credibility.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts.
	DSDP05.6 01	Verification and Validation (V&V) information should be documented and published in compliance with adopted standards and policy.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts.
DSDP05.7		M&S asset developers should publish and maintain metacards for the discovery of M&S assets.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts.
	DSDP05.7 01	M&S asset developers should create metacards for the information resources exposed by a web service environment, subject to operational, security, and environmental constraints.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA A069
	DSDP05.7 02	M&S asset developers should use the same controlled vocabularies for discovery content and message content when appropriate	Adapted from: JC2 RA A282r1
DSDP05.8		M&S asset providers publish service and data contracts.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA DSDP 05.8
	DSDP05.8 01	An M&S asset provider may include a use agreement form as part of the amplifying information published with the contracts.	In the future, services or an enterprise catalog or repository is envisioned for the purpose of publishing metadata, taxonomies, vocabularies, interface documentation, validation information, and contracts. Adapted from: JC2 RA A052
DSDP05.9		Defense M&S capabilities utilize common access mechanisms to enable access to Defense M&S modular components.	Adapted from: JC2 RA DSDP 05.10

	DSDP05.901	Thin client presentation interfaces should conform to the HTML or Extensible HTML (XHTML) standards, and not use browser-specific extensions.	Adapted from: JC2 RA A016
	DSDP05.902	Thin client presentation interfaces should be designed in accordance with adopted standards of the World Wide Web Consortium (http://www.w3.org/standards/) to ensure browser compatibility.	Derived from: DODI 8550.01, DoD Internet Services and Internet-based Capabilities. Security Technical Implementation Guides (STIG) for current browsers used in DoD are available at http://iase.disa.mil/.
DSDP05.10		Defense M&S capabilities should leverage Defense M&S enterprise services if the services meet their needs.	
DSDP05.11		When intended to support test or operational systems, Defense M&S capabilities must conform to DoD test and interoperability policy and guidance.	
SAP01		The GIG is critical to DoD operations and is a high-value target for many highly motivated and well-equipped adversaries. As such, it must be conscientiously designed, managed, protected, and defended.	

SAP01.1		Defense M&S capabilities should comply with, and be protected in accordance with, applicable cybersecurity policy and law.	Policies include: - DODI 8500.01, Cybersecurity - DODI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations - DODI 8510.01, Risk Management Framework (RMF) for DoD Information Technology - DODI 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense - DODI 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense - DODI 8310.01, Information Technology Standards in the DoD - DODI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS) - CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND) - CJCSI 6285.01, Multinational and other Mission Partner (MNMP) Information Sharing Requirements Management Process
SAP01.2		Defense M&S capabilities should protect data in transit and at rest according to their confidentiality level, Mission Assurance category, and level of exposure.	Adapted from: DoD IEA, SAR 01
SAP02		The globalization of information technology, particularly the international nature of hardware and software (including supply chain) development and the rise of global providers of Information Technology (IT) and communications services presents a very new and unique security challenge. GIG resources must be designed, managed, protected, and defended to meet this challenge.	
SAP02.1		The requirements and design of Defense M&S capabilities include cybersecurity solutions sufficient for all projected and intended deployment environments.	

SAP03		Global missions and globally dispersed users require global network reach. Information Assurance mechanisms and processes must be designed, implemented, and operated to enable a seamless DoD Information Enterprise.	
SAP04		Agility and precision are the hallmark of 21st century national security operations. Information Assurance mechanisms and processes must be designed, implemented, and operated to enable rapid and precise changes in information access and flow, and resource allocation or configuration.	
SAP04.1		As feasible, Defense M&S capability access control policies and mechanisms are based on user and environmental attributes so that changes in the mapping of users to their attributes can quickly result in changes of access privileges.	Adapted from: JC2 RA SAP 04.1
SAP04.2		Defense M&S capability access control policies and rule sets are maintained in distributed storage that is synchronized or federated so that access policies may be changed and propagated rapidly to other applicable locations.	Adapted from: JC2 RA SAP04.2
SIP01		GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	
SIP02		The GIG shall enable connectivity to all authorized users.	
SIP03		GIG infrastructure must be scalable, changeable, deployable, and rapidly manageable while anticipating the effects of the unexpected user.	
CIRP01		Computing infrastructure must support all missions of the Department, and provide the edge with effective, on-demand, secure access to shared spaces and information assets across functional, security, national, and interagency domains.	

CIRP02		Consolidation of computing infrastructure fixed-node operations is a desired result for cost efficiencies. It shall not be accomplished, however, at the expense of degrading mission capabilities and operational effectiveness.	
CIRP02.1		Defense M&S capabilities can operate across multiple enterprise, regional, and local DoDIN infrastructures as appropriate based on access and interoperability requirements, enterprise value, cost, and security.	
	CIRP02.1 01	Defense M&S capabilities should give preference to hosting on existing cloud infrastructure over creation of new infrastructure if infrastructure to meet operational needs is available.	See Appendix A – Cloud Migration. Adapted from: JC2 RA A399
CIRP03		Computing infrastructure must be able to provide secure, dynamic, computing platform-agnostic and location-independent data storage.	
CIRP04		Computing infrastructure hosting environments must evolve and adapt to meet the emerging needs of applications and the demands of rapidly increasing services.	
CIRP04.1		M&S capabilities leverage cloud technology to ensure efficient use of resources and remote execution.	Adapted from: JC2 RA CIRP 04.1
	CIRP04.1 01	Software modules should be designed so they will work when multiple instances are running.	Adapted from: JC2 RA: CIRP 04.1 A288
	CIRP04.1 02	Adopt the cloud concept of a self-service interface that allows for the provisioning of virtual machines remotely at a centralized data center.	Derived from: NIST Special Publication 800-145: The NIST Definition of Cloud Computing
	CIRP04.1 03	Adopt the cloud concept of data center scalability, to allow the data center to scale-up as future demand for “compute” services increase or decrease.	Derived from: NIST Special Publication 800-145: The NIST Definition of Cloud Computing

	CIRP04.104	Adopt the cloud concept of application level scalability (elasticity) that allows cloud services to scale up and scale down applications on demand.	Derived from: NIST Special Publication 800-145: The NIST Definition of Cloud Computing
	CIRP04.105	Adopt the cloud concept of broad network access, making capabilities available remotely, available over the network and accessed through standard mechanisms on client platforms. (e.g., computers, laptops, mobile phones, etc.)	Derived from: NIST Special Publication 800-145: The NIST Definition of Cloud Computing
	CIRP04.106	Adopt the cloud concept of pooling the cloud provider's computing resources to serve multiple cloud consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include disk storage, processing memory, network bandwidth, application programming interfaces (APIs), and virtual machines.	Derived from: NIST Special Publication 800-145: The NIST Definition of Cloud Computing
	CIRP04.107	Adopt the cloud concept of measured service to automatically control and optimize cloud resource use by leveraging a metering capability appropriate to the type of service, allowing the cloud provider and user to monitor, control, and report resource usage.	Derived from: NIST Special Publication 800-145: The NIST Definition of Cloud Computing

APPENDIX B: Standards Viewpoint 1 (StdV-1)

StdV-1

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
IEEE 1278.1-2012	IEEE Standard for Distributed Interactive Simulation – Application Protocols - Published by IEEE in December 2012	Mandated	Active	Listed in NATO standards profile
IEEE 1278.2-1995	IEEE standard for distributed interactive simulation - application protocols, Reaffirmed 2002	Mandated	Active	Listed in NATO standards profile
IEEE 1278.4-1997	IEEE trial-use recommended practice for distributed interactive simulation - verification, validation, and accreditation, Published Date 20 July 1998	Mandated	Active	Listed in NATO standards profile
IEEE 1516-2010	IEEE 1516–2010 – IEEE Standard for Modeling and Simulation High Level Architecture (HLA) – Federate Interface Specification	Mandated	Active	Listed in NATO standards profile

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
IEEE 1516.1-2010	IEEE 1516.1–2010 – IEEE Standard for Modeling and Simulation High Level Architecture (HLA) – Federate Interface Specification	Mandated	Active	Listed in NATO standards profile
IEEE 1516.2-2010	IEEE 1516.2-2010 – IEEE Standard for Modeling and Simulation High Level Architecture (HLA) – Object Model Template (OMT) Specification	Mandated	Active	Listed in NATO standards profile
IEEE 1516	IEEE 1516-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules	Mandated	Active	Promulgated
IEEE 1516.1-2010	IEEE 1516.1-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Federate Interface Specification Mandated	Mandated		
IEEE 1516.2-2010	IEEE 1516.2-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Object Model Template (OMT) Specification	Mandated	Active	Promulgated

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
IEEE 1730:2010	IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP)	Active I/G	Active	Listed in NATO Standards Profile
ISO 19110:2005 w/Amd 1:2011	Geographic Information – Methodology for feature cataloguing, 11 February 2005, w/Amd 1, 17 June 2011	Mandated	Active	
ISO/IEC 18023-1:2006 w/ Amd 1:2012	Information technology -- SEDRIS -- Part 1: Functional specification, 19 May 2006, , w/Amd 1: 2012	Mandated	Active	Promulgated
ISO/IEC 18023-2:2006(E)	Information technology -- SEDRIS -- Part 2: Abstract transmittal format, 13 July 2006	Mandated	Active	Promulgated
ISO/IEC 18023-3:2006 w/Amd 1:2012	Information technology -- SEDRIS -- Part 3: Transmittal format binary encoding, 13 July 2006 , w/Amd 1: 2012	Mandated	Active	Promulgated
ISO/IEC 18024-4:2006 w/Amd1: 2012	Information technology -- SEDRIS language bindings -- Part 4: C, 19 May 2006, w/Amd 1:2012	Mandated	Active	Promulgated

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
ISO/IEC 18025:2014	Information technology -- Environmental Data Coding Specification (EDCS), 2014	Mandated	Active	Promulgated
ISO/IEC 18026:2009(E)	Information technology -- Spatial Reference Model (SRM), 13 July 2009	Mandated	Active	Promulgated
ISO/IEC 18041-4:2007(E)	Information technology -- Computer graphics, image processing and environmental data representation -- EDCS language bindings -- Part 4: C, 15 August 2007	Mandated	Active	Ratification in Process
ISO/IEC 18042-4:2006 w/Amd 1:2011	Information technology -- Computer graphics and image processing -- Spatial Reference Model (SRM) language bindings -- Part 4: C, 21 July 2006, w/Amd 1: 2011	Mandated	Active	Ratification in Process
ISO/IEC TR 29163-2:2009	Information Technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition – Part 2: Content Aggregation Model Version 1.1, 12/3/2009	Mandated		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
ISO/IEC TR 29163-3:2009	Information Technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition – Part 3: Run-Time Environment Version 1.1, 12/3/2009	Mandated		
ISO/IEC TR 29163-4:2009	Information Technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition – Part 4: Sequencing and Navigation Version 1.1, 12/3/2009	Mandated		
MIL-STD-3022 w/Chg 1	Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations Change 1, 05-Apr-2012	Active I/G	Active	Listed in NATO Standards Profile
MIL-STD-6011F	Tactical Data Link (TDL) 11/11B Message Standard, 30June 2016	Mandated	Active	
MIL-STD-6016E	Tactical Data Link (TDL) 16 Message Standard, 20 July 2012	Mandated	Active	
MIL-STD-6017C	Variable message Format (VMF), 31 May 2012	Mandated	Active	

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
DI-MSSM-81750	Department of Defense (DOD) Modeling and Simulation (M&S) Accreditation Plan		Active	Listed in NATO Standards Profile
DI-MSSM-81751	Department of Defense (DOD) Modeling and Simulation (M&S) Verification and Validation (V&V) Plan		Active	Listed in NATO Standards Profile
DI-MSSM-81752	Department of Defense (DOD) Modeling and Simulation (M&S) Verification and Validation (V&V) Report		Active	Listed in NATO Standards Profile
DI-MSSM-81753	Department of Defense (DOD) Modeling and Simulation (M&S) Accreditation Report		Active	Listed in NATO Standards Profile
NGA.STND.0019_2.0	Time-Space-Position Information (TSPI), Version 2.0 (2012-04-05)	Mandated		
NGA.STND.0026_5.0	NSG Topographic Data Store (TDS) Content Specification, Version 5.0, 20 August 2012	Mandated		
OGC CAT 2.0.2	OpenGIS Catalogue Service (CAT) Implementation Specification (2.0.2), 23 February 2007	Active I/G		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
OGC CAT 2.0.2 – ISO Metadata	OpenGIS Catalogue Services Specification 2.0.2 – ISO Metadata Application Profile 1.0, 2007-07-19	Active I/G		
ISO 19136:2007	Geographic information - Geography Markup Language, 2007-08-23	Mandated		Listed in NATO Standards Profile
OGC GML Application Schema - Coverages, v.1.0.1	OGC GML Application Schema - Coverages, v.1.0.1, 2012-05-11	Mandated		
OGC GML sfp v2.0 w/Cor	Geography Markup Language (GML) simple features profile, v.2.0, 2011-05-24 (with Corrigendum, 2012-04-05)	Mandated		
OGC GMLCOV for GeoTIFF	OGC GML Application Schema -Coverage GeoTIFF Coverage Encoding Profile, 23 August 2014.	**Mandated**		
OGC CDB 1.0	CDB Standard: Model and Physical Data Store Structure Ver1.0 2016-09-23	Emerging		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
OMG UPDM v2.1	Unified Profile for the Department of Defense Architecture Framework (DoDAF) and the Ministry of Defence Architecture Framework (MODAF), Version 2.1, formal/ 2013-08-04 (**sunset date 31 Dec 2019**)	Mandated		
SISO-STD-001	Standard Guidance for Rationale, and Interoperability Modalities (GRIM) for the Real-time Platform Reference Federation Object Model (RPR FOM)		Active	
SISO-STD-001.1	Standard for Real-time Platform Reference Federation Object Model (RPR FOM)		Active	
SISO-STD-002-2006	Standard for: Link16 Simulations (approved 10 Jul 06)	Mandated		Promulgated
STANAG 3809 Edition 4	Digital Terrain Elevation Data (DTED) Exchange Format, 19 January 2004	Mandated	Active	Listed in NATO Standards Profile
T3D v8.0.3	Tasked Target Text Data Version 8.0.3, 10 Feb 2017	Mandated		
SISO-STD-003	Base Object Model (BOM) Template Specification		Active	Listed in NATO Standards Profile

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
SISO-STD-003.1-2006	Guide for Base Object Model (BOM) Use and Implementation		Active	Listed in NATO Standards Profile
SISO-STD-004-2004	Standard for Dynamic Link Compatible HLA API Standard for the HLA Interface Specification (v1.3) *(reaffirmed 19 Nov 2015)*		Active	
SISO-STD-004.1-2004	Standard for Dynamic Link Compatible HLA API Standard for the HLA Interface Specification (IEEE 1516.1 Version) *(reaffirmed 19 Nov 2015)*		Active	
SISO-STD-006-2010	Standard for Commercial Off-the-Shelf (COTS) Simulation Package Interoperability (CSPI) Reference Models *(reaffirmed 19 Nov 2015)*		Active	
STANAG 5602 ED.3	Standard Interface for Multiple Platform Link Evaluation (SIMPLE)		Active	Promulgated
STANAG -5525 ED.1	Joint Command, Control and Consultation Information Exchange Data Model (JC3IEDM)		Active	Ratified
SISO-STD-007-2008	Military Scenario Definition Language (MSDL), 14 October 2008	Emerging	Active	

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
SISO-STD-008-	Standard for Core Manufacturing Simulation Data (CMSD)-UML Model		Active	
SISO-STD-011-2014	Coalition Battle Management Language (C-BML) Phase 1, Version 1.0, 31 October 2013	Emerging	Active	Listed in NATO Standards Profile
SISO-STD-012-2013	Standard for Federation Engineering Agreements Template (FEAT), 2 Aug 2013		Active	
SISO-STD-013-2014	Standard for Common Image Generator Interface (CIGI), Version 4.0, 22 Aug 2014		Active	Listed in NATO Standards Profile
ISO/PAS 17506:2012	Industrial automation systems and integration – COLLADA digital asset schema specification for 3D visualization of industrial data, First Edition, Publically Available Specification, 2012-07-15	Mandated		Listed in NATO Standards Profile
ISO/IEC 19775-1:2013	Information technology -- Computer graphics, image processing, and environmental data representation -- Extensible 3D (X3D) -- Part 1: Architecture and base components, 15 November 2013	Mandated		Listed in NATO Standards Profile

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
ISO/IEC 19775-2:2015	Information technology - Computer graphics, image processing and environmental data representation - Extensible 3D (X3D) - Part 2: Scene access interface (SAI), Edition 3, 2015	Mandated		Listed in NATO Standards Profile
DODAF v2.02	DoD Architecture Framework, Version 2.02, August 2010	Active I/G		Listed in NATO Standards Profile
OMG SysML v1.5	Object Management Group Systems Modeling Language (OMG SysML), version 1.5, May 2017	Emerging		Listed in NATO Standards Profile
OGC KML 2.3 12-007r2	Open Geospatial Consortium (OGC) Keyhole Markup Language (KML), Version 2.3 Document Number 12-007r2, 2015-08-04	Mandated		
OMG UML v2.5	OMG Unified Modeling Language (UML), Version 2.5, March 2015	Mandated		
OGC SWE Service Model 2.0	OpenGIS SWE Service Model Implementation Standard v2.0, 2011-03-21	Mandated		
SWE Common 2.0	OGC SWE Common Data Model Encoding Standard v2.0, 2011-01-04	Mandated		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
GFD-P-R.184	Open Cloud Computing Interface (OCCI) - Infrastructure	Mandated		
OGF GFD-P-R.183	Open Cloud Computing Interface (OCCI) - Core, Open Grid Forum, Grid Final Document.183, June 21, 2011	Mandated		
OGF GFD-P-R.185	Open Cloud Computing Interface (OCCI) - RESTful HTTP Rendering, Open Grid Forum (OGF), Grid Final Document, June 21, 2011	Mandated		
DSP0263 v1.0.1	Cloud Infrastructure Management Interface 5 (CIMI) Model and RESTful HTTP-based Protocol: an Interface for Managing Cloud Infrastructure, 2012-09-12	Emerging		
NIEM Spec v3.0:2014	National Information Exchange Model Conformance Specification, Version 3.0, August 15, 2014	Active I/G		
IETF RFC 7159	JavaScript Object Notation (JSON), Data Interchange Format, March 2014	Active I/G		
IC-TDF.XML.V2014-DEC-r2017-JUL … (other versions retired)	XML Data Encoding Specification for	Mandated		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
	IC-Trusted Data Format, Version 2014-DEC-Revision 2017-JUL			
IC-EDH.XML.V2016- SEP (other versions retired)	XML Data Encoding Specification for IC-Enterprise Data Header, Version 2016- SEP	Mandated		
ARH.XML.V3	XML Data Encoding Specification for Access Rights and Handling, Version 3, 6 September 2013	Mandated		
ISM.XML.V13r.2017-JAN (other versions retired)	XML Data Encoding Specification for Information Security Marking Metadata, Version 13 Revision 2017-JAN (see DISR for retired versions)	Mandated		
ISM.XML.V2016-SEP-r2017-JUL	XML Data Encoding Specification for Information Security Marking Metadata, Version 2016-SEP-Revision 2017-JUL	Mandated		
NTK.XML.V2015-AUG (other versions retired)	XML Data Encoding Specification for Need-to-Know Metadata, Version 2015-AUG (see DISR for older versions)	Mandated		
IC-GENC.CES.V2017-SEP	XML CVE Encoding	Mandated		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
	Specification for Geopolitical Entities, Names and Codes, Version 2017-SEP			
OpenSearch 1.1- 20051206	Open Search 1.1 and Extension-20051206	Mandated		
CDR Deliver V2	IC/DoD Interface Encoding Specification for CDR Deliver, v2, 10 March 2014	Emerging		
CDR REST Retrieve V2.0	IC/DoD REST Interface Encoding Specification for CDR Retrieve, V2.0, 3 October 2012	Mandated		
CDR SOAP Retrieve V2.0	IC/DoD SOAP Interface Encoding Specification for CDR Retrieve, V2.0, 3 October 2012	Mandated		
CDR SOAP Search V3.0	IC/DoD SOAP Interface Encoding Specification for CDR Search, V3.0, 3 October 2012	Mandated		
CDR REST Search V3.0	IC/DoD REST Interface Encoding Specification for CDR Search, V3.0, 3 October 2012	Mandated		
Atom Result Set V2.0	Atom Data Encodign Specification for Content Discovery & Retrieval Result Sets, Version 2, 10 April 2013	Mandated		
AUDIT.XML.V2016-SEP-r2018-FEB	XML Data Encoding	Mandated		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
	Specification for Enterprise Audit Exchange, Version 2016-SEP-Revision 2018-FEB			
IETF Standard 66/RFC 3986	Uniform Resource Identifier (URI): Generic Syntax, January 2005	Mandated		
ISO/IEC 11179-3:2013	ISO/IEC 11179-3:2013, Information Technology – Metadata registries (MDR) – Part 3: Registry metamodel and basic attributes, Third Edition, 2013-02-12	Mandated		
ISO/IEC/IEEE 31320-1-2012	ISO/IEC/IEEE International Standard - Information technology -- Modeling Languages -- Part 1: Syntax and Semantics for IDEF0, 2012	Mandated		
IEEE 31320-2-2012	ISO/IEC/IEEE International Standard - Information technology -- Modeling Languages -- Part 2: Syntax and Semantics for IDEF1X97 (IDEFobject), 2012	Mandated		
OWL 2	OWL 2 Web Ontology Language Document Overview (Second Edition), W3C	Mandated		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
	Recommendation, 11 December 2012			
XML 1.0	Extensible Markup Language (XML) 1.0 (Fourth Edition), (3rd Ed. retired: 2017-12-01)	Mandated		
NGA.STND.0038_1.0.1 WMS	National System for Geospatial-Intelligence (NSG) OGC Web Map Service 1.3 Interoperability Standard, version 1.0.1, 22 May 2013	Emerging		
NGA.STND.0062_1.0_WFS	National Systems for Geospatial Intelligence (NSG) Web Feature Service 2.0 Implementation Profile, v1.0	Emerging		
CORBA 3.3 Part 1,2,3	Common Object Request Broker Architecture (CORBA) Specification, Version 3.3, Part 1,COBRA Interfaces; Part 2, CORBA Interoperability; Part,3 CORBA Components, November 2012	Mandated		
SDSFIE-M v1.0.2	Spatial Data Standards for Facilities, Infrastructure, and Environment (SDSFIE) Metadata, Conceptual Schema, Version	Emerging		

Identifier	Title	DISR Status*	ASSIST Status*	STANAG Status*
	1.0.2, 28 August 2014			
SDSFIE-V v4.0	Spatial Data Standards for Facilities, Infrastructure, and Environment Vector (SDSFIE-V): Specification Document, Version 4.0. 22 April 2016	Mandated		
SMIS v1.0.2	Spatial Data Standards for Facilities, Infrastructure, and Environment (SDSFIE) Metadata, Implementation Specification, Version 1.0.2, 28 August 2014	Emerging		
IEEE1730.1	Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP) Multi-Architecture Overlay (DMAO)		Active	
ISO 19142:2010	Geographic information – Web Feature Service, 6 December 2010	Mandated		
ITOP 1.1.001	General guidance for incorporating modeling and simulation in test operation procedures		Active	

**status as of 17 August 2018*

APPENDIX C: Standards Viewpoint 2 (StdV-2)

(As of May 2016)

StdV-2

Gap	Candidates	Status
Interface specifications	Simple Object Access Protocol (SOAP)	Several SOAP-based specifications for IC/DoD Content Discovery and Retrieval are registered in the DISR
VV&A descriptive metadata to support composability	None	This represents a technical gap for which no standard is in progress.
Conceptual modeling	None	This represents a technical gap for which no standard is in progress.
Semantic metadata to support composability	None	This represents a technical gap for which no standard is in progress.
Simulation decomposition	None	This represents a technical gap for which no standard is in progress.
Cloud - PaaS	OASIS- Cloud Application Protocol (CAMP) v1.1	There are currently no adopted standards in the DISR or ASSIST supporting the Platform as a Service (PaaS) cloud service model.
Multi-Architecture Interoperability	SISO-REF-010-2015 Reference for Enumerations for Simulation Interoperability, Version 21	No adopted standard in DISR or ASSIST providing enumerations for simulation interoperability
M&S Discovery – Metadata Harvesting	OAI-PMH Open Archives Initiative – Protocol for Metadata Harvesting, version 2	No adopted standard in DISR or ASSIST for automating metadata harvesting

APPENDIX D: Cloud Migration

Cloud computing has been widely accepted as the preferred IT business model within the Federal Government and DoD moving forward. This pattern guides the user through a set of questions to:

- Determine the suitability of an organizational capability for migration to the cloud
- Identify the appropriate cloud service and deployment models
- Formulate a quantitative framework for identifying a suitable cloud service provider (CSP)

APPENDIX E: Decomposition of Simulations into Modular Components

Modular components are self-contained functions, often dependent on other components to provide a capability. These components can be in the form of services which are loosely coupled and composable. This pattern guides the user through a set of questions to determine the suitability of a simulation for decomposition into modular components.

APPENDIX F: Verification and Validation of Modular Components

Verification and Validation (V&V) are processes used to build trust and credibility in a component. V&V of modular components and composed simulations requires additional considerations. This pattern guides the user through a set of questions to:

- Identify and describe the intended use for a modular component or composed simulation
- Identify V&V limitations
- Assess risk of using component
- Based on the intended use and risk associated with use of a component, or composed simulation, formulate a V&V plan.

APPENDIX G: Documentation

Documentation is key to using and reusing all the technical capabilities defined in the DMSRA. Without technically accurate, correctly formatted, discoverable documentation, technical capabilities cannot be used and reused. This pattern guides the user through a set of questions to:

- Identify the types of documentation necessary to achieve the DMSRA vision
- Identify the documentation formats relevant to specific types of capabilities
- Identify potential venues for hosting documentation to make it broadly available

APPENDIX H: SOA Primer

This pattern will introduce SOA, providing standards, resources, and best practices to guide the user in application of DMSRA Principle DSDP02.1, “Create a SOA”.

APPENDIX I: Remote Execution

This pattern will guide the user through assessing the feasibility of remote execution for services and composed simulations.

APPENDIX J: Data

This pattern will guide the user through considerations for how data is managed (e.g. stored, accessed, secured) in a SOA or cloud-based architecture by modular components.

APPENDIX K: Accommodating Occasional / Sporadic Connectivity

This pattern will help the user address occasional or sporadic connectivity issues in architecture and component design.

APPENDIX L: Cross Domain Solutions

This pattern will guide the user through considerations for selection of a cross domain solution.

APPENDIX M: Distributed Simulation/ Federation Engineering

This pattern will guide the user through federation engineering and distributed simulation considerations.

APPENDIX N: Enterprise Services

This pattern will provide guidance on use of enterprise services and a description of services available.

APPENDIX O: Gaming Architectures

This pattern will guide using commercial gaming and game technologies, architectures, and the latest innovations in network protocols, cloud computing, and graphics processing to build massively scalable, connected, immersive worlds for individual and collaborative purposes. The DoD M&S community can in some cases take advantage of these commercial advances for entity level simulations. This can be done by leveraging gaming architectures through either the direct use of game engines, application of game specific libraries or services, or replicating the lessons learned from gaming. This pattern focuses on identifying best practices for leveraging commercial gaming technologies for defense modeling and simulation (M&S) in a modular architecture and for integration with Live, Virtual, and Constructive (LVC) capabilities.

In the context of defense M&S, gaming architectures are those built on game engines designed to support the development of video games. This pattern guides the user through a set of questions to:

- Identify M&S domains where gaming and/or game technologies be applied
- Identify if the circumstances exist for an organization to consider applying gaming and/or game technologies
- Determine if policy implications unique to gaming vs traditional M&S are applicable
- Determine if key technical challenges in integrating gaming and/or game technologies apply to an organization's architecture
- Determine if the choice of game engine drives other technical, architectural decisions, and/or the selection of other technologies to be integrated
- Identify factors impact that the choice of game engine

The pattern also identifies:

- Other resources or efforts that might be of interest to organizations looking to applying gaming
- Lessons learned available from other organization about gaming / game technologies
- Game engines that have been applied within the DoD