NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

OPEN SYSTEM ACQUISITION (OSA) PRACTICAL GUIDE

by

Christopher R. Gunderson

May 2015

Approved for public released; distribution is unlimited

Prepared for: Office of the Undersecretary of Defense for Intelligence (OUSD (I))

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
27-05-2015	Technical	01-10-2009 - 27-05-2015

4. TITLE AND SUBTITLE

Open System Acquisition (OSA) Practical Guide

5a. CONTRACT NUMBER
NA

5b. GRANT NUMBER
NA

5c. PROGRAM ELEMENT NUMBER
NA

5d. PROJECT NUMBER
NA

5e. TASK NUMBER
NA

5f. WORK UNIT NUMBER
NA

6. AUTHOR

Christopher R. Gunderson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Christopher R. Gunderson
Department of Information Science
Naval Postgraduate School Monterey CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

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

John Snevely
Office of the Undersecretary of Defense for Intelligence 1400 Defense Pentagon
Washington, DC 20301

10. SPONSOR/MONITOR'S ACRONYM(S)
OUSD (I)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NA

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES
NA

14. ABSTRACT

Government policy has emphasized use of "enterprise," "open," and "collaborative" approaches to building information systems for many years. However, myriad watchdog reports document many failures and relatively few successes. Nevertheless, both successes and failures point to some best practices, and practices to avoid. This high level summary of observations and recommendation, together with the detailed appendices, provide specific, how-to guidance for government Open Enterprise Information System project stakeholders. The guidance is based on eleven years of applied research conducted on behalf of the Office of the Secretary of Defense, and hand-in-hand with information system acquisition practitioners. The template sample language aligns with Intelligence, Surveillance, and Reconnaissance (ISR) systems, but with slight modification the templates will support acquisition of OEIS to support any operational domain.

15. SUBJECT TERMS
Open Systems, Product Line Architecture, Agile Acquisition, Bending the Cost Curve, Plug Fest Plus, Defense Acquisition, Systems Engineering, Information Systems, Intelligence Surveillance and Reconnaissance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Christopher R. Gunderson
Unclassified	Unclassified	Unclassified	Unclassified	58	**19b. TELEPHONE NUMBER** ***(include area code)*** 831 224 5182

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route
President

Douglas Hensler
Provost

The report entitled "Open Systems Acquisition Practical Guide" was prepared for the Undersecretary of Defense for Intelligence and funded by the Defense Intelligence Agency

Further distribution of all or part of this report is authorized.

This report was prepared by:

Author C. R. Gunderson
Title Research Associate

_____
Author
Title

Reviewed by:

_____
Name, Chairman
Department Name

Released by:

_____
Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Government policy has emphasized use of "enterprise," "open," and "collaborative" approaches to building information systems for many years. However, myriad watchdog reports document many failures and relatively few successes. Nevertheless, both successes and failures point to some best practices, and practices to avoid. This high level summary of observations and recommendation, together with the detailed appendices, provide specific, how-to guidance for government Open Enterprise Information System project stakeholders. The guidance is based on eleven years of applied research conducted on behalf of the Office of the Secretary of Defense, and hand-in-hand with information system acquisition practitioners. The template sample language aligns with Intelligence, Surveillance, and Reconnaissance (ISR) systems, but with slight modification the templates will support acquisition of Open Enterprise Information Systems (OEIS) to support any operational domain.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

ABSTRACT 1

OBSERVATIONS 1

RECOMMENDATIONS 3

APPENDIX A: SAMPLE OEIS ACQUISITION STRATEGY 1

1. REQUIREMENT 1
2. RISK MANAGEMENT 3
3. COMPETITION 5
4. METRICS 5

APPENDIX B: SAMPLE OEIS PROJECT WORK STATEMENT (PWS) 1

PART 1 GENERAL INFORMATION 2
PART 2 GOVERNMENT FURNISHED ITEMS AND SERVICES 7
PART 3 CONTRACTOR FURNISHED ITEMS AND SERVICES 7
PART 4 SPECIFIC TASKS 7
PART 5 APPLICABLE PUBLICATIONS 9

APPENDIX B: 01 CONTRACT LINE ITEM NUMBERS (CLIN) 1

APPENDIX B: 02 OSA PROJECT EXECUTION PLAN (PEP) DATA ITEM DESCRIPTION (DID) 1

APPENDIX B: 03 OSA PRODUCT LINE ARCHITECTURE (PLA) DID 7

APPENDIX B: 04 OSA PLUG TEST PLAN DID 1

APPENDIX B: 05 OSA IT USERS' GUIDE DID 1

APPENDIX C: SAMPLE OEIS MEASURES OF PERFORMANCE AND EFFECTIVENESS 1

MEASURES OF PERFORMANCE AND EFFECTIVENESS FOR X-ISR SYSTEM 1
OPERATIONAL SYSTEM-LEVEL METRICS 2
SYSTEM LEVEL MOP: 3
PROCESS-LEVEL MOE: 5

THIS PAGE INTENTIONALLY LEFT BLANK

OPEN SYSTEM ACQUISITION (OSA) PRACTICAL GUIDE

By C. R. Gunderson
Naval Postgraduate School, Department of Information Science

On behalf of Office of the Undersecretary of Defense for Intelligence (OUSD (I))

Abstract

Government policy has emphasized use of "enterprise," "open," and "collaborative" approaches to building information systems for many years. However, myriad watchdog reports document many failures and relatively few successes. Nevertheless, both successes and failures point to some best practices, and practices to avoid. This high level summary of observations and recommendation, together with the detailed appendices, provide specific, how-to guidance for government Open Enterprise Information System project stakeholders. The guidance is based on eleven years of applied research conducted on behalf of the Office of the Secretary of Defense, and hand-in-hand with information system acquisition practitioners. The template sample language aligns with Intelligence, Surveillance, and Reconnaissance (ISR) systems, but with slight modification the templates will support acquisition of Open Enterprise Information Systems (OEIS) to support any operational domain.

Observations

Open system development is fundamentally different than traditional waterfall development. Government PMs are not typically trained in appropriate open system acquisition practices. Likewise government contractors are typically not expert in open system development.

In developing open systems, the most important requirements, and the greatest risk, is associated with carefully scoping, defining and assuring interoperability. Both "operational interoperability", i.e. ability to usefully share networked data and

resources in run time, and "engineering interoperability", i.e. ability to plug-and-play off-the-shelf hardware and software, are critical.

Information Assurance (IA) is an element of both operational and engineering interoperability. Traditional approaches to IA and Certification and Accreditation (C&A) do not adequately address "need-to-share" and severely inhibit ability to achieve the desired level of interoperability.

The objective of open system development is to leverage agile plug-and-play development to improve utility-per-capability, speed-to-capability, and lifecycle cost-per-capability. Success requires carefully defining and testing against objective metrics for each of these objectives.

In the early 1990's the Secretary of Defense recognized that (1) software was becoming an increasingly important aspects of military systems; and (2) that success in acquiring software would require new paradigms that emphasize flexibility and agility. In response, the Office of the Secretary of Defense (OSD) issued Military Standard number 498 (MILSTD 498.) MILSTD 498 provides tailorable templates called Data Item Descriptions (DID). These templates translate laymen's descriptions of requirements associated with software-intensive projects into clear technical descriptions of contract deliverables.

OSD, expecting that better commercial standards would quickly evolve, believed that MILSTD 498 would be become obsolete and stopped maintaining it. However, no commercial standard for best practices across the disciplines of project management, software-intensive systems engineering, and contracting, ever emerged. Fortunately, MILSTD 498 – even though it is not maintained -- remains an excellent tool for crafting procurement artifacts aligned with OEIS.

According to the Defense Acquisition University (DAU) a Systems Engineering Plan (SEP) helps "…Program Managers develop, communicate, and manage the overall systems engineering (SE) approach that guides all technical activities of the program. A SEP documents key technical risks, processes, resources, metrics, SE products, and completed and scheduled SE activities…the Government SEP should accompany the request for proposal (RFP) as guidance to the offerors. The developer's systems engineering management plan (SEMP), which is the contractor-developed plan … should be consistent with the Government SEP…." Despite this clear guidance, frequently the government either does not provide a SEP with its solicitation, or provides a traditional SEP that is not well aligned with OEIS best practices.

Existence of excellent, tailorable, tools such as MILSTD 498 and SEP notwithstanding, government OEIS solicitations and contract award processes tend to reuse legacy boilerplate language and process that is not appropriate for developing modern OEIS.

Recommendations

Use MILSTD 498 , and/or DIDS developed by successful projects, as a guide for tailoring software-intensive contract deliverables.

Identify targeted cost, performance and schedule efficiencies enabled by operational and engineering interoperability. Likewise, identify associated risks that have historically precluded achieving these objectives. Develop a risk/reward optimization strategy and acquisition strategy including for COTS-friendly, OEIS accordingly. (See Appendix (A) for example.)

Use Performance Work Statement (PWS) for contract language, Statement of Objectives (SOO) for solicitations, rather than traditional Statement of Work (SOW) format. PWS and SOO focus on outcomes and encourage contractor innovation. Be careful to provide objective measures of desired outcomes. (See Appendix (B) for example.)

Develop validated and verifiable MOE and MOP, associated threshold and objective values, and test methods. Include these in the PWS and RFP. (See Appendix (C) for example.)

Make IA a critical consideration. Build security in from the ground up, but with need-to-share and need-to-protect carefully balanced. Require contractor to address this concern explicitly in RFP.

Develop a government Systems Engineering Plan (SEP) based on the considerations explained above. Use the OSD SEP Outline as a guide, but streamline and tailor extensively as appropriate for OEIS. The tailored SEP should include high-level drawings of target architecture, schedule, risk strategy and test strategy…all aligned with open systems approaches. Include the SEP in the RFP. The SEP should address IA explicitly. The SEP should explain boundary conditions such as requirements, any mandated standards, enforceable policies, budgets, timelines, and especially specially targeted outcomes in explicit, objective, engineering terms. It should not constrain vendor innovation in the detail of execution, on the contrary!

Develop source selection criteria based on contractor's credibility with respect to assuring engineering and operational interoperability, per SEP.

Appendix A: Sample OEIS Acquisition Strategy

PROGRAM: X-ISR System

Attachments:

I: CONOPS
II: X-ISR SYSTEM Systems Engineering Plan
- A. Metrics
- B. Risk/Reward Optimization Strategy
- C. Design drawings and documents

DESCRIPTION OF PROGRAM:

… Presently there are insufficient Intelligence Surveillance Reconnaissance (ISR) capabilities, and lack of efficient Processing, Exploitation and Dissemination (PED) capabilities in joint, multi-agency, and multi-national construct which limits the ability to detect, identify, track, target, and interdict high-value people, places, and/or events. …..

The acquisition is for a (pick one) (new)/(incremental lifecycle improvement of) X-ISR SYSTEM that will interoperate with, and support existing Defense, Law Enforcement, and Coalition systems and missions. Accordingly, interoperability with existing hardware and software is critical to successful X-ISR SYSTEM missions….

1. Requirement

Continuously evolving requirements for the X-ISR SYSTEM are derived from the "living" CONOPS documentation provided as Attachment I to this acquisition strategy. Attachment II explain how X-ISR SYSTEM will apply tightly coupled, objective, leading and lagging metrics to clearly articulated goals, objectives, and associated risks to assure that targeted value is delivered. Generally desired outcomes to be satisfied are as follows:

(1) Continuously improve the ability of the X-ISR SYSTEM to collect (through multiple means), process, and share information in collaboration with mission partners securely, across stakeholder information domains throughout system lifecycle.

(2) Achieve enhanced speed-to-capability by leveraging Open System Architecture (OSA) to rapidly test, evaluate, and integrate best available Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) Information Technology (IT).

(3) Enhance value returned on investment in lifecycle upgrade of X-ISR SYSTEM and interoperating systems by leveraging OSA to re-use best available GOTS and COTS IT.

(4) Enhance security and privacy of information shared with/by X-ISR SYSTEM through high assurance, dynamic, policy-based, virtual techniques.

b. The X-ISR SYSTEM project will use performance-based methods in accordance with Federal Acquisition Regulation (FAR) Subpart 37.6 Service Acquisition.

b. The US Government (USG) will use threshold and objective criteria keyed to objective Measures of Effectiveness (MOE), Measures of Performance (MOP), and Measures of Suitability (MOS) to define the success of this acquisition in terms of cost, performance, and schedule. These measures will address operational, system, process, and financial performance according to the following high-level strategy:

Improve the ability of X-ISR SYSTEM to collect, process, and share information in collaboration with mission partners securely, across stakeholder information domains.

> Threshold: Operational test validates that new capability enhances specified MOE, MOS, and/or MOP compared to specified legacy benchmark.
>
> Objective: Operational test validates that new capability enhances specified MOE, MOS, and/or MOP by at least ten percent compared to specified legacy benchmark.
>
> Threshold: Capabilities delivered under X-ISR SYSTEM program deliver data and value-added products to mission partner systems.
>
> Objective: Capabilities delivered under X-ISR SYSTEM program receive data and value-added products from mission partner systems.

Achieve enhanced speed-to-capability by leveraging OSA to rapidly test, evaluate, and integrate best available COTS and GOTS IT.

> Threshold: new capability identified, integrated, tested, and certified within twelve months of task start date
>
> Objective: new capability identified, integrated, tested, and certified within six months of task start date

Improve value returned on lifecycle costs of X-ISR SYSTEM and interoperating systems by leveraging OSA, specifically Product Line Architecture (PLA) to re-use best available GOTS and COTS IT.

> Threshold: Government-approved lifecycle cost model of new capability predicts enhanced capability-per-cost across specified lifecycle
>
> Objective: Government-approved lifecycle cost model of new capability predicts at least 10% capability-per-cost improvement across specified lifecycle

Enhance security and privacy of information shared with/by X-ISR SYSTEM through high assurance, dynamic, policy-based, virtual techniques.

> Threshold: New data and/or network resources certified and accredited (C&A) to share, low-to-high, across one security level, in near real-time, via specified Internet Protocol (IP) networks.
>
> Objective: New data and/or network resources C&A'd to share, high-to-low, across one security level, in near real-time, via specified IP networks.

c. The challenges for this acquisition concern overcoming historical government acquisition process difficulties in achieving interoperability across system boundaries (including security issues) and fielding emerging technology fast enough to harvest its competitive advantage. Accordingly this acquisition strategy identifies both of those factors as principle risks and implements appropriate methods, tools, and incentives to overcome them.

d. Clinger Cohen Act (CCA) 40 USC Chapter 11 (CCA) mandates that government should apply commercial best practices, including especially OSA, in order to harvest the value of COTS IT capabilities. X-ISR SYSTEM program office aims specifically to capture commercial best practices for interoperability and agile development within constraints of government acquisition process. Hence, X-ISR SYSTEM goals, objectives, measures, risk management strategy, and contract award criteria all specifically focus on achieving measurably better acquisition value-per-cost-per-time by consuming best-of-breed COTS IT in rapid development spirals.

2. Risk Management

The X-ISR System Risk/Reward Optimization Strategy describes the X-ISR System risk management methodology in detail. This X-ISR System strategy includes the notion that risk must be evaluated in context with targeted reward. The contractor shall plan and objectively track both progress toward achieving "reward," and mitigating

associated risk. The X-ISR System T&E plan shall specifically support the X-ISR System risk management plan. See guidance here.

Cost risk is (pick one) HIGH/MEDIUM/LOW: Chief risk to cost is that lifecycle maintenance costs are not sustainable. Chief reward is substantially reduced life cycle costs across the enterprise achievable by standardizing the family of ISR systems via the Open Standard Approach (OSA), namely PLA, being applied by the X-ISR SYSTEM acquisition.

X-ISR SYSTEM risk/reward optimization strategy for cost includes: a) designing the X-ISR SYSTEM OSA according to COTS best practices for OSA so that best available COTS and GOTS components, with predicable lifecycle costs, can be readily consumed; b) using credibly modeled lifecycle costs as a key performance metric and down-select criteria.

Schedule risk is (pick one) HIGH/MEDIUM/LOW: Chief risk to schedule is that the acquisition process will not field rapidly evolving COTS technology fast enough to harvest the competitive advantage. Chief reward comes from best available COTS IT that is quickly integrated into the X-ISR SYSTEM and will provide an asymmetric information processing advantage over the adversary.

X-ISR SYSTEM risk/reward optimization strategy for schedule includes: a) making acquisition process efficiency (measured in terms of calendar time required to down-select or develop, bundle, test, and certify incremental capability upgrades) a key performance metric; b) using commercial best practices for PLA to rapidly integrate best available COTS/GOTS components.

Performance risk is (pick one) HIGH/MEDIUM/LOW: Chief risk to performance is that the X-ISR SYSTEM will not be interoperate adequately with mission partner systems. Chief rewards are reduced acquisition costs/schedule associated with reusing system components and enhanced operational effectiveness associated with focused access to more networked data and resources.

X-ISR SYSTEM risk/reward optimization strategy for performance includes: defining run-time and build-time interoperability objectively, and including build-time and run-time interoperability as key performance metric; defining need-to-share security policies in addition to need-to-protect security policies.

d. Technical risk is (pick one) HIGH/MEDIUM/LOW: Chief technical risk is closely related to chief performance risk, i.e. that X-ISR SYSTEM will not adequately interoperate with other information system. One chief technical risk is potential failure to adequately define, and strictly comply with open standard interfaces associated with PLA. Government acquisitions typically struggle with this issue.

Another chief technical risk is that by emphasizing use of generic open standard components, specialized performance requirements will not be adequately addressed. Chief rewards are the same as associated with performance risk, namely reduced acquisition costs/schedule associated with reusing system components and enhanced operational effectiveness associated with focused access to more networked data and resources.

X-ISR SYSTEM risk/reward optimization strategy for technical concerns includes: using best commercial practices for specifying and verifying functions and interfaces within PLA; making compliance with interface specifications a key performance metric; working with Joint Interoperability Test Command (JITC) throughout capability lifecycle to assure compliance with best practices for interoperability engineering; working with all relevant IA Approving Officers (AO) throughout capability lifecycle to assure that IA C&A arguments balance the need-to-protect with the need-to-share data and resources.

3. Competition

a. Market Research - …

Publish Requests for Information (RFI) to be answered via "Plug Test" methodology for demonstrating, validating, and verifying interoperability and functionality within mission and system context.

Perform literature review of GAO and other watchdog reports.

Discuss with government leaders within various programs and projects with similar objectives.

Discuss with specialists and researchers at government and not-for-profit institutions.

Discuss with current mission partners.

4. Metrics

The contractor will propose, and/or the government will provide/approve objective operational level, system level, process efficiency, and financial MOE, MOS, and MOP. The government will furnish guidance by providing the current version of Attachment B: X-ISR SYSTEM Value Assurance Framework to the contractor.

Operational level measures include Probability of Detection (P_D) and/or Probability of Intercept (P_I) or other similar quantifiable indicators of mission effectiveness approved by government operational customers.

System level measures include reliability, availability, message latency, protection level, camera resolution, field of view, standard compliance, or other quantifiable indicators of system effectiveness approved by government technical authority.

Process level measures include sequential calendar time required to perform activities such as inventing new capabilities, discovering and evaluating existing capabilities, bundling existing capabilities, testing, certifying, performing overhead functions, or other quantifiable measure of availability of acquisition process efficiency approved by government technical authority.

Financial measures shall objectively quantify expected lifecycle costs as predicted by standard commercial and/or government models approved by the government.

Contractor shall propose, and government will approve baseline values, threshold and objective evaluation criteria, and acceptable approaches to Validation and Verification (V&V).

Contractor shall provide, and government will approve Test and Evaluation (T&E) plans that explain the V&V strategy and provide schedule of T&E and other V&V events.

Contractor shall explicitly include T&E strategy and schedule as a central component of a risk tracking and mitigation strategy.

The contractor will propose the government will approve models and measurement techniques to be applied in test and/other V&V events.

The contractor shall apply any government provided historical baseline values, or determine baseline values prior to V&V using the same modeling and/or measurement techniques as to be used in the test or other V&V technique.

Government intends to leverage best available commercial off the shelf (COTS) Information Technology (IT) components. Wherever appropriate, contractor shall equate X-ISR SYSTEM system-level performance standards and measures to commercial best practice.

APPENDIX B: SAMPLE OEIS PROJECT WORK STATEMENT (PWS)

for

(Pick one) Delivery/Lifecycle Upgrade and Maintenance of (X-ISR SYSTEM) and Interoperating Sensors, Processors, Communications Sub-Systems

PART 1 GENERAL INFORMATION

1. **General**: This is a non-personnel services contract to (pick one) deliver/provide Lifecycle Upgrade and Maintenance of the X-ISR SYSTEM. The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.1 Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Lifecycle Upgrade and Maintenance of the Global Discovery (GD) Intelligence Surveillance and Reconnaissance (ISR) System of System (SoS) as defined in this Performance Work Statement except for those items specified as government furnished property and services. The contractor shall perform to the standards in this contract.

1.2. U. S. Government (USG) Investment strategy. The USG investment strategy for ISR programs aims to enable cross-organizational collaboration by incentivizing and supporting effective information collection and sharing of time sensitive data and information. Information systems must support rapidly evolving missions, mission partners, areas of operations, and concept of operations. These systems must heavily leverage and not replicate information technology infrastructure and/or tools provided by other government organizations and/or Commercial off the Shelf products and services.

The Defense Intelligence Information Enterprise (DI2E) Framework provides the building blocks for the Defense Intelligence Community to more efficiently, effectively and securely develop, deliver, and interface their mission architectures. The key building blocks are standards and specifications, including web service specifications, which enable a stable but agile enterprise supporting rapid technology insertion.

The "DI2E Clearinghouse" is a repeatable, persistent, process that evaluates candidate technology components against the DI2E community standards, specifications, and technical profiles. The "DI2E Storefront" provides a convenient interface to DI2E conformant components. Software components that achieve and maintain threshold scores in the clearinghouse process are posted within the DI2E Storefront. Contractors participating in X-ISR SYSTEM development will fully support all DI2E Framework processes. In particular, all software components implemented with the X-ISR SYSTEM will undergo, or have undergone, the D2E Clearinghouse process and be identified in the DI2E Storefront.

The X-ISR SYSTEM acquisition will employ "Product Line Architecture" (PLA) to implement the DI2E Framework guidance within the specific mission and business objectives of the X-ISR Program. PLA is the set of IT design characteristic and implementation processes at the intersection of an enterprise's e-business model, and its open standard IT platform. PLA aims to optimize the latter to achieve the former. (Both Mac and Windows, for example, apply PLA very effectively within their respective IT device product lines.)

PLA imposes the discipline necessary to prevent the "verticals," i.e. the product providers, in an enterprise from competing with each other on the basis of proprietary "horizontal" infrastructure. Correspondingly, PLA provides consumers with a single point of access to the entire suite of e-products provisioned by the enterprise of interest. PLA thus supports rapid speed-to-capability for initial capability, lifecycle refresh, and extending the scope of capability. It also enables decreased cost-per-capability through simplified integration and reuse of existing capabilities.

For reference, see the body of work by Carnegie Mellon University (CMU) Software Engineering Institute (SEI) that thoroughly explains and describes "Software Product Lines" (SPL) in context with multiple real world use cases. (CMU SEI). SPL are essential building blocks for the broader concept of PLA.

Although the term PLA has often been associated with relatively narrowly defined enterprise software frameworks such as Mac or Windows, or telecommunications platforms such as Nokia, the same concept can be applied more abstractly to more loosely defined and more federated Enterprise Information Systems (EIS). For example, the eFile standards and policies governed by the Internal Revenue Service (IRS) represent a PLA of sorts. In any case, PLA is designed to accelerate the transition of IT-enabled capability.

Achieving the potentially catalytic benefits of PLA requires provisioning a suite of PLA-derived tools and processes to developers. The PLA suite's aim is to streamline and parallelize the myriad activities associated with transitioning evolving IT capabilities into operations. Here are some of those PLA utilities for rapid, iterative, parallel developing, testing, certifying, offering, consuming, and refreshing capability:

- Bottom up process, informed by customer-in-the-loop, for continuously adapting emerging standards against enterprise functional and performance specifications.
- Persistent, open, online "plug test" PLA Reference Implementation (RI) for developing, testing, and certifying inventions. Includes an evolving library of documented PLA-compliant components, developers' guides, and Software Development Kits (SDK).

- Certification requirements for security and interoperability are embedded in the technical guidance and the RI so that successfully compiled offerings inherit certification controls from the enterprise framework itself.
- Pre-negotiated contractual vehicles that address compensation and obligations to all parties, including intellectual property rights.

Note that Apple, Microsoft, Google, Android, etc. provision these PLA utilities to a huge global community of potential innovators. They do that via convenient resources available through open standard developers' portals at Apps Stores and similar online venues. These enterprises thereby crowd source technology transition by exposing a convenient transition path to their enterprise product lines. That is, the PLA-based developers' portal makes typically difficult activities -- such as Analysis of Alternatives (AoA), prototyping, iterative development, test and evaluation, certification, production, delivery, and lifecycle support --relatively easy and inexpensive to perform. In this sense, the online PLA portal provides a virtual laboratory for developing the invention, and a channel to market to transition the innovation. When the invention functions properly in the lab, it can transition as a certified, lifecycle-sustained, product that can be immediately lucrative for both the provider and consumer. If the invention fails to be adopted, it fails fast and cheap, with feedback for the next try.

The PLA utilities enumerated above align very well with the COTS best practices that Defense acquisition policy suggests are appropriate for sustainment of software intensive capability explained previously. Further, procurement of COTS products and services as a means to satisfy government requirements is not only legal, the FAR explicitly favors that approach. Finally, the recently implemented "IT Box" option for Joint Capabilities Integration and Development System (JCIDS) prescribes a COTS-friendly software development process.

Experimentation within the Defense "Plug Fest" initiative, PFP has demonstrated an effective and efficient approach for assembling Information Systems (IS) through integration of open standard components such as those identified within the DI2E Framework. A "Plug Fest" is a demonstration venue that is based on a methodology for evaluating interoperability called a "Plug Test". Plug Tests require that potential solutions actually configure in a realistic system environment, according to published open standards, in order to demonstrate interoperability and functionality.

Accordingly, X-ISR Program Office will use Plug Tests to perform accelerated Analysis of Alternatives (AoA), Validation and Verification (V&V), and certification of candidate off-the-shelf information technology. X-ISR SYSTEM Plug Fest events will allow vendors to objectively demonstrate how their capabilities perform against DI2E Framework standards, in context with X-ISR SYSTEM mission threads, as verified by government officials, and as compared to other candidate solutions.

Technical standards, specifications, and technical profiles for DI2E generally, and for the X-ISR System PLA in particular, together with descriptions of existing X-ISR PLA-compliant subsystems are at Appendix II.

1.3 Objectives: The objectives of this acquisition are as follows:

1.3.1. Rapidly evolve and improve the ability of the X-ISR System to collect, process, and share information in collaboration with mission partners, securely, across stakeholder information domains.

1.3.2. Achieve enhanced speed-to-capability by leveraging Open System Architecture (OSA) to rapidly test, evaluate, and integrate best available COTS and GOTS IT.

1.3.3. Reduce lifecycle costs of X-ISR System and interoperating systems by leveraging re-use of best available GOTS and COTS IT.

1.3.4. Enhance security and privacy of information shared with/by X-ISR System through integration of high assurance, dynamic, policy-based, virtual techniques.

1.4 Scope: Respondents should define the effort required to design, build, test, certify, enhance, improve, deploy and maintain the X-ISR System via OSA in general, and via enhancement to the previously developed XXXX and YYYY subsystems in particular.

All systems shall be designed to support rapidly evolving missions, mission partners, areas of operation and Concepts of Operations (CONOPS). Systems shall be designed to intercept rapidly evolving technological tools. An OSA shall be used with rapid adaptive engineering and acquisition techniques. All hardware and software developed for X-ISR SYSTEM will have plug-and-play functionality with existing hardware and software.

Test and engineering support is required for both engineering evaluations (informal testing) and formal testing. Engineering evaluations are significantly smaller in scope than formal testing. Test support shall include test planning, test execution and post-test analysis. Engineering evaluation contractor support services shall include engineering evaluation planning, execution and post-engineering evaluation analysis.

1.4. Deliverables: Engineering evaluation deliverables shall include engineering evaluation plans, procedures, and reports. An engineering evaluation will typically run two weeks and is narrowly focused on specific capability, subsystem or system.

1.5 Interoperability: Interoperability with existing hardware and software, including that of mission partners, is critical. Accordingly, interoperability is the critical performance objective, and primary "technical risk" and "risk to performance." in the X-ISR SYSTEM, interoperability is defined in both engineering, and operational terms as follows:

> **Engineering interoperability** = Component-level off-the-shelf functionality, i.e., capability configures out-of-the box in the target architecture with specified short time period; is readily certifiable; is readily consumed from a convenient catalog and/or repository, and procurement vehicle; comes with well-specified life-cycle support model at known costs.
>
> **Operational interoperability** = Meaning of the data is shared; the content of the information exchange requests are unambiguously defined; and delivery of critical information to critical decision nodes is assured per a specified information availability metric.

1.6. Data Rights: Vendor will propose an intellectual property rights model consistent with a conceptual "Open Systems Architecture License Right" (OSALR). (See references _____ and _____) (Note: these are the OSA Contract Guide, and the IP Guidance brochure.) The OSALR concept is a mutually beneficial arrangement where the Government receives only limited data rights for the inner workings of the functional plug-and-play component developed by the commercial partner. The commercial partner accepts responsibility for providing or contributing to the standard interfaces and utilities (per license similar to General Purpose License (GPL)) that comprise the "open" elements of a specified PLA. Intent is a government-industry partnership wherein the government avoids "vendor-lock" via an open "plug-and-play" architecture wherein components can be individually and competitively acquired. The commercial partner may exclusively market its protected products to a variety of customers without having to compete with competitors' implementation of the same intellectual property. In particular:

1.6.1. The Government may not release or disclose OSALR software or data to any person, other than its support services contractors, except as expressly permitted by the Vendor.

1.6.2. The Government may use OSALR software and data for program purposes only.

1.6.3. The Government cannot disclose OSALR software or data outside the Government for a specified period of time subsequent to program completion.

1.6.4. The OSALR commercial partner retains: "rights to software and data

generated by the concern in the performance of an OSALR award."

1.6.5. The Government will not use anything other than the external characteristics of the module (information associated with segregating it from the rest of the system or reintegrating a replacement) with OSALR rights to produce future technical procurement specifications.

1.6.6. The Government receives a nonexclusive, royalty free license for software and technical data, but may not disclose them during the protection period, except for very limited purposes.

PART 2 GOVERNMENT FURNISHED ITEMS AND SERVICES

2.1 Government Furnished Information and equipment (GFI/E): The Government will provide the contractors with the most recent versions of the design documents for the X-ISR SYSTEM and associated interface kits as well as copies of any documents on the PART 6 reference list that are not generally available to the public.

PART 3 CONTRACTOR FURNISHED ITEMS AND SERVICES

3.1 General: The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not listed under Section 2.

PART 4 SPECIFIC TASKS

4. SPECIFIC TASKS: The following paragraphs describe specific categories of tasks to be performed under this contract. Task Orders will include specific standards and deliverables.

4.1. Basic Services: In execution of this contract, the Contractor shall provide the following:

4.1.1. The contractor shall study the reference material in part 5 and apply as appropriate in the performance of all tasks.

4.1.2. The contractor shall apply commercial best practices for rapid, adaptive, engineering of open system architecture as defined by the Defense Acquisition University in order to improve measured mission outcomes, speed-to-capability,

and cost-per-capability delivered. Use of "Plug Test" methodology satisfactorily addresses this task.

4.1.3. The contractor shall establish processes for frequent interaction with and feedback with both the operational customer community and the acquisition community.

4.1.4. The contractor shall apply methods such as described in MILSTD 498 to propose tailoring of Data Item Descriptions (DID) associated with each specific task deliverable. These DIDS will deliberately tailor the documentation process while maintaining sufficient rigor and repeatability as required to satisfy the intent of Defense Acquisition Guidebook of 28 Jun 2013, DAU OSA Contract Guidebook v1.1 of Jun 2013, INCOSE SEBoK, and PMIBoK.

4.1.5. The contractor shall propose performance tailored metrics, information assurance approaches, and risk management strategies that optimize value achieved though sharing information among all operational participants as well as among acquisition participants.

4.1.6. The contractor shall propose methods to streamline capturing and sharing government-developed designs, processes, and software such as use of open repositories and open licenses for implementation and repeatability. In particular the contractor shall either choose software components from the DI2E Storefront, or apply the DI2E clearinghouse process to register any introduced software in the DI2E Storefront

4.2. <u>X-ISR SYSTEM PED SUBSYSTEM</u>

4.2.1. <u>PED Host Environment:</u> The contractor shall integrate open standard PED software and/hardware according to the GFI X-ISR PED PLA (Attachment II such that identified operational outcomes are measurably improved, lifecycle costs and methods are identified and documented, as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.2.2. <u>PED Communications Kit:</u> The contractor shall select, provide, and/or integrate communications equipment within GD ground stations according to the X-ISR SYSTEM PED reference architecture, to improve and enhance information and data sharing among operational users such that identified system-level performance standards are achieved, lifecycle costs and methods are identified and documented as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.3. <u>X-ISR SYSTEM AIRBORNE SEGMENT</u>

4.3.1. Sensor Integration: The contractor shall select, provide, and/or integrate sensors within GD and system airborne platforms according to the X-ISR SYSTEM AIRBORNE SEGMENT PLA, such that identified system-level performance standards are achieved, lifecycle costs and methods are identified and documented, as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.3.2. Communications System Integration: The contractor shall select, provide, and/or integrate communications equipment such as antennae and radio processors within X-ISR SYSTEM airborne platforms according to the X-ISR SYSTEM AIRBORNE SEGMENT PLA, such that identified system-level performance standards are achieved, lifecycle costs and methods are identified and documented, as discussed in paragraph 4.1.2, and that operators and maintainers are trained. Task order will provide specific performance standards and deliverables.

4.4. X-ISR SYSTEM XXXXX SEGMENT

4.5.Virtual Dynamic Real-time Cross-Domain Services (VDRC): The contractor shall select, provide, fabricate, and/or integrate VDRC according to X-ISR SYSTEM PLA, such that GFI need-to-share policy is implemented and certified across at least one level of security, via the requisite communications network. This implementation will make use of a hypervisor and the architecture will follow the guidelines of the trusted Computing Base, such as described by NSA 2014. Task order will provide specific performance standards and deliverables.

4.5. Test and Evaluation (T&E): The contractor shall perform T&E tasks associated with any or all deliverables under this contract, including early development of a Test Plan and identification of resources necessary to complete the assigned task, reports, consistent with operational, system, and process level performance statements specified in task order.

4.6. Certification and Accreditation (C&A): The contractor shall perform evidence collection and documentation tasks necessary to support C&A of any or all deliverables under this contract. Task order will provide specific performance standards and deliverables.

PART 5 APPLICABLE PUBLICATIONS

5. APPLICABLE PUBLICATIONS: The following publications are applicable to the work described in this document.

a. Bloch M, B. S. (2012). Delivering large-scale IT projects on time, on budget, and on value. McKinsey & Company, Business Technology Office. McKinsey & Company.

b. Brooks, F. (1995). No Silver Bullet Refined. In F. Brooks, The Mythical Man Month. United States: Addison Wesley.

c. Brooks, F. P. (1986). No Silver Bullet. Information Processsing 1986, the Proceedings of the Tenth World Computing Conference (pp. 1069-1076). Amsterdam, The Netherlands: Elsevier Science B.V.

d. Brownsword, L., Albert, C., Carney, D., Place, P., Hammons, C., & Hudak, J. (2013). Isolating Patterns of Failure in Department of Defense Acquisiton. Carnegie Mellon University Software Engineering Institute. Pittsburg, PA: Carnegie Mellon University.

e. Chairman Joint Chief of Staff. (2012, March). CJCSI 6212.01F: Netready Key Performance Parameter (NR KPP). Washington, DC, US.

f. CMU SEI. (n.d.). A Framework for Software Product Line Practice, Ver 5.0. Retrieved July 14, 2014, from Software Engineering Institute, Carnegie Mellon University: http://www.sei.cmu.edu/productlines/frame_report/index.html

g. Defense Acquisition University (DAU) . (n.d.). Defense Acquisition Guidebook. Retrieved Dec 10, 2014, from Defense Acquisition Guidebook: https://dag.dau.mil/

h. Defense Science Board. (2009). DoD Policy and Procedures for the Acquisition of Information Technology. Washington DC: OUSD AT&L.

i. Department of Defense (DoD). (2008, December 15). DoD Instruction 5000.02: The Defense Acquisition System. 47. Washington, DC: USD AT&L.

j. Department of Defense. (2009). Department of Defense Reliability, Availability, and Maintainability and Cost Rationale Report Manual. Washington DC: Office of the Secretary of Defense.

k. Department of Defense. (2006). Risk Management Guide for DoD Acquisition (Sixth Edition). Washington DC: DoD.

l. DoD. (2006). Earned Value Management Implementation Guide . DCMA. Washington DC: DoD.

m. DoD. (2007). DOD Directive 8320.02: Data Sharing in a Net-centric Department of Defense. Washington, DC: DoD.

n. DoD. (2014, March 12). DODI 8510.01: Risk Management Framework. Washington, DC, USA: DoD.

o. DoD. (2000, June). DoD Financial Management Regulation, Voume 2A. DoD Financial Management Regulation , 2A Chapt 1 paragraph 01208 , 1-19. Washington, DC, USA.

p. DoD. (1994, Dec 5). Military Standard 498: Software Development and Documentation. Mil-Std-498 . Washi (International Council on Systems Engineering (INCOSE)) (Defense Acquistion University (DAU)) (Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L), 2013)ngton, DC, USA: Department of Defense.

q. GAO. (2014). Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practies. Washington DC: GAO.

r. Gunderson, C. R. (2014, June 5). Enterprise Information System (EIS) Value Assurance Framework (VAF) Risk-Reward Optimization . Submitted to Journal of Enterprise Transformation . Herndon, VA, USA.

s. Gunderson, C. R. (2014). Enterprise Information System Value Model. NPS Technical Report . Washington, DC: Naval Postgraduate School.

t. Gunderson, C. R. (2014). Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF). Naval Postgraduate School, Information Science. Monterey, CA: NPS.

u. Gunderson, C. R., & Minton, D. (2009). CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2. 2009 AFCEA GMU Critical Issues in C4I Symposium. Fairfax VA: George Mason University.

v. Hokins, R., & Jenkins, K. (2008). Eating the IT Elephant: Moving from Greenfield to Brownfield Development. IBM Press.

w. International Council on Systems Engineering (INCOSE). (n.d.). Systems Engineering Body of Knowlege. (INCOSE, Producer) Retrieved Dec 10, 2014, from http://g2sebok.incose.org/

x. Joint Chiefs of Staff. (2012, January 19). Joint Capability Integration Development System Manual. Washington, DC, USA: JCS.

y. Kurzweil, R. (2006). The Singularity is Near. London, England, UK: Penguin Books.

z. Nagy B, F. J. (2013). Statistical Basis of Predicting Technological Progress. (N. U. Lisa A. Nunes Amaral, Ed.) PLOS One (2).

aa. NIST. (2010). NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems. National Institute of Standards, Security Division. Gaithersburg, MD: NIST.

bb. NIST. (2013). NIST SP-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards, Computer Security Division. Gaithersburg, MD: NIST.

cc. Northern, C., Mayfield, K., Benito, R., & Casagni, M. (2010). Handbook for Implementing Agile in Department of Defense Information Technology Acquisition. MITRE. The Mitre Corporation .

dd. Project Management Institute. (2013). Project Management Body of Knowledge, 5th Edition. New Town Square, Pennsylvania, USA: Project Management Institute, Inc.

ee. Schaller, B. (1997). Moore's Law: The Benchmark of Progress in Semiconductor Electronics. IEEE Spectrum , 34 (6), 53-59.

ff. Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L). (2013). DoD Open Systems Architecture Contract Guidebook for Program Managers. Washington, DC, US: AT&L.

gg. Unified Cross Domain Management Office (UCDMO). (2014). UCDMO Cross Domain Baseline List. Washington, DC : UCDMO.

hh. USAF Space and Missile Systems Center (SMC). (2014). ACQUIRING AND ENFORCING THE GOVERNMENT'S RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE UNDER DOD CONTRACTS: A PRACTICAL GUIDE FOR ACQUISITION PROFESSIONALS. USAF Space and Missile Systems Center (SMC). Huntsville, AL: SMC.

ii. Weatherall, J. (2014). The Physics of Wall Street: A Brief History of Predicting the Unpredicable. New York, New York, USA: First Mariner Books.

APPENDIX B: 01 CONTRACT LINE ITEM NUMBERS (CLIN)

A001 Evolutionary Prototype Execution Plan (E-PEP) per Data Item Description (DID) SAF-AQ-BTCC-EPEP-3-18-15* as tailored and reported monthly. (New DID describes rapid evolutionary OSA programmatic artifacts.)

A002 Executable software application, license, user manual and Concept of Operations (CONOPS) for specified USAF applications specification per DID SAF-AQ-BTCC-SW Spec-3-18-15*. (New DID describes requirements for documentation of new IT for operators and administrators in specific mission context.)

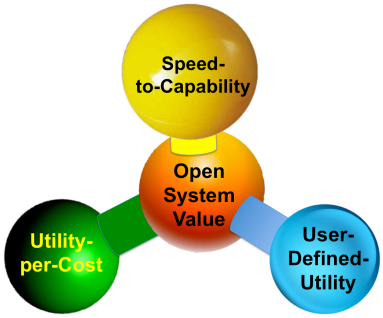
A003 Software Test Report per DID SAF-AQ-BTCC-PT -3-18-15*. (New DID describes Plugtest methodology for mitigating risk in open system acquisition.)

A004 RMF template per DID SAF-AQ-BTCC-RMF-3-18-15*. (New DID describes how vendor will assist government in evolving new C&A paradigms based on "need to share" in addition to "need to protect," and open standard virtual technology.)

A005 Product Line Architecture per DID SAF-AQ-BTCC-PLA-3-18-15* that addresses broad implantation and tech refresh of VOS3. PLA will be sufficiently robust to support implementation of core technology into various form factors such as enterprise cloud services, tactical UAVs, and hand held mobile devices. (New DID describes how vendor will align operational requirements, e.g. need-to-protect and need-to-share information, business efficiency, i.e. capability-per-cost and speed-to-capability, with evolving, reusable, open standard technology.

APPENDIX B: 02 OSA PROJECT EXECUTION PLAN (PEP) DATA ITEM DESCRIPTION (DID)

Open System Acquisition (OSA) Project Execution Plan (PEP)



April, 2015

Secretary of the Air Force Acquisition Open System Acquisition

Revision History

.

REVISION HISTORY			
REVISION/WORKSITE #	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Draft -			

Approvals

Insert Project Approvals here.

NAME	ROLE	DATE

1. Introduction

1.1 Purpose

This DID describes the required elements of a rapid adaptive Open System Acquisition.

1.2 Scope

This DID describes the specific format, content, and level of detail required for planning and reporting execution against the plan for rapid, evolutionary, OSA projects. It emphasizes value-based metrics and incentives; test-based development and risk-reward optimization within short iterative capability delivery cycles; parallelizing independent activities; identifying dependencies across parallel activities and provisioning for integration across them; built-in security layers based on logical separation enabled via virtualization technology.

This DID describes the required content of the OSA Project Execution Plan (PEP) deliverable and the key acceptance criteria for the document.

1.3 References

A. Bloch M, B. S. (2012). Delivering large-scale IT projects on time, on budget, and on value. McKinsey & Company, Business Technology Office. McKinsey & Company.
B. Brooks, F. (1995). No Silver Bullet Refined. In F. Brooks, The Mythical Man Month. United States: Addison Wesley.
C. Brownsword, L., Albert, C., Carney, D., Place, P., Hammons, C., & Hudak, J. (2013). Isolating Patterns of Failure in Department of Defense Acquisiton. Carnegie Mellon University Software Engineering Institute. Pittsburg, PA: Carnegie Mellon University.
D. Chairman Joint Chief of Staff. (2012, March). CJCSI 6212.01F: Netready Key Performance Parameter (NR KPP). Washington, DC, US.
E. CMU SEI. (n.d.). A Framework for Software Product Line Practice, Ver 5.0. Retrieved July 14, 2014, from Software Engineering Institute, Carnegie Mellon University: http://www.sei.cmu.edu/productlines/frame_report/index.html
F. Defense Acquisition University (DAU).Defense Acquisition Guidebook. Retrieved Dec 10, 2014, from Defense Acquisition Guidebook: https://dag.dau.mil/
G. Defense Science Board. (2009). DoD Policy and Procedures for the Acquisition of Information Technology. Washington DC: OUSD AT&L.

H. Department of Defense (DoD). (2008, December 15). DoD Instruction 5000.02: The Defense Acquisition System. 47. Washington, DC: USD AT&L.
I. Department of Defense. (2009). Department of Defense Reliability, Availability, and Maintainability and Cost Rationale Report Manual. Washington DC: Office of the Secretary of Defense.
J. Department of Defense. (2006). Risk Management Guide for DoD Acquisition (Sixth Edition). Washington DC : DoD.
K. DoD . (2006). Earned Value Management Implementation Guide . DCMA. Washington DC: DoD.
L. DoD. (2007). DOD Directive 8320.02: Data Sharing in a Net-centric Department of Defense. Washington, DC: DoD.
M. DoD. (2014, March 12). DODI 8510.01: Risk Management Framework. Washington, DC, USA: DoD.
N. DoD. (2000, June). DoD Financial Management Regulation, Volume 2A. DoD Financial Management Regulation, 2A Chapt 1 paragraph 01208 , 1-19. Washington, DC, USA.
O. DoD. (1994, Dec 5). Military Standard 498: Software Development and Documentation.
P. Mil-Std-498 . Washington, DC, USA: Department of Defense.
Q. GAO. (2014). Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practies. Washington DC: GAO.
R. Gunderson, C. R. (2014, June 5). Enterprise Information System (EIS) Value Assurance Framework (VAF) Risk-Reward Optimization. Submitted to Journal of Enterprise Transformation. Herndon, VA, USA.
S. Gunderson, C. R. (2014). Enterprise Information System Value Model. NPS Technical Report. Washington, DC: Naval Postgraduate School.
T. Gunderson, C. R. (2014). Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF). Naval Postgraduate School, Information Science. Monterey, CA: NPS.
U. Gunderson, C. R., & Minton, D. (2009). CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2. 2009 AFCEA GMU Critical Issues in C4I Symposium. Fairfax VA: George Mason University.
V. Hokins, R., & Jenkins, K. (2008). Eating the IT Elephant: Moving from Greenfield to Brownfield Development. IBM Press.
W. International Council on Systems Engineering (INCOSE). (n.d.). Systems Engineering Body of Knowlege. (INCOSE, Producer) Retrieved Dec 10, 2014, from http://g2sebok.incose.org/
X. Joint Chiefs of Staff. (2012, January 19). Joint Capability Integration Development System Manual. Washington, DC, USA: JCS.
Y. Nagy B, F. J. (2013). Statistical Basis of Predicting Technological Progress. (N. U. Lis A. Nunes Amaral, Ed.) PLOS One (2).
Z. NIST. (2010). NIST SP 800-37: Guide for Applying the Risk Management Framework to Fedieral Information Systems. National Institute of Standards, Security Division. Gaithersburg, MD: NIST.

AA. NIST. (2013). NIST SP-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards, Computer Security Division. Gaithersburg, MD: NIST.
BB. Northern, C., Mayfield, K., Benito, R., & Casagni, M. (2010). Handbook for Implementing Agile in Department of Defense Information Technology Acquisition. MITRE. The MITRE Corporation.
CC. Project Management Institute. (2013). Project Management Body of Knowledge, 5th Edition. New Town Square, Pennsylvania, USA: Project Management Institute, Inc.
DD. Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L). (2013). DoD Open Systems Architecture Contract Guidebook for Program Managers. Washington, DC, US: AT&L.
EE. USAF Space and Missile Systems Center (SMC). (2014). ACQUIRING AND ENFORCING THE GOVERNMENT'S RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE UNDER DOD CONTRACTS: A PRACTICAL GUIDE FOR ACQUISITION PROFESSIONALS. USAF Space and Missile Systems Center (SMC). Huntsville, AL: SMC.

1.4 Acronyms

BoK	Body of Knowledge
BTCC	Bending the Cost Curve
COTS	Commercial Off the Shelf
DAG	Defense Acquisition Guidebook
DID	Data Item Description
INCOSE	International Council on Systems Engineering
OSA	Open System Acquisition
PEP	Project Execution Plan
PM	Project Manager
PMIBOK	Project Management Institute Body of Knowledge
PWS	Performance Work Statement
RFP	Request for Proposal

2. Deliverable Description

2.1 Purpose

The PEP provides the minimal set of documentation required to effectively describe the evolving plan for iterative, streamlined, parallel, engineering and procurement efforts associated with OSA of a particular capability portfolio. Intent is to minimizing bureaucratic overhead by concisely describing measurable risks, rewards, goals and objectives.

2.2 Delivery Requirements

The initial PEP shall be delivered electronically, and presented verbally, in contractor's formant within 30 days of award, i.e. _____. Updates that track either accomplishment and/or modification of previous iterations shall be delivered electronically and verbally every 30 days on _____ throughout the life of the OSA project of interest per PWS.

2.3 Review Requirements

The government Project Manager (PM) and the duly designated representative of the contract officer (who may or may not be the PM) shall approve the initial PEP and all updates in writing, within one working week of receipt.

2.4 Acceptance Criteria

2.4.1 The PEP must describe the specific methodology used to optimize risk and reward on this project. A general description of risk management theory is not acceptable. The description must explain how theory will be applied to provide objective estimates of magnitude and likelihood of risks and associated targeted positive outcomes. In particular, PEP must explain how the project test plan specifically supports the project risk optimization plan. In OSA, the risk optimization plan must explain targeted efficiencies and risks associated with the project "plug-and-play" interoperability model.

2.4.2 PEP must explain how work is subdivided into scheduled modules with, clear, responsibilities and objective, verifiable exist criteria. PEP updates must report status of verification against exit criteria.

2.4.3 PEP must include a project schedule that clearly defines the critical path to project milestones in terms of parallel, independent activities such as component engineering and testing, and activities designed to integrate parallel efforts, such as bundling and integration/interoperability testing. Schedule must carefully address critical shared resources such as test resources.

2.4.4 PEP must include a continually evolving test plan that describes the validation and verification (V&V) of all scheduled work. Must include entry and exit criteria, evaluation methodology, metrics, and threshold and objective values. "Validation" means Measures of Effectiveness (MOE) correlate to customer-confirmed targeted outcomes, and that Measures of Performance (MOP) are testably correlated to MOE. "Verification" means that the evaluated artifact achieved at least threshold levels of MOP and MOE.

2.4.5 PEP must include a value accretion plan (VAP) and reporting method that captures utility delivered, as a function of both cost and time required to deliver capability. "Utility" in this sense means "requirements satisfied." Hence, the VAP must explain targeted improvements in MOP and MOE as compared to identified baseline values, i.e. targeted utility improvement. The VAP must then explain how the test plan measures incremental accrual of improved utility

(i.e. operational and technical performance) per budget and schedule spent accruing it. Finally VAP must incrementally report actuals.

3. Preparation Instructions

3.1 General Instructions

3.1.1 Format.

PEP may be in contractor format or per a template provided by government.

3.1.2 Applicable Standards

Defense Acquisition Guidebook (DAG), especially chapters 4, 7, and 9

Defense Intelligence Information Environment (DI2E) Services View (SV) 4

INCOSE BoK Part 3 & 4

ISO/IEC/IEEE 15288

MIL-STD-498, especially paragraphs: 4.2.3.1, 4.2.4.2, 5.7-5.11.7

PMIBoK, especially paragraphs: 1.7.1, 4.2-7.4.3, 11.2-11.2.3, 11.4-11-6.3

3.2 Content Requirements

PEP may be in contractor format. Traditional systems engineering and project management artifacts, e.g. per DAG, INCOSEBoK, and PMIBoK, may be streamlined and abstracted as appropriate for rapid, evolutionary, OSA. Agile software development artifacts, e.g. per SCRUM and EXTREME Programming, are generally consistent with PEP requirements. Contractors should avoid bureaucratic and/or conceptual language, and emphasize reporting of essential, objective, data.

3.2.1 Requirements

Template at Appendix A

3.2.2 Risk-Reward Optimization Plan

Template at Appendix B

3.2.3 Work breakdown, Modularization, and Parallelization Plan

Template at Appendix C

3.2.4 Master Schedule

Template at Appendix D

3.2.5 Test Plan

Template at Appendix E

3.2.6 Value Accrual Plan

Template at Appendix A

3.2.7 Appendices

Appendices may be added, as needed to clarify or provide additional detail to the deliverable.

Acronyms and Glossary

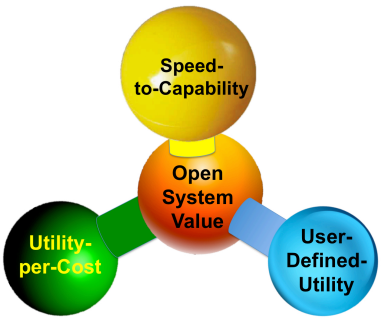
An acronym list and glossary of key terms used in the deliverable shall be provided.

Referenced Documents

If other documents or materials were cited in the document, a list of the referenced materials shall be provided. The reference list shall include the title of the material, author of the material, date of the material, and location where the material is stored.

APPENDIX B: 03 OSA PRODUCT LINE ARCHITECTURE (PLA) DID

Open System Acquisition (OSA) Product Line Architecture (PLA)



April, 2015

Secretary of the Air Force Acquisition Open System Acquisition

Revision History

.

REVISION HISTORY			
REVISION/WORKSITE #	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Draft -			

Approvals

Insert Project Approvals here.

NAME	ROLE	DATE

4.Introduction

4.1 Purpose

This DID describes the required elements of a rapid adaptive Open System Acquisition OSA) Product Line Architecture (PLA).

4.2 Scope

Product Line Architecture is an industrial best practices for optimizing application of modular Information Technology against the mission and business objectives of the enterprise of interest. Accordingly, this DID describes the specific format, content, and level of detail required for specifying interoperable information System (IS) functional elements, and the open standard interfaces between them as optimized for achieving user-specified Measures of Effectiveness (MOE).

4.3 References

jj. Brownsword, L., Albert, C., Carney, D., Place, P., Hammons, C., & Hudak, J. (2013). Isolating Patterns of Failure in Department of Defense Acquisiton. Carnegie Mellon University Software Engineering Institute. Pittsburg, PA: Carnegie Mellon University.

kk. Chairman Joint Chief of Staff. (2012, March). CJCSI 6212.01F: Netready Key Performance Parameter (NR KPP). Washington, DC, US.

ll. CMU SEI. (n.d.). A Framework for Software Product Line Practice, Ver 5.0. Retrieved July 14, 2014, from Software Engineering Institute, Carnegie Mellon University: http://www.sei.cmu.edu/productlines/frame_report/index.html

mm. Defense Acquisition University (DAU).Defense Acquisition Guidebook. Retrieved Dec 10, 2014, from Defense Acquisition Guidebook: https://dag.dau.mil/

nn. Defense Science Board. (2009). DoD Policy and Procedures for the Acquisition of Information Technology. Washington DC: OUSD AT&L.

oo. Department of Defense (DoD). (2008, December 15). DoD Instruction 5000.02: The Defense Acquisition System. 47. Washington, DC: USD AT&L.

pp. Department of Defense. (2009). Department of Defense Reliability, Availability, and Maintainability and Cost Rationale Report Manual. Washington DC: Office of the Secretary of Defense.

qq. Department of Defense. (2006). Risk Management Guide for DoD Acquisition (Sixth Edition). Washington DC : DoD.

rr. DoD. (2007). DOD Directive 8320.02: Data Sharing in a Net-centric Department of Defense. Washington, DC: DoD.

ss. DoD. (2014, March 12). DODI 8510.01: Risk Management Framework. Washington, DC, USA: DoD.

tt. DoD. (1994, Dec 5). Military Standard 498: Software Development and Documentation.

uu. Gunderson, C. R. (2014, June 5). Enterprise Information System (EIS) Value Assurance Framework (VAF) Risk-Reward Optimization. Submitted to Journal of Enterprise Transformation. Herndon, VA, USA.

vv. Gunderson, C. (2014). A Platform Across the Valley of Death: Tech Transition via Open Enterprise Information System Development. Naval Postgraduate School, Information Sciences. Monterey: NPS.

ww. Gunderson, C. R. (2014). Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF). Naval Postgraduate School, Information Science. Monterey, CA: NPS.

xx. Gunderson, C. R., & Minton, D. (2009). CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2. 2009 AFCEA GMU Critical Issues in C4I Symposium. Fairfax VA: George Mason University.

yy. International Council on Systems Engineering (INCOSE). (n.d.). Systems Engineering Body of Knowledge. (INCOSE, Producer) Retrieved Dec 10, 2014, from http://g2sebok.incose.org/

zz. NIST. (2010). NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems. National Institute of Standards, Security Division. Gaithersburg, MD: NIST.

aaa. NIST. (2013). NIST SP-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards, Computer Security Division. Gaithersburg, MD: NIST.

bbb. Northern, C., Mayfield, K., Benito, R., & Casagni, M. (2010). Handbook for Implementing Agile in Department of Defense Information Technology Acquisition. MITRE. The MITRE Corporation.

ccc. Project Management Institute. (2013). Project Management Body of Knowledge, 5th Edition. New Town Square, Pennsylvania, USA: Project Management Institute, Inc.

ddd. Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L). (2013). DoD Open Systems Architecture Contract Guidebook for Program Managers. Washington, DC, US: AT&L.

eee. USAF Space and Missile Systems Center (SMC). (2014). Acquiring and enforcing the government's rights in technical data and computer software under dod contracts: a practical guide for acquisition professionals. USAF Space and Missile Systems Center (SMC). Huntsville, AL: SMC.

4.4 Acronyms

BoK	Body of Knowledge
BTCC	Bending the Cost Curve
CMU SEI	Carnegie Mellon University Software Engineering Institute
DAG	Defense Acquisition Guidebook
DID	Data Item Description
DoDAF	Department of Defense Architectural Framework
INCOSE	International Council on Systems Engineering
IPR	Intellectual Property Rights
OSA	Open System Acquisition
PLA	Product Line Architecture
PM	Project Manager
PMIBOK	Project Management Institute Body of Knowledge
RMF	Risk Management Framework

5. Deliverable Description

5.1 Purpose

The PLA provides the minimal set of documentation required to effectively describe the way functional modules of technology will be connected together effectively within the various form factor of interest. Intent is to:

5.1.1 Optimize application of best available current technology against system operational and business requirements

5.1.2 Enable engineering-level "plug-and-play" interoperability and/or tech refresh of lifecycle supported COTS and GOTS components.

5.1.3 Deploy new technology as it reaches sufficient maturity

5.1.4 Enable operational-level interoperability of data and application functionality across enterprise system boundaries

5.1.5 Host the same core technology in different form factors, e.g. cloud servers, device clients, including mobile clients.

5.1.6 Inherit cyber security controls from open standard PLA "security" layer

5.1.7 Quantify lifecycle tech refresh cycles and costs up front

5.2 Delivery Requirements

The initial PLA shall be delivered electronically, and presented verbally, in contractor's formant within ____ days of award, i.e. not later than _____. Updates that track either accomplishment and/or modification of previous iterations shall be delivered electronically and verbally every _____ days on _____ throughout the life of the OSA project of interest.

5.3 Review Requirements

The government Project Manager (PM) and the duly designated representative of the Contract Officer (who may or may not be the PM) shall approve the initial PLA and all updates in writing, within one working week of receipt.

5.4 Acceptance Criteria

The PLA shall describe generally and in detail how new capability will interface efficiently and effectively with government furnished legacy capability, and planned next generation government capability.

5.4.1 PLA shall document how system-level, testable MOP are positively correlated with user-defined and testable mission level and business level MOE. Documentation shall include test results.

5.4.2 PLA shall describe specific engineering approaches for supporting extensibility, scalability, and interoperability through open standard interfaces, adapters, Software Development Kits (SDK), Application Program Interface (API), etc.

5.4.3 PLA shall describe how software-defined capability can or cannot be virtualized within relevant cloud service models.

5.4.4 PLA shall describe how software-defined capability can or cannot be re-hosted across device form factors of interest with particular emphasis on Disconnected, Intermittent, Low-bandwidth environments.

5.4.5 PLA shall describe how software-defined capability will provision and or/inherit cyber security controls to/from cyber security layers.

5.4.6 PLA shall describe how Intellectual Property Rights (IPR) implemented via software and/or hardware licenses positively and negatively impact the vendor's engineering approaches for supporting extensibility, scalability and interoperability.

5.4.7 PLA shall describe how software and/or hardware licenses fees support maintenance and technology refresh across vendor's capability lifecycle.

5.4.8 PLA shall describe how hardware and/or software license fees support maintenance and technology refresh of system's open standard interfaces.

6. Preparation Instructions

6.1 General Instructions

6.1.1 Format.

PLA may be in contractor format or per a template provided by government. Vendor may select relevant views from DoDAF and/or alternative architectural formats. Government acknowledges that DoDAF is not designed to address the detailed enterprise perspective required under this DID.

6.1.2 Applicable Standards

Chairman Joint Chief of Staff Instruction 6212.01 (latest version): Net Ready Key Performance Parameter

Carnegie Mellon University (CMU) Software Engineering Institute (SEI) Framework for Software Product Line Practice.

CMU SEI Intuitive Model for Product Line Economics (SIMPLE)

Defense Acquisition Guidebook (DAG), especially chapters 4, 5, 7, and 9

Defense Intelligence Information Environment (DI2E) Services View (SV) 4

Department of Defense Architectural Framework (DoDAF) (current version) or vendor-provided alternative points of departure.

DoD Instruction 8510.01 Risk Management Framework (RMF) for Information Technology (IT) (current version)

INCOSE BoK Part 3 & 4 & 5

ISO/IEC/IEEE 15288

MIL-STD-498, especially chapters 4 and 5.

6.2 Content Requirements

PLA may be in contractor format. Traditional systems engineering and project management artifacts, e.g. per DoD Architectural Framework (DoDAF), INCOSEBoK, and PMIBoK, may be streamlined and abstracted as appropriate. \ Agile software development artifacts, e.g. per SCRUM and EXTREME Programming, are generally consistent with PLA. Contractors should avoid bureaucratic and/or conceptual language, and emphasize reporting of essential, objective, data.

6.2.1 Appendices

Appendices may be added, as needed to clarify or provide additional detail to the deliverable.

Acronyms and Glossary

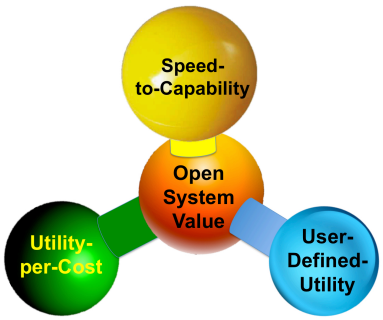
An acronym list and glossary of key terms used in the deliverable shall be provided.

Referenced Documents

If other documents or materials were cited in the document, a list of the referenced materials shall be provided. The reference list shall include the title of the material, author of the material, date of the material, and location where the material is stored.

APPENDIX B: 04 OSA PLUG TEST PLAN DID

Open System Acquisition (OSA) Plug Test Plan (PTP)



April, 2015

Secretary of the Air Force Acquisition Open System Acquisition

Revision History

.

REVISION HISTORY			
REVISION/WORKSITE #	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Draft -			

Approvals

Insert Project Approvals here.

NAME	ROLE	DATE

7.Introduction

7.1 Purpose

This DID describes the required elements of a rapid adaptive Open System Acquisition OSA) Test Plan.

7.2 Scope

Plug Testing is an industrial best practices for Validating and Verifying (V&V) that a particular modular technology component configures efficiently and effectively within the target system or system of system architecture. A Plug Test system consists of three interoperable subsystems: an instrumented reference implementation of the target architecture; a suite of test tools and services; an instance of the technology under test. The Plug Test evaluates any or all of the following: run time conformance to open standard interfaces; conformance with cyber security requirements; functional performance of components; cross-component interoperability in run time and build time; and system/mission level performance against Live, Virtual and Constructive (LVC) models and simulations. The Plug Test process generates documentation of each tested offering in any or all of these areas.

The OSA Plug Test approach aims to reuse any and all testing already performed by technology developers. Therefore entry criteria for Plug Testing activity include evaluating, verifying and validating developers' prior performance, including especially any previously collected tested results.

OSA solicitations, source selections, and contract performances metrics are based on Plug Test cases. That is, projects describe desired capabilities in terms of objective, plug testable requirements. Descriptions include details of the plug test system and how to get access to environment. The outcomes of plug tests of candidate offerings drive source selection. Contract language specifies plug testable threshold and objective requirements for deliverable technology.

OSA uses the results of Plug Tests to identify pre-approved-as-interoperable-and-sustainable COTS and GOTS components. In this sense the PTP is closely aligned with the associated Product Line Architecture (PLA). PLA supports optimal open system designs according to enterprise business and operational goals. PTP validates that PLA is on the mark, and verifies that technology components of interest comply with PLA.

The OSA Plug Test concept spans across distributed, virtual, Development, Test, Evaluation, and Certification environments. For example, an OSA Plug Test suite might span various physical cloud data centers owned and/or operated by government and/or industrial organizations.

Accordingly, this DID describes the specific format, content, and level of detail required for specifying application of plug testing for the project of interest.

7.3 References

fff. Brownsword, L., Albert, C., Carney, D., Place, P., Hammons, C., & Hudak, J. (2013). Isolating Patterns of Failure in Department of Defense Acquisiton. Carnegie Mellon University Software Engineering Institute. Pittsburg, PA: Carnegie Mellon University.

ggg. Chairman Joint Chief of Staff. (2012, March). CJCSI 6212.01F: Netready Key Performance Parameter (NR KPP). Washington, DC, US.

hhh. CMU SEI. (n.d.). A Framework for Software Product Line Practice, Ver 5.0. Retrieved July 14, 2014, from Software Engineering Institute, Carnegie Mellon University: http://www.sei.cmu.edu/productlines/frame_report/index.html

iii. Defense Acquisition University (DAU).Defense Acquisition Guidebook. Retrieved Dec 10, 2014, from Defense Acquisition Guidebook: https://dag.dau.mil/

jjj. Defense Science Board. (2009). DoD Policy and Procedures for the Acquisition of Information Technology. Washington DC: OUSD AT&L.

kkk. Department of Defense (DoD). (2008, December 15). DoD Instruction 5000.02: The Defense Acquisition System. 47. Washington, DC: USD AT&L.

lll. Department of Defense. (2009). Department of Defense Reliability, Availability, and Maintainability and Cost Rationale Report Manual. Washington DC: Office of the Secretary of Defense.

mmm. Department of Defense. (2006). Risk Management Guide for DoD Acquisition (Sixth Edition). Washington DC : DoD.

nnn. DoD. (2007). DOD Directive 8320.02: Data Sharing in a Net-centric Department of Defense. Washington, DC: DoD.

ooo. DoD. (2014, March 12). DODI 8510.01: Risk Management Framework. Washington, DC, USA: DoD.

ppp. DoD. (1994, Dec 5). Military Standard 498: Software Development and Documentation.

qqq. Gunderson, C. R. (2014, June 5). Enterprise Information System (EIS) Value Assurance Framework (VAF) Risk-Reward Optimization. Submitted to Journal of Enterprise Transformation. Herndon, VA, USA.

rrr. Gunderson, C. R. (2014). Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF). Naval Postgraduate School, Information Science. Monterey, CA: NPS.

sss. Gunderson, C. R., & Minton, D. (2009). CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2. 2009 AFCEA GMU Critical Issues in C4I Symposium. Fairfax VA: George Mason University.

ttt. International Council on Systems Engineering (INCOSE). (n.d.). Systems Engineering Body of Knowledge. (INCOSE, Producer) Retrieved Dec 10, 2014, from http://g2sebok.incose.org/

uuu. NIST. (2010). NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems. National Institute of Standards, Security Division. Gaithersburg, MD: NIST.

vvv. NIST. (2013). NIST SP-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards, Computer Security Division. Gaithersburg, MD: NIST.

www. Northern, C., Mayfield, K., Benito, R., & Casagni, M. (2010). Handbook for Implementing Agile in Department of Defense Information Technology Acquisition. MITRE. The MITRE Corporation.

xxx. Project Management Institute. (2013). Project Management Body of Knowledge, 5th Edition. New Town Square, Pennsylvania, USA: Project Management Institute, Inc.

yyy. SAF AQ Director of Transformational Innovation. (2014, October). Plug Fest Plus Action Plan. Washington , DC, US: SECAF.

zzz. Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L). (2013). DoD Open Systems Architecture Contract Guidebook for Program Managers. Washington, DC, US: AT&L.

aaaa. USAF Space and Missile Systems Center (SMC). (2014). Acquiring and enforcing the government's rights in technical data and computer software under dod contracts: a practical guide for acquisition professionals. USAF Space and Missile Systems Center (SMC). Huntsville, AL: SMC.

7.4 Acronyms

BoK	Body of Knowledge
BTCC	Bending the Cost Curve
CMU SEI	Carnegie Mellon University Software Engineering Institute
DAG	Defense Acquisition Guidebook
DID	Data Item Description
DoDAF	Department of Defense Architectural Framework
INCOSE	International Council on Systems Engineering
IPR	Intellectual Property Rights
OSA	Open System Acquisition
PLA	Product Line Architecture
PM	Project Manager
PMIBOK	Project Management Institute Body of Knowledge
PTP	Plug Test Plan

RMF	Risk Management Framework
SWaP	Size Weight and Power

8. Deliverable Description

8.1 Purpose

The Plug Test Plan provides the minimal set of documentation required to describe Validation and Verification of the efficiency and effectiveness of the relevant modules of technology within the target system architecture. I.e.:

8.1.1 Implement Test Driven Development in context with rapid, adaptive, Open System Acquisition (OSA).

8.1.2 Reuse test artifacts generated by technology developers in their own internal processes.

8.1.3 Validate that technology component(s) add(s) measurable value to operational and business use cases of interest.

8.1.4 Verify engineering-level "plug-and-play" interoperability of lifecycle supported COTS and GOTS components within target system architecture.

8.1.5 Verify modular component(s) support system performance requirements regarding latencies, loads, Size Weight and Power (SWaP), etc within target system architecture.

8.1.6 Verify operational-level interoperability of data and application functionality across enterprise system boundaries

8.1.7 Verify compliance with specified software assurance standards.

8.1.8 Verify that technology component(s) either inherit or provision cyber security controls from/to open standard "security" layer

8.1.9 Validate that technology component(s) under development and/or tech refresh achieve targeted utility improvement, cost-per-capability, and speed-to-capability targets.

8.2 Delivery Requirements

The initial PTP shall be delivered electronically, and presented verbally, in contractor's formant within ____ days of award, i.e. not later than _____. Updates that track either accomplishment and/or modification of previous iterations

shall be delivered electronically and verbally every _____ days on _____ throughout the life of the OSA project of interest.

8.3 Review Requirements

The government Project Manager (PM) and the duly designated representative of the Contract Officer (who may or may not be the PM) shall approve the initial PTP and all updates in writing, within one working week of receipt.

8.4 Acceptance Criteria

The PTP shall document a plan for V&V of how new capability will interface efficiently and effectively with government furnished legacy capability, and planned next generation government capability. In the regard, the PTP shall align with the associated PLA. In particular the PTP shall provision for the following:

8.4.1 V&V of plug test entry criteria against OSA requirements. Entry criteria for plug testing includes: documentation of Developmental Testing (DT) performed by vendor on all relevant COTS/GOTS components; prior performance of vendor regarding execution of OSA; existing Assessment and Authorization (A&A) documentation; documentation of prior plug testing, other interoperability testing, and Operational Testing (OT); existing technology licenses.

8.4.2 Development and/or refinement of a suite of MOE in collaboration with operational SMEs. MOE must be expressed in terms of measurable operational outcomes of interest.

8.4.3 Development and/or refinement of suite of select suite of MOP that are testably correlated to MOE, and address: functionality, interoperability, sustainability, and security.

8.4.4 Establishment of threshold and objective values for MOE and MOP and targeted continuous incremental improvement targets.

8.4.5 V&V of vendor-provided plug test entry criteria against OSA requirements. Entry criteria for plug testing includes: documentation of Developmental Testing (DT) performed by vendor on all relevant COTS/GOTS components; prior performance of vendor regarding execution of OSA; existing Assessment and Authorization (A&A) documentation; documentation of prior plug testing, other interoperability testing, and Operational Testing (OT); existing technology licenses.

8.4.6 Plug tests during every development increment that validate that system-level, testable MOP are positively correlated with user-defined and testable mission level and business level MOE for utility, speed-to-capability, and cost-per-capability, according to appropriate PLA.

8.4.7 Plug tests that V&V specific engineering approaches for supporting extensibility, scalability, and interoperability, e.g. open standard interfaces, adapters, Software Development Kits (SDK), Application Program Interface (API), etc.

8.4.8 Plug tests that evaluate how software-defined capability can or cannot be virtualized within relevant cloud service models.

8.4.9 Plug tests that evaluate how software-defined capability can or cannot be re-hosted across device form factors of interest with particular emphasis on Disconnected, Intermittent, Low-bandwidth environments.

8.4.10 Plug tests that verify how software-defined capability will provision and or/inherit cyber security controls to/from cyber security layers.

8.4.11 Plans and schedules for coordinating and allocating testing resources across parallel development activity, particularly during frequently scheduled integration events.

9. Preparation Instructions

9.1 General Instructions

9.1.1 Format.

PTP may be in contractor format or per a template provided by government.

9.1.2 Applicable Standards

Chairman Joint Chief of Staff Instruction 6212.01 (latest version): Net Ready Key Performance Parameter

Defense Acquisition Guidebook (DAG), chapter 9

DoD Instruction 8510.01 Risk Management Framework (RMF) for Information Technology (IT) (current version)

ISO/IEC/IEEE 29119

MIL-STD-498, chapter 5

NASA STD 8739.8: Standard for Software Assurance

9.2 Content Requirements

PTP may be in contractor format. It shall include scheduled preparatory and test events, and associated deliverable outcome artifacts. It shall explain how plug testing will be used to support rapid, adaptive open system test driven design. It shall document processes used to develop metrics and threshold and objective values as well as actual test equipment and procedures. Traditional systems engineering and project management artifacts, e.g. per DoD Architectural Framework (DoDAF), INCOSEBoK, and PMIBoK, may be streamlined and abstracted as appropriate. Agile software development artifacts, e.g. per SCRUM and EXTREME Programming, are generally consistent with PTP. Contractors should avoid bureaucratic and/or conceptual language, and emphasize reporting of essential, objective, data.

9.2.1 Appendices

Appendices may be added, as needed to clarify or provide additional detail to the deliverable.

Acronyms and Glossary

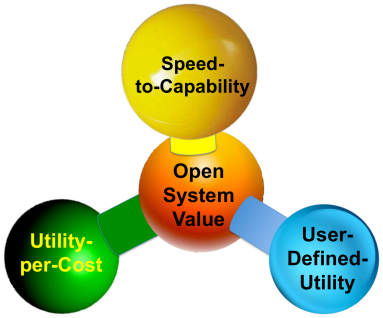
An acronym list and glossary of key terms used in the deliverable shall be provided.

Referenced Documents

If other documents or materials were cited in the document, a list of the referenced materials shall be provided. The reference list shall include the title of the material, author of the material, date of the material, and location where the material is stored.

APPENDIX B: 05 OSA IT USERS' GUIDE DID

Open System Acquisition (OSA) Information Technology Users' Guide (ITUG)



April, 2015

Secretary of the Air Force Acquisition Open System Acquisition

Revision History

.

REVISION HISTORY			
REVISION/WORKSITE #	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Draft -			

Approvals

Insert Project Approvals here.

NAME	ROLE	DATE

10. Introduction

10.1 Purpose

This DID describes the required elements of a rapid adaptive Open System Acquisition (OSA) Information Technology Users Guide (ITUG).

10.2 Scope

ITUG includes a "living" Concept of Operations (CONOP), developed in partnership with, and in support of the operational community of interest. ITUG also includes a detailed ever-evolving instruction manual for systems. The instruction manual explains to administrators, and operators how to operate, maintain, and update the evolving capability of interest in context with the evolving CONOP.

The CONOP is the means by which the operational community of interest explains its requirements for technology in context with its requirements for executing its mission threads. As such, the technology provider works with the supported operators and system administrators to capture critical as-is and to-be mission threads. Mission thread descriptions address workflows; supporting doctrine; mission systems and equipment; and enterprise infrastructure. The CONOP explains how organic and collaborating personnel, material, and doctrine combine to achieve targeted mission outcomes. The CONOP also explains how mission threads should evolve in step with the mission and adversaries' counter measures.

10.3 References

bbbb. Defense Acquisition University (DAU).Defense Acquisition Guidebook. Retrieved Dec 10, 2014, from Defense Acquisition Guidebook: https://dag.dau.mil/

cccc. Defense Science Board. (2009). DoD Policy and Procedures for the Acquisition of Information Technology. Washington DC: OUSD AT&L.

dddd. Department of Defense (DoD). (2008, December 15). DoD Instruction 5000.02: The Defense Acquisition System. 47. Washington, DC: USD AT&L.

eeee. DoD. (1994, Dec 5). Military Standard 498: Software Development and Documentation.

ffff. International Council on Systems Engineering (INCOSE). (n.d.). Systems Engineering Body of Knowledge. (INCOSE, Producer) Retrieved Dec 10, 2014, from http://g2sebok.incose.org/

gggg. Joint Chiefs of Staff. (2011, August 11). Joint Publication - 05: Joint Operations Planning. Washington, DC, USA.

hhhh. Northern, C., Mayfield, K., Benito, R., & Casagni, M. (2010). Handbook for Implementing Agile in Department of Defense Information Technology Acquisition. MITRE. The MITRE Corporation.

iiii. Project Management Institute. (2013). Project Management Body of Knowledge, 5th Edition. New Town Square, Pennsylvania, USA: Project Management Institute, Inc.

jjjj. Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L). (2013). DoD Open Systems Architecture Contract Guidebook for Program Managers. Washington, DC, US: AT&L.

kkkk. USAF Space and Missile Systems Center (SMC). (2014). Acquiring and enforcing the government's rights in technical data and computer software under DoD contracts: a practical guide for acquisition professionals. USAF Space and Missile Systems Center (SMC). Huntsville, AL: SMC.

10.4 Acronyms

BoK	Body of Knowledge
CONOP	Concept of Operations
CMU SEI	Carnegie Mellon University Software Engineering Institute
DAG	Defense Acquisition Guidebook
DID	Data Item Description
DoDAF	Department of Defense Architectural Framework
INCOSE	International Council on Systems Engineering
IPR	Intellectual Property Rights
ITUG	Information Technology Users' Guide
OSA	Open System Acquisition
PLA	Product Line Architecture
PM	Project Manager
PMIBOK	Project Management Institute Body of Knowledge
RMF	Risk Management Framework
SME	Subject Matter Expert

11. Deliverable Description

11.1 Purpose

The PLA provides the minimal set of documentation required to effectively describe the way functional modules of technology will be connected together effectively within the various form factor of interest. Intent is to:

11.1.1 Reuse existing technology specifications and users' guides.

11.1.2 Capture continuously evolving operational requirements, from the operational customers, in the operational customers' own language and context (i.e. via CONOP).

11.1.3 Explain in detail how the delivered technology satisfies operational requirements in context of relevant and evolving mission threads.

11.1.4 Provide step-by-step instructions for operating the delivered technology.

11.1.5 Provide step by step instructions for maintaining and upgrading delivered technology

11.1.6 Provide any and all technical documentation and license language necessary for all the above.

11.2 Delivery Requirements

The initial ITUG shall be delivered electronically, and presented verbally, in contractor's formant within ____ days of award, i.e. not later than _____. Updates that track either accomplishment and/or modification of previous iterations shall be delivered electronically and verbally every _____ days on _____ throughout the life of the OSA project of interest.

11.3 Review Requirements

The government Project Manager (PM) and the duly designated representative of the Contract Officer (who may or may not be the PM) shall approve the initial ITUG and all updates in writing, within one working week of receipt.

11.4 Acceptance Criteria

The ITUG shall describe generally and in detail how to operate, maintain, and upgrade the delivered technology, in context with user-defined mission threads of interest.

11.4.1 Performer shall work directly with designated operational Subject Matter Experts (SME) to develop a CONOP that explains missions, workflows, legacy and to-be technical architectures, and legacy and to-be doctrine in context with system of interest.

11.4.2 Performer shall establish and explain a feedback process with the operational customer for continuously evolving the CONOP. At minimum, CONOP updates will be published every _____ months.

11.4.3 Performer shall provide an operator's manual that explains in detail how operate the system in context with CONOP. Update in step with tech refresh. Explain update process.

11.4.4 Performer shall provide a system administrators' manual that explains in detail how maintain and update the system in context with CONOP. Update in step with tech refresh. Explain update process.

11.4.5 Performer shall explain and propose any and all technology licenses necessary to achieve the above.

12. Preparation Instructions

12.1 General Instructions

12.1.1 Format.

ITUG, including CONOP, Operators' Manual, System Administrators' Manual, and all supporting technology specifications may be in contractor format, or per a template provided by government, e.g. DAG CONOP Template.

12.1.2 Applicable Standards

Defense Acquisition Guidebook (DAG), CONOP Template (Optional)

ISO/IEC 26513:2009

MIL-STD-498, 5.12.3

Joint Publication – 05: Chapter IV

12.2 Content Requirements

ITUG artifacts may be in providers' format. The Government encourages providers to reuse existing specifications and language from existing manuals, modified as appropriate. Providers must explain how they will establish a continuous feedback loop with operational customers to keep CONOP up to

date, and to align Operators' and System Administrators' manuals with updated CONOP and technology. Appendices

Appendices may be added, as needed to clarify or provide additional detail to the deliverable.

Acronyms and Glossary

An acronym list and glossary of key terms used in the deliverable shall be provided.

Referenced Documents

If other documents or materials were cited in the document, a list of the referenced materials shall be provided. The reference list shall include the title of the material, author of the material, date of the material, and location where the material is stored.

APPENDIX C: SAMPLE OEIS MEASURES OF PERFORMANCE AND EFFECTIVENESS

Measures of Performance and Effectiveness for X-ISR SYSTEM

Effective systems engineering requires carefully scoped requirements captured in objective, testable, metrics together with targeted objective and threshold values for those metrics. Metrics should include Measures of Effectiveness (MOE) that come directly from operational user descriptions of critical use cases and desired outcomes, typically described by operational community members via "living" CONOPS document. MOE should be tightly coupled to objective Measures of Performance (MOP) that describe critical measurable and testable aspects of systems and processes. Given MOE, MOP, and associated objective and threshold values, a chief engineer can objectively manage risk by devoting sufficient time, people, equipment and funds to execute a test strategy that iterates around requirements measured at key integration points.

MOE and MOP for X-ISR SYSTEM capabilities address finding, fixing, and engaging high value individuals, events, and/or assets. MOE and MOP for acquisition process will address "speed-to-capability", i.e. the ability to rapidly intercept new technologies and apply them to rapidly evolving CONOPS and missions.

Notional Mission-Level CONOPS:

Daily operations are planned based on commander's intent and current intelligence. This process identifies daily Courses of Action (COA) and Critical, Conditions of Interest (CCI). CCI are alert criteria for observable people, events, or things whose identification will result in changes in planned COA. For example, if a high value target is identified, all assets might be dynamically re-assigned to interdict that target.

Operators deploy across area or responsibility (AOR) to execute their daily missions. The X-ISR SYSTEM and interoperating collection platforms perform ISR mission aligned with highest priority requirements. Analysts and watch standers collect and evaluate incoming intelligence. In the event that CCI are discovered while executing planned COA, ALCON respond accordingly to execute the emergent critical COA.

Engineering/Acquisition-Level CONOPS:

The X-ISR investment strategy aims to catalyze cross-organizational collaboration by incentivizing and enabling effective information collection and sharing among those program boundaries. X-ISR information systems must support rapidly evolving missions, mission partners, areas of operations, and CONOPS. Further, these systems must be designed to intercept rapidly evolving technological tools. Hence, a modular, open, standard, architecture (OSA), together with agile engineering and acquisition "plug-and-play" functionality, is key. In particular, systems designed and deployed to support one customer and mission must not only leverage the previously deployed capability, but also adapt to support future, as yet unknown, requirements.

Operational System-Level Metrics

MOE:

E1. Outcome (for finding): High Probability of Detection (Pd) of the individuals, events, and/or assets of interest supports successful collection and interdiction.

> **Measure**: Percent improvement in modeled/simulated Pd compared to baseline value where, e.g., Pd = (Correct IDs ÷ Total Incidents) – (False Positives ÷ Total Incidents)
>
> **Objective**: Pd = 100%.
> **Threshold**: Pd improves with every delivery spiral.

E2. Outcome (for fixing): Fixed spatial and temporal location of critical individual, event, or asset are sufficiently accurate to support successful interdiction and legal prosecution.

> **Measure**: Horizontal coordinates, e.g., degrees and decimal degrees of latitude and longitude per WGS 84, and seconds and decimal seconds per UTC of critical person, event, or thing.
>
> **Threshold**: Surveilled object's horizontal position fixed at +/- 3m σ_{90} from airborne ISR platform. Ground mobile PED node horizontal position fixed at location fixed +/- 10m σ_{90}.
>
> **Objective**: Surveilled object's horizontal position fixed at +/- 1cm σ_{90} from airborne ISR platform. Ground mobile PED node horizontal position fixed at location fixed +/- 3m σ_{90}.

E3. Outcome (for engaging): Detect-to-decision time line is short enough to support successful interdiction of critical targeted people, events, and things.

Measure: Minutes, and seconds between identification of CCI of and execution of associated decision to interdict
Threshold: 20 minutes. (For example…. The important consideration is that capability measurably improves over time as equipment and CONOPS improve.)
Objective: 10 minutes (For example…)

System Level MOP:

P1. Outcome: Critical Conditions of Interest CCI are identified.
Measure: yes/no
Threshold: yes
Objective: yes

P2. Outcome: All ground nodes can cue/slew airborne sensors/PED in response to evolving CCI in near real-time

Measure: yes/no complies with STANAG 4586 Interoperability Level 3; latency in seconds and decimal seconds
Threshold: yes; 1 sec
Objective: yes; 0.01 sec

P3. Outcome: XYZ radar cues FMV field of view to moving target of interest for ID and fixing

Measure: yes/no complies with STANAG 4586 Interoperability Level 3
Objective: yes
Threshold: yes

P4. Outcome: distributed, deployed operators and analysts share interactive Common Operating Picture (COP) in near real time

Measure: Tracks exist on shared COP yes/no; latency in decimal seconds
Threshold: yes; 1.0 second
Objective: yes; 0.01 second

P5. Outcome: Unambiguous and correctly identified tracks and contacts appear on COP along with notations

Measure: yes/no
Threshold: yes
Objective: yes

P6. Outcome: Each node can update COP with images, notations, contacts and/or tracks (as appropriate) and can interact via Internet Relay Chat.

Measure: yes/no
Threshold: yes
Objective: yes

P7. Outcome: Sensitivity of sensor plus Processing, Exploitation and Dissemination (PED) tools is sufficient to identify CCI from within aircraft mission profile.

Measure: Industry standard sensitivity metrics for sensors?
Threshold: ?
Objective: ?

P8. Outcome: Beyond line of sight (BLOS) bandwidth supports sharing Full Motion Video usefully.

Measure: MBS per second
Threshold: 3 MBS
Objective: 5 MBS

P9. Outcome: Beyond line of sight (BLOS) range is sufficient to share COP, including FMV, across all relevant nodes.

Measure: Dimensions of operational area of interest
Threshold: Dimensions of typical tactical Operational Area (per CONOP)
Objective: Dimensions of strategic Area of Interest

P10. Outcome: Critical message latency, including FMV, text, and NITF files supports successful interdiction of emergent targeted individual, event, or thing.

Measure: minutes, seconds, decimal seconds
Threshold: XX (Per CONOP)
Objective: YY (Per CONOP)

P11. Outcome: Need-to-share policy is specified and implemented robustly. (Need-to-share policy is the basis for allowing or denying access to network data and resources. In that sense, need-to-share policy is the basis of IA/CDS risk analysis.)

Measure: yes/no
Threshold: yes
Objective: yes

P12. Outcome: Certified and Accredited Cross-domain Solution (CDS) implements dynamic need-to-share policy across security domains in order to support interdiction of emergent targeted person, event, or thing, i.e., in near real time.

> **Measure**: Number of security levels crossed; message latency in decimal seconds
> Threshold: Across one level of security; 1.0 second
> Objective: Across two levels of security; 0.01 second

Engineering/Acquisition Process-Level Metrics

Process-Level MOE:

E4. Outcome: Continuously improving, cost-effective, capability.

> **Measure**: Value-per-Time-per-Cost where the measure of value is MOE; measure of time is delivery schedule; and measure of cost is lifecycle support budget in dollars.
> **Threshold**: Threshold MOE, delivered on schedule on budget
> **Objective**: Objective MOE, delivered on schedule on budget

<u>Process-Level MOP</u>:

P13. Outcome: Capability modules, i.e. system components, include life cycle support, i.e. guaranteed tech refresh, at known cost.

> **Measure**: yes @ cost in annual dollars; for some percent of required capability/no
> **Threshold**: yes @ budget; for 70% of required capability
> **Objective**: yes @ budget; for 90% of required capability

P14. Outcome: System components configure out-of-the-box.

> **Measure**: time in months and weeks required to bundle, test, and certify capability component
> **Threshold**: six months
> **Objective**: three months

P15. Outcome: System components are readily consumable via convenient procurement vehicle and delivery mechanism

> **Measure**: procurement lead-time in days, weeks, and months required to receive delivery of capability component
> **Threshold**: one month
> **Objective**: one week

P16. Outcome: New capability components that are developed at government expense (rather than procured off-the-shelf) are consistent with OSALR and include lifecycle support model, configure out-of-the-box within specified time window, and are readily consumable via convenient procurement vehicle and delivery mechanism

> **Measure**: OSALR intellectual property rights model for developed capability exists yes/no; MOP per above going forward.
> **Threshold**: yes; per Threshold MOP above
> **Objective**: yes; per Objective MOP above

> **Measure**: All delivered software is registered in the DI2E Storefront. yes/no; MOP per above going forward.
> **Threshold**: yes; per Threshold MOP above
> **Objective**: yes; per Objective MOP above

LIST OF REFERENCES

A. Bloch M, B. S. (2012). Delivering large-scale ITrojects on time, on budget, and on value. McKinsey & Company, Business Technology Office. McKinsey & Company.
B. Brooks, F. (1995). No Silver Bullet Refined. In F. Brooks, The Mythical Man Month. United States: Addison Wesley.
C. Brownsword, L., Albert, C., Carney, D., Place, P., Hammons, C., & Hudak, J. (2013). Isolating Patterns of Failure in Department of Defense Acquisiton. Carnegie Mellon University Software Engineering Institute. Pittsburg, PA: Carnegie Mellon University.
D. Chairman Joint Chief of Staff. (2012, March). CJCSI 6212.01F: Netready Key Performance Parameter (NR KPP). Washington, DC, US.
E. CMU SEI. (n.d.). A Framework for Software Product Line Practice, Ver 5.0. Retrieved July 14, 2014, from Software Engineering Institute, Carnegie Mellon University: http://www.sei.cmu.edu/productlines/frame_report/index.html
F. Defense Acquisition University (DAU).Defense Acquisition Guidebook. Retrieved Dec 10, 2014, from Defense Acquisition Guidebook: https://dag.dau.mil/
G. Defense Science Board. (2009). DoD Policy and Procedures for the Acquisition of Information Technology. Washington DC: OUSD AT&L.
H. Department of Defense (DoD). (2008, December 15). DoD Instruction 5000.02: The Defense Acquisition System. 47. Washington, DC: USD AT&L.
I. Department of Defense. (2009). Department of Defense Reliability, Availability, and Maintainability and Cost Rationale Report Manual. Washington DC: Office of the Secretary of Defense.
J. Department of Defense. (2006). Risk Management Guide for DoD Acquisition (Sixth Edition). Washington DC : DoD.
K. DoD . (2006). Earned Value Management Implementation Guide . DCMA. Washington DC: DoD.
L. DoD. (2007). DOD Directive 8320.02: Data Sharing in a Net-centric Department of Defense. Washington, DC: DoD.
M. DoD. (2014, March 12). DODI 8510.01: Risk Management Framework. Washington, DC, USA: DoD.
N. DoD. (2000, June). DoD Financial Management Regulation, Volume 2A. DoD Financial Management Regulation, 2A Chapt 1 paragraph 01208 , 1-19. Washington, DC, USA.
O. DoD. (1994, Dec 5). Military Standard 498: Software Development and Documentation.
P. Mil-Std-498 . Washington, DC, USA: Department of Defense.

Q. GAO. (2014). Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practies. Washington DC: GAO.
R. Gunderson, C. R. (2014, June 5). Enterprise Information System (EIS) Value Assurance Framework (VAF) Risk-Reward Optimization. Submitted to Journal of Enterprise Transformation. Herndon, VA, USA.
S. Gunderson, C. R. (2014). Enterprise Information System Value Model. NPS Technical Report. Washington, DC: Naval Postgraduate School.
T. Gunderson, C. R. (2014). Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF). Naval Postgraduate School, Information Science. Monterey, CA: NPS.
U. Gunderson, C. R., & Minton, D. (2009). CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2. 2009 AFCEA GMU Critical Issues in C4I Symposium. Fairfax VA: George Mason University.
V. Hokins, R., & Jenkins, K. (2008). Eating the IT Elephant: Moving from Greenfield to Brownfield Development. IBM Press.
W. International Council on Systems Engineering (INCOSE). (n.d.). Systems Engineering Body of Knowlege. (INCOSE, Producer) Retrieved Dec 10, 2014, from http://g2sebok.incose.org/
X. Joint Chiefs of Staff. (2012, January 19). Joint Capability Integration Development System Manual. Washington, DC, USA: JCS.
Y. Nagy B, F. J. (2013). Statistical Basis of Predicting Technological Progress. (N. U. Lis A. Nunes Amaral, Ed.) PLOS One (2).
Z. NIST. (2010). NIST SP 800-37: Guide for Applying the Risk Management Framework to Fedieral Information Systems. National Institute of Standards, Security Division. Gaithersburg, MD: NIST.
AA. NIST. (2013). NIST SP-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards, Computer Security Division. Gaithersburg, MD: NIST.
BB. Northern, C., Mayfield, K., Benito, R., & Casagni, M. (2010). Handbook for Implementing Agile in Department of Defense Information Technology Acquisition. MITRE. The MITRE Corporation.
CC. Project Management Institute. (2013). Project Management Body of Knowledge, 5th Edition. New Town Square, Pennsylvania, USA: Project Management Institute, Inc.
DD. Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L). (2013). DoD Open Systems Architecture Contract Guidebook for Program Managers. Washington, DC, US: AT&L.
EE. USAF Space and Missile Systems Center (SMC). (2014). ACQUIRING AND ENFORCING THE GOVERNMENT'S RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE UNDER DOD CONTRACTS: A PRACTICAL GUIDE FOR ACQUISITION PROFESSIONALS. USAF Space and Missile Systems Center.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943

4. Office of the Undersecretary of Defense for Intelligence
   1400 Defense Pentagon
   Washington, DC 20301

5. Office of the Secretary of the Air Force (Acquisition)
   1060 Air Force Pentagon
   Washington DC 20330