Administrative Changes to AFMAN 33-402, *Service Development and Delivery Process (SDDP)*

OPR: Has changed from SAF/A6CB to SAF/MGB

References to "SAF CIO A6" are hereby changed to "SAF/MG". 9 May 2016

References to hyper link "https://cs.eis.af.mil/afdbt/SDDP/default.aspx" are now https://cs.eis.af.mil/sites/10100/SDDP/default.aspx. 9 May 2016

Submit all Field User questions and inquiries for SDDP to the following link: https://cs1.eis.af.mil/sites/AFExec_UST/SiteAssets/Field%20User.aspx. 9 May 2016

Para 1.6.8.4. and Figure 2.7 referencing hyperlink https://cs.eis.af.mil/afdbt/COI/default.aspx is now https://cs.eis.af.mil/sites/10100/COI/default.aspx . 9 May 2016

Para 1.6.8.4 reference to usaf.pentagon.saf-us-m.mbx.af-coi-coord-panel@mail.mil will now be usaf.pentagon.saf-mg.mbx.mgb-cmo-secretariat@mail.mil. 9 May 2016

SDDP Tactics, Techniques and Procedures (TTP) can be found utilizing the following link: https://cs1.eis.af.mil/sites/AFEXEC_UST/SitePages/Home.aspx. 9 May 2016

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 33-402

25 SEPTEMBER 2014

Incorporating Change 1, 16 October 2014

Communications and Information

SERVICE DEVELOPMENT AND DELIVERY PROCESS (SDDP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6CB

Certified by: SAF/CIO A6S
(Brig Gen Sarah E. Zabel)

Pages: 71

This Air Force Manual (AFMAN) provides guidance for the definition, design, acquisition, implementation and delivery of Business Mission Area (BMA) capabilities using the Service Development and Delivery Process (SDDP). The SDDP is end user-centric to better align the assistance required by an end user to address a process-based problem across a holistic set of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) solutions. The SDDP details the processes and procedures by which Information Technology (IT) capabilities supporting Air Force (AF) processes are identified, defined, developed and delivered in a way that ensures IT capabilities are necessary, and maximize the potential for successful implementation of IT investments. The SDDP is applicable to large and small scale problems and can be used to implement IT capabilities of all sizes and types.

This Manual implements AF Policy Directive (AFPD) 33-4, *Information Technology Governance*, and AF Instruction (AFI) 33-401, *Enterprise Architecture*, by providing guidance for developing and implementing DOTMLPF-P requirements, including IT capabilities. It applies to all military and civilian AF personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. In accordance with AFI 33-360, *Publications and Forms Management*, this is a non-tiered compliance item. It applies to Air Force enterprise level capability delivery. Waiver authority for applying this AFMAN is SAF/CIO A6.

Send all recommendations for changes or comments to Air Force Chief Information Officer (SAF/CIO A6), 1600Air Force Pentagon, Washington DC 20330-1790, through appropriate channels, using AF Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

SUMMARY OF CHANGES

This interim changes adds Attachment 2 and 3 to AFMAN 33-402 and other administrative changes. A margin bar (|) indicates newly revised material.

Chapter 1—SERVICE DEVELOPMENT AND DELIVERY PROCESS OVERVIEW **4**

1.1. SDDP Objectives. 4

1.2. Executive Summary. 4

1.3. Information about this Manual. 5

1.4. PPBE, JCIDS, and DAS Alignment. 6

1.5. SDDP and Air Force Smart Operations for the 21st Century (AFSO21). 6

1.6. SDDP Roles and Responsibilities. 7

Chapter 2—SDDP OUTCOMES AND ACTIVITIES **15**

2.1. SDDP Targeted Outcomes. 15

2.2. SDDP Activities. 15

Table 2.1. SDDP Steps 16

Figure 2.1. SDDP 6 Steps Official Flow Overview 18

2.3. Conditions for Executing the SDDP. 18

2.4. Executing the SDDP. 19

Figure 2.2. PRM Information 22

Figure 2.3. BRM Information 26

Figure 2.4. DOTMLPF-P Implementation Plan 28

Figure 2.5. Contextual Model Example. 30

Figure 2.6. SRM Information (Parts 1-4) 35

Figure 2.7. DRM Information 40

Figure 2.8. M-Implementation Plan 42

Table 2.2. Skill sets included on Project Team 43

ATTACHMENT 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION **51**

Attachment 2—PERFORMANCE MEASUREMENT WITHIN THE SDDP **67**

Attachment 3—PLATFORM ENVIRONMENT AND BASELINES **70**

Chapter 1

SERVICE DEVELOPMENT AND DELIVERY PROCESS OVERVIEW

1.1. SDDP Objectives.

1.1.1. The primary objective of the SDDP is to focus diverse skill sets, resources and organizations on solving defense business system needs without placing the burden on the operator to be skilled in all the activities required when defining, developing and implementing solutions (e.g., architecture, system engineering, process improvement, project management, governance). This user-centric perspective focuses on explicit understanding of AF processes and organizational structures to help the user solve specific problems, and may result in process-derived, IT-enabled capabilities that can be effectively deployed on AF-provisioned classified or unclassified networks.

1.1.2. Use of the SDDP leads the end user to explore and identify the broader DOTMLPF-P solution set, including materiel solutions. When an IT capability is needed, the broader DOTMLPF-P solution set informs the change management strategy to assure successful implementation. To gain full support of the AF, the end user obtains sponsorship, usually from an AF Functional organization. Implementation of non-materiel solutions is executed by the Sponsor supporting the users through other existing methods, e.g., organizational change requests and policy development. Thus, the end user does not have to be a programmatic specialist to execute the SDDP. Instead, the end user relies on the Sponsor to enlist the support of specialists with required skill sets, to assist in the completion of the SDDP and the delivery of the process-derived capabilities in accordance with the business case supporting the materiel solution. When pursuit of a materiel solution is required (as determined by the Sponsor and appropriate requirements oversight organization), the SDDP process continues through a disciplined process of refining requirements, delivering the materiel solution, integrating, testing, and deploying full operational capability. The SDDP process, in Steps 3-6, relies on the partnership between the sponsor and the project team.

1.2. Executive Summary.

1.2.1. The SDDP improves the definition, design, acquisition, implementation and delivery of Information Technology (IT) Business Mission Area (BMA) capabilities. The SDDP is end user-centric to better align the assistance required by an end user to initially address process-based problems. The SDDP comprises six individual Steps that can be scoped to accommodate any size problem or need. Tasks can be accomplished in parallel and scoped appropriately to the complexity and scale of the problem to shorten development/delivery timelines. Each Step in the SDDP has specific product outcomes that serve as the basis for downstream activities in SDDP and facilitate enterprise-level analysis to maximize reuse of existing capabilities. Maximizing reuse will eliminate duplicate implementation activities across the AF and assure individual user problems or needs are not solved at the cost of overall enterprise benefits. Successful execution of the SDDP produces a well-described requirement, to include acquisition and implementation activities to support delivery of the capability. Success may also be demonstrated by the resolution of the user's problem without a materiel solution. The success of the SDDP in delivering IT defense business system capability is measured against the solution of the original problem brought forth by the end user.

1.2.2. The SDDP is centered on the end user and solving the end user's need/problem. In the SDDP, the requirements definition, architecture and design for an IT BMA capability is not outsourced to a contractor. Instead, the SDDP calls for a Sponsor to support the end user in obtaining assistance from multiple AF enterprise functions, potentially from different organizations, to define the requirement and design for an IT BMA capability such that the actual development can be acquired through detailed, controlled contract actions. The SDDP ensures the end user and the Sponsor consider all possible DOTMLPF-P solutions to the end user's need/problem, maximizes successful implementation of IT investments and ensures IT capabilities are not acquired unnecessarily.

1.2.3. The end user problems, addressed by the SDDP, are driven by a need to improve the effectiveness and efficiency in the execution of AF business processes. These processes include the BMA processes associated with logistics, personnel, finance, acquisition and other AF business operations. The SDDP is not intended for the development of specific AF resources such as weapons platforms, IT embedded in weapons platforms (sometimes referred to as Platform Information Technology or PIT) or physical network infrastructure.

1.2.4. The first two Steps of the SDDP focus on defining the end user problem in detail, streamlining business or mission processes, and identifying a set of potential DOTMLPF- P actions to address the need or problem. The remaining four Steps focus on the implementation of a materiel solution in the form of IT capabilities, assessing the success of the implementation against performance measures identified as part of the end user's need/problem statement. It is conceivable a successful SDDP effort would terminate after Step 2, as in the case where a Sponsor selects an identified non-materiel solution that would resolve the original user problem. Termination would still be considered a success, as user problems may be solved with a non-materiel solution.

1.2.5. The SDDP will generate information that can be used to support existing Joint Capabilities, Integration and Development System (JCIDS), Programming, Budgeting & Execution (PPBE), Defense Acquisition System (DAS) tasks/processes without adding duplicative work and will be combined into existing review and approval processes.

1.3. Information about this Manual.

1.3.1. This AF Manual documents the SDDP, providing both an overview of the SDDP and detailed descriptions of each Step, the objectives and expected outcomes for each Step, and the products for each Step. Process maps for each Step are included as part of the SDDP descriptions. Process maps and the detailed Steps illustrate functions that should be performed by individuals with skill sets described in Paragraph 1.6. For example, the AF Architects assist the Sponsor to look into the various repositories within which the AF Enterprise Architecture (AF EA) is captured to discover potentially reusable capabilities. The outputs of each Step are described in terms of the information captured as part of completing the Step. Specific formats for submitting this information will align with guidance/policy for the decision-makers/governance authorities being used (JCIDS, PPBE, DAS); Figures 2.2. – 2.8 provide basic examples for creating the products.

1.3.2. Detailed descriptions of the products that form the primary Enterprise Architecture (EA) artifacts are included. The content for these artifacts, which include the Performance Reference Model (PRM), the Business Reference Model (BRM), the Service Reference Model (SRM) and the Data Reference Model (DRM), are depicted in separate diagrams for

each reference model in the main body of this AFMAN. Examples of these products are available at **https://cs.eis.af.mil/afdbt/SDDP/default.aspx** on the SAF/US(M) SDDP SharePoint site. These artifacts are not the only products generated during the SDDP. Other products include: programmatic artifacts such as work plans, schedules and review packages; technical content such as analyses, test reports, evaluations and assessments; and business content such as cost estimates and business case analyses. These other products are described in more detail in the documentation of each Step **https://cs.eis.af.mil/afdbt/SDDP/default.aspx**.

1.3.3. DoD-level efforts underway continue to redesign the JCIDS and IT Box requirements processes. SAF/CIO A6 Portfolio Management Division will monitor these activities and refine the SDDP and this AFMAN as those decisions impact the SDDP and lessons learned are applied.

1.3.4. Other desirable enabling initiatives were identified during the development of the SDDP (such as the definition and configuration control of the baselines identified in Attachment 3 and the development of an EA Environment that facilitates the architectural analysis described within the SDDP). SAF/CIO A6 will continue to advocate for other enabling initiatives that will make the SDDP more efficient and effective.

1.4. PPBE, JCIDS, and DAS Alignment.

1.4.1. The SDDP will generate information to directly support other processes (e.g., acquisition, contracting, engineering, governance). PPBE, JCIDS, and the DAS are governance processes that support decisions related to requirements validation, funding certification and acquisition oversight. The SDDP will develop information documentation fully compatible with the PPBE, JCIDS, and DAS governance processes. Information will be generated one time and used many times in these various processes.

1.4.2. Documentation generated by the SDDP has been mapped against PPBE, JCIDS (AFROC/JROC), DoDI 5000.02 documentation to ensure SDDP integrates effectively into existing processes without adding duplicative work. A copy of that mapping is available at https://cs.eis.af.mil/afdbt/SDDP/SDDP%20Library/Forms/AllItems.aspx. The SDDP assures that information captured aligns to or exceeds the information requirements of JCIDS and other processes. In established PPBE, Acquisition, JCIDS guidance, since sponsor review is already required before meeting JCIDS or acquisition system authorities, SDDP will align with JCIDS review/approval (includes associated Acquisition & PPBE). This is likely to occur within all 6 steps. See Reference SDDP Acquisition Alignment Document for a mapping of SDDP to DoDI 5000.02 documents.

1.4.3. Other governance bodies (such as the Investment Review Board (IRB) and Defense Business Council (DBC) for Defense Business Systems (DBS)) may impose specific documentation requirements on projects coming to them for review. Information generated by SDDP activities would be used to populate those specific documents.

1.5. SDDP and Air Force Smart Operations for the 21st Century (AFSO21).

1.5.1. AFSO21 is the Air Force's dedicated effort to maximize value and minimize waste in all of our AF processes, focusing on continuous process improvement and root cause analysis, and leveraging collective experience, expertise, tools and best practices in identifying the best way to do work. AFSO21 is the Air Force's process change agent; it is

strongly encouraged that SDDP practitioners look to AFSO21 for support. However, because AFSO21 was not intended to focus specifically on the delivery of IT capability, it is important that SDDP activities augment and reinforce AFSO21 outputs in order to assure that the information captured is detailed enough to support the characterization of information exchange requirements that are a critical part of the IT capability requirement definition.

1.6. SDDP Roles and Responsibilities.

1.6.1. The processes outlined in this Manual are described in terms of specific activities to be conducted by personnel with specific skill sets. These are captured in the accompanying process maps in different swim lanes. This section describes, in general terms and at a high level, what those skill sets are and the roles and responsibilities of personnel providing those skill sets. Where possible and to aid the Sponsor in obtaining assistance, it also describes where those skill sets are currently working within the Air Force and where training on how to perform those activities might be obtained.

1.6.2. **SAF/CIO A6.** Overall responsibility for the successful deployment of IT capability is the SAF/CIO A6. It oversees activities within the BMA through the SDDP. An SDDP activity is shared among members of the Project Team, with the Sponsor taking the principal role to manage project work in Steps 1, 2 and 3, and the Project Lead taking principal management responsibilities in Steps 4, 5 and 6. The Project Lead will often be equivalent to a program manager. However, within the construct of the SDDP, a Project Lead could be responsible for more than one program. Therefore, we use the term Project Lead to distinguish this multiple responsibility from that of a single program manager. The Sponsor has the overarching responsibility to monitor all SDDP work performed in support of the problem statement/need and to work closely with the Project Lead to assure the capability developed and deployed satisfies the original problem statement/need.

1.6.3. **Functional/Subject Matter Expert (SME)**. The SME is usually the Core Function Lead (CFL). It performs activities in all six Steps of the SDDP. Personnel performing these activities understand, at an operational level, the stated problem and the mission processes that deliver the required capabilities. These SMEs remain assigned to the project lead throughout the SDDP process to ensure that definition, development and deployment activities are tightly focused on resolving the user's original problem statement. It is important to the success of the SDDP that SMEs be drawn from the community that is currently performing the subject mission (on the "front lines" of the mission) because the AF's operating environments are dynamic and rapidly changing. This skill set is also referred to in this Manual as the functional/SME or the warfighter. This skill set represents the needs of the end user community.

1.6.4. **Sponsor**.

1.6.4.1. The Sponsor is usually the HAF Functional and also performs activities in all six Steps of the SDDP. The Sponsor is the principal decision-maker and leads/controls the work performed in Steps 1, 2 and 3, and coordinates closely with the project lead who helps direct the work performed in Step 3 and leads/controls the work performed in Steps 4, 5 and 6 to ensure that the development and delivery of capability satisfy the requirement as defined in Steps 1-3. The Sponsor should have the authority to: resource the activities of the SDDP; make the decisions described in this Manual; direct the involvement of SMEs; and provide, direct or advocate for the necessary funding to

procure any materiel solution identified as part of the DOTMLPF-P capability set. If AF Corporate Structure review is needed to support the allocation of resources, the Sponsor will facilitate those reviews/approvals. The Sponsor enlists the support of skill sets as needed to complete SDDP activities satisfactorily and reviews/approves the major outputs of each Step. The Sponsor should be a general officer or senior executive.

1.6.5. **Enterprise Architecture (EA) Team**.

1.6.5.1. The AF EA is developed by SAF/CIO A6 and captures the structure of the AF, its missions, organizations and mission or business processes, the relationships between components, and the principles and guidelines governing their design and evaluation over time. The AF EA includes tracing these elements of the Air Force structure to the technical capabilities that are or will be implemented to support each of those elements. Thus, the AF EA maintains the links between specific AF mission processes and the specific materiel solution capabilities that support or automate those processes. The trace is maintained through connection to the Baselines that are under development by Air Force components, whose overall responsibilities for the Baselines are defined in AFPD 33-1, *Cyberspace Support*. These baselines include the Target Baseline, Implementation Baseline and Operational Baseline, which characterize the environment in which materiel solutions are deployed in support of mission processes. The AF EA maintains the traceability from user need to mission process to components of a materiel solution to enable the Air Force to identify reusable components in any materiel solution development.

1.6.5.2. The architects that make up the Architecture Team provide the skills needed to advise and assist the functional SMEs and Sponsor to: (1) generate information and capture the output of the SDDP activities into appropriate architectural artifacts (including DoDAF if required); (2) discover architectural content from the AF EA; and (3) retrieve and aid in the analysis of architectural artifacts by the SDDP team. The Architecture Team will conduct analysis of the AF EA that will include but not be limited to the following:

1.6.5.2.1. Identification of processes that may be impacted by re-engineering any particular process prior to any re-engineering.

1.6.5.2.2. Identification of duplicate processes to prevent redundant process re-engineering and to reduce the risk of negatively impacting one process with the results of re- engineering another process.

1.6.5.2.3. Identification of reusable components of materiel solutions, including reusable services, interfaces and information assets, to reduce cost and schedule impacts of new materiel solutions.

1.6.5.2.4. Identification of reusable EA artifacts, including process models, vocabularies, etc. to reduce time and cost of any SDDP activity.

1.6.5.2.5. Support for the identification and satisfaction of compliance requirements for a materiel solution by analyzing the AF EA for reusable artifacts or identifying potential inheritance of compliance certifications and accreditations, including information assurance (IA) certification, from other components within the AF EA.

1.6.5.3. Architects can be found in many places within the AF. The SAF/CIO A6 EA Division will validate HAF functional and MAJCOM architects that support their functional architectures. The Sponsor will have access to or know where to get support from architects. Alternatively, a Sponsor could choose to contract for architectural support for a specific SDDP project. The Architecture Team could comprise individual architects from across HAF offices or MAJCOMs. This would be particularly desirable, if the subject problem touched multiple functional or command communities. It would be useful if the Architecture Team included SMEs familiar with specific topics, such as Cybersecurity or compliance.

1.6.5.4. Architects should be conversant with Federal Enterprise Architecture (FEA), the Department of Defense (DoD) Enterprise Architectures (Warfighting, Business, Intelligence and Infrastructure, as appropriate to their problem space) and AF EA. Architects should have experience in capturing SDDP-like content into architectural artifacts. Training for architects is available both commercially and through Defense Acquisition University (DAU) and AF Institute of Technology (AFIT).

1.6.6. **Process Team**. The Process Team performs a fairly specific activity in facilitating a group of Functional/SMEs to understand, explain and capture their mission processes and to identify areas where processes could be improved, and to capture information needs of those processes. The tools and techniques of the AFSO21 methodology are particularly useful in conducting process re-engineering and improvement. Training in AFSO21 methodologies is available through MAJCOM and Wing AFSO21 offices or from SAF/US(M)S.

1.6.7. **System Engineering/Design Team**.

1.6.7.1. The System Engineering/Design team is responsible for generating the Step 3 architectural artifacts that describe the requirements of the materiel solution. From the information flows and targeted mission processes captured by the Process Team during Step 2 the System Engineering/Design team builds the information exchange requirements. These information exchange requirements form the core of the Contextual Model, which specifies the initial services to be included in the materiel solution. During Steps 4 and 5 these architectural artifacts are used to provide the familiar, traditional system engineering artifacts to define and control the development activities.

1.6.7.2. The System Engineering/Design team should also assure that the identified compliance requirements are captured in the materiel solution design delivered from Step 3. For example, Cybersecurity requirements may be tailored based on the course of action (COA) selected. Cybersecurity SMEs should advise in the requirements definition to assure the appropriate Cybersecurity considerations are designed into the materiel solution.

1.6.7.3. System Engineers can be found in many places within the AF, but are predominantly within the acquisition community since they can provide information on the risks, effort and, ultimately, the cost of providing a materiel solution. The Sponsor should be able to request support from the relevant Program Executive Officer (PEO). Alternatively, a Sponsor could choose to contract for system engineering support for a specific SDDP project. The System Engineering/Design Team could consist of individual engineers from across HAF offices or MAJCOMs; a particularly desired approach when the subject problem touches multiple functional or command communities.

1.6.7.4. Training on system engineering and design can be obtained from a variety of commercial and academic organizations, or through DAU and AFIT.

1.6.8. **Communities of Interest (COI) and the COI Coordination Panel**.

1.6.8.1. AF COIs support the implementation of process-derived, IT-enabled capabilities through the definition and articulation of detailed information requirements supporting the information exchanges identified within the targeted mission processes. The COIs capture the detailed information requirements in the Vocabulary Package, a major component of the DRM information that is included in the bounded user requirements resulting from Step 3 of the SDDP. The Vocabulary Package comprises the following individual products: 1) Identification of Authoritative Data; 2) Recommendation of Authoritative Data Source; 3) Roles and Permissions; and 4) Ontology. These requirements are then delivered for acquisition and implementation of the IT capabilities included in the materiel solution.

1.6.8.2. An AF COI includes Functional/SMEs from the SDDP product and additional stakeholders collaborating on behalf of various AF enterprise components for the purpose of exchanging information during the execution of their defined mission processes. These stakeholders have a vested interest in the problem statement/need but may come with a variety of roles and responsibilities from different organizations and functional areas.

1.6.8.3. The COI Coordination Panel provides AF enterprise level management and oversight for all AF COI activities. It operates under the authority and direction of the Enterprise Senior Working Group (ESWG). The Panel ensures normalization and harmonization of vocabularies and products across all AF COIs. The Panel will ensure maximum reuse of COI products, specifically vocabularies, to minimize duplication and conflict across COIs.

1.6.8.4. Additional information regarding AF COIs and the COI Coordination Panel, including training and templates to be used by AF COIs are available from the Panel Secretariat at USAF Pentagon SAF-US-M Mailbox AF COI Coord Panel <mailto:**usaf.pentagon.saf-us-m.mbx.af-coi-coord-panel@mail.mil**> or at **https://cs.eis.af.mil/afdbt/COI/default.aspx**.

1.6.9. **Governance Bodies**.

1.6.9.1. Governance is a management activity to oversee a capability implementation. To avoid conflict of interest, governance is conducted outside the Sponsor's authority. Governance assures that the delivered capability meets Legal, Regulatory and Policy (LRP) compliance criteria and makes sense in terms of return against the requested investment (ROI). Governance ensures that the implementation plan is sufficient to deliver the capability within the time-to-need specified by the user. Governance of an SDDP activity is provided by the ESWG under the IT Governance Executive Board (ITGEB). The ESWG will make decisions, where appropriate, and recommendations to peer Governance groups, for the specific decision or activity that needs Governance approval. The specific governance reviews needed to support SDDP activities are dependent on the type, size and cost of the materiel solution and therefore must be scoped in conjunction with the appropriate Governance team and captured into the project Integrated Master Schedule (IMS).

1.6.9.2. In Step 3, at the point at which a specific COA is selected, the appropriate Governance body reviews and validates the requirement. AF/A5R chairs the AFROC which validates all operational AF requirements. Defense Business Systems Management Committee has validation authority for any Defense Business System (DBS) that is not part of weapon system or directly involved in the fulfillment of military or intelligence mission. In addition, requirements may need to be validated by the DoD, depending on scope and complexity, either by the JROC or by the DBC, which has authority to certify the expenditure of funds. **Note:** As process efficiency, the ESWG also validates compliance for DBS modernizations costing over $1M.

1.6.9.3. Governance of acquisition activities is provided by the Acquisition Authority in accordance with AFI 63-101/20-101, *Integrated Life Cycle Management*. The AF Service Acquisition Executive (SAF/AQ) is responsible to oversee acquisition with ultimate responsibility resting with Under Secretary of Defense for Acquisition, Training and Logistics (AT&L). The acquisition authorities may delegate this responsibility to a PEO in accordance with DoDI 5000.02, Enclosure 3, Table 1. The Acquisition Decision Authority also serves as the Milestone Decision Authority (MDA).

1.6.9.4. The AF Corporate Structure also provides governance in terms of assuring programming of resources to support AF requirements. The AF Corporate Structure may review an SDDP activity's proposed capabilities and their general cost estimates in order to ensure alignment with AF Corporate strategic objectives and make necessary resource allocation decisions to support the implementation of the IT capability.

1.6.10. **Project Lead.**

1.6.10.1. The Project Lead for an SDDP activity is selected in coordination with the appropriate Program Office or PEO at the point in Step 1 when a specific materiel solution COA is selected. Once the requirement and resources are delivered at the end of Step 3, the Project Lead assumes primary responsibility of the project and maintains accountability through delivery of the capability to the user in Step 6. The Project Lead oversees the activities of the Project Team, which may directly report or may be virtually assigned to support the SDDP project, and assures that all necessary acquisition, governance, engineering, requirements traceability, contracting, development, platform engineering, testing, deployment and sustainment activities are captured in the Integrated Master Schedule (IMS). IMS activities should be accomplished in parallel and scoped appropriate to the specific materiel solution to expedite development/delivery of the capability. The Project Lead is accountable to the Acquisition Authority for cost, schedule, performance and material readiness of the materiel solution and to the Sponsor to assure that the capability delivered satisfies the user's problem statement/need within the time of need. The Project Lead develops all programmatic documentation required by law, regulation or policy, scoped as appropriate to support the IT capability.

1.6.10.2. The responsibilities of the Project Lead assigned by the PEO will correlate to those of a Program Manager, as defined in AFI 63-101/20-101. Depending on the scope and complexity of the requirement under development, the PEO may choose to establish a new program office, identify an existing program office to take responsibility for the project, or identify another PEO to oversee a project that is managed by the functional/sponsor or a supporting Field Operating Agency (FOA). It would be the

responsibility of the PEO and the functional/sponsor to assure that the selected Project Lead was appropriately trained. Project management training is available from a variety of commercial and academic organizations, or through DAU.

1.6.11. **Platform Engineering Team**.

1.6.11.1. The Platform Engineers support the platform environment into which the materiel solution is intended for deployment. The appropriate Platform Engineers are identified through coordination with AFSPC/A6 and the Infrastructure PEO (PEO C3I&N), which are responsible for provisioning the AF Operational Environment or Platform. Platform Engineers review the materiel solution requirements to assure it will deploy successfully into the Platform. If the Platform Engineers determine that changes to the Operational Environment are needed, they take the appropriate steps outlined in AFPD 33-4 to request change to the Target, Implementation and Operational Baselines which govern the Platform configuration. The Platform Engineers also assist with describing the technical requirement to connect to legacy systems and environments, and thus place requirements on the materiel solution.

1.6.11.2. Training for Platform Engineering is available from a variety of commercial and academic organizations, or through training provided by the communications career field functional manager.

1.6.12. **Integrated Test Team**.

1.6.12.1. The overarching functions of testing are to mature system designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force Test and Evaluation (T&E) community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities. The Integrated Test Team (ITT) is a cross-functional team of empowered representatives from multiple disciplines and organizations and co-chaired by operational testers and the program manager. The ITT is responsible for developing the T&E strategy and Test and Evaluation Master Plan (TEMP), assisting the acquisition community with T&E matters, and guiding the development of test plans that are integrated. Detailed instructions on the ITT can be found in AFI 99-103.

1.6.12.2. Testing occurs within the SDDP throughout the development and deployment of a capability, both as limited user evaluations of the software under development and as independent tests conducted by the Test Community. During IMS development, the ITT will recommend the appropriate combination and level of testing to be accomplished for development test, government acceptance test, integration test, independent test and user acceptance test.

1.6.12.3. The Project Lead is responsible for coordinating with the ITT to assure that appropriate testing organizations are represented on the Project Team. Testing advises in the development of performance measures and metrics to assure metrics are testable, participates in IMS development, oversees testing activities and with the Information Technology Lifecycle Capability (ITLC) assures that the Test Environment is requested and available to support testing activities.

1.6.12.4. Training for Test personnel is provided by the broader Test Community, including courses offered by DAU and AFIT.

1.6.12.5. The official direction for testing is AFI 99-103, *Capabilities-Based Test and Evaluation.* It describes the planning, conduct, and reporting of cost effective T&E programs as an efficient continuum of integrated testing known as seamless verification.

1.6.13. **Information Technology Lifecycle Capability (ITLC)**. The ITLC is a cross-functional capability that coordinates the test and integration efforts for the lifecycle of the new IT capabilities. The ITLC is a set of capabilities consisting of the functions listed below. Availability of these ITLC functions must be coordinated by the Project Lead from AF resources. For example, System Engineering functions may be available through the PEO responsible for the project. Help Desk functions may be available through the AF Integrated Network Operations and Security Centers.

1.6.13.1. System Engineering – ITLC system engineers will support architecture and technical analysis in addition to supporting Certificate of Networthiness activities associated with the ITLC mission.

1.6.13.2. ITLC Environment Management – The ITLC will define, request, and establish the CONOPS/Service Level Agreement (SLA) for the environment needed as a part of the ITLC mission in addition to maintaining the configuration of that environment in accordance with the Implementation Baseline.

1.6.13.3. Integration Services – As a part of performing Integration Services, the ITLC will support the Development Team, perform continuous integration, validate build packages, support quick look tests, and support deployment decisions.

1.6.13.4. ITLC Management Services - The ITLC Management Team will support the Project Team to provide assistance with product testing, configuration management, ITLC relevant contracting activities and other activities as requested.

1.6.13.5. Enterprise Help Desk Services – The ITLC will update and provide training for help desk for ITLC applications and operate the tier 2 help desk which will be integrated with other enterprise help desks.

1.6.13.6. Software Sustainment Support – The ITLC will sustain (within the boundaries of their organic skill sets) applications which have followed the SDDP process by evaluating the severity of fixes required by those ITLC applications and then proceeding to fix those ITLC applications as directed by the appropriate Sponsor/PEO.

1.6.13.7. IT&E Management Services – The ITLC will orchestrate Integrated Test and Evaluation (IT&E) for all ITLC applications by coordinating the participation of test organizations for all phases, and performing tests as assigned by the ITT.

1.6.14. **Contracting Team**. Contracting describes the skill set needed to capture a specific requirement or deliverable into a contract assigned to a specific vendor for delivery. The authority to enter into contracts on behalf of the Government is restricted to a Contracting Officer with an appropriate warrant. The Sponsor and the Project Lead will identify the appropriate Contracting Officer to support the Project Team. Training for Contracting Officers is provided by the contracting career field functional manager.

1.6.15. **Finance Team**. Finance describes the skill set needed to assure that funding is available to support the implementation of a materiel solution. Finance will assist with characterization of the funding profile (what type of money is needed when) and will verify that the business case supporting a materiel solution is adequate to justify the expenditure of resources. The Finance Team is not the approval authority for funds obligation or expenditure.

1.6.16. **Network Operations Team**. This skill set operates and maintains the platform and monitors the platform and applications deployed onto the platform. People who perform this task come from the organizations that provide a platform hosting environment (e.g., 24 AF or DISA). Training for Network Operations is provided by the communications career field functional manager.

Chapter 2

SDDP OUTCOMES AND ACTIVITIES

2.1. SDDP Targeted Outcomes. The SDDP is applied when an end user needs support in improving the effectiveness and efficiency of AF mission processes. The execution of the SDDP results in process-derived solutions across the entire DOTMLPF-P spectrum. The SDDP is applied to mission processes that utilize resources, such as operations planning, flight scheduling or in-transit visibility, or mission processes that manage those resources, such as command and control, just-in-time inventory or cyberspace operations. The SDDP is not intended for problems arising with the development of specific AF resources, such as weapons platforms or physical network infrastructures.

2.1.1. Key to successful SDDP employment is the early identification of outcomes that improve mission effectiveness (e.g., help improve the quality of the user's performance) or efficiency (e.g., enable the user to perform more quickly or accomplish the same performance with fewer resources) as compared to the user's current level of performance. Improved performance, both in terms of effectiveness and efficiency, is captured through high-level performance measures identified in Step 1 and refined through the remaining Steps. If a materiel solution is necessary, these performance measures support the definition of specific performance requirements for the materiel solution developed and inform the test and evaluation of the capability delivered.

2.1.2. The SDDP is designed to encourage the decomposition of warfighter needs into discrete and manageable components, each of which have standalone value to the warfighter. This allows for more rapid delivery of high-priority warfighter capabilities.

2.1.3. The SDDP depends on the reuse of products and information gathered from each Step for use in successive activities. Information or requirements identified in the early Steps will be reused to support oversight, compliance, test, accreditation and other activities later in the process. Work is only done once, and is done where it should be, with responsibilities and accountability remaining within the government. In addition, SDDP explicitly requires examination of existing fielded capabilities and artifacts for reuse. This reuse will allow the AF to realize savings of time and money that would otherwise have been expended to define duplicative capabilities/artifacts, such as compliance approvals, certification and accreditation (C&A) and training materials that would have had to be created for a new capability. By reusing previously generated artifacts, the Sponsor inherits capability, compliance and previous approvals, enabling the Sponsor to reduce resource consumption or shorten development timelines. For example, inheritance includes the situation in which an IT capability receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application.

2.1.4. The SDDP is designed for early and timely decision-making regarding the progress of the capability development. These early and timely decisions are intended to ensure that resources are not wasted in pursuing solutions that are neither feasible nor cost effective.

2.2. SDDP Activities.

2.2.1. The SDDP is employed for capabilities delivered to support mission processes. The SDDP commences with an end user's statement of a problem or need. This statement can come from a number of standard AF processes or activities, previously validated high- level requirements, problem statements and process descriptions derived from AFSO21 8- Step analyses (which will be the starting point for capturing the additional information flows within the process descriptions necessary to complete SDDP-derived IT requirements). These processes may be trigger events that generate a need to do more detailed requirements analysis and implementation using SDDP. By clearly defining requirements, decomposing capabilities into smaller, modular components, and reusing capability whenever possible, SDDP supports the rapid delivery of urgent requirements.

2.2.2. The end user aligns with a sponsoring organization that provides access to a wide range of AF corporate skill sets and support organizations that will assist in defining and implementing a solution that will meet the end user's needs or problems. The Sponsor will guide the activity through the AF Corporate Structure and appropriate Governance authorities to acquire the certifications, approvals and resource allocation needed to implement successfully the solution derived during execution of the SDDP. If a materiel solution is required and funded, the Sponsor delivers the requirement to the acquisition community, which takes primary responsibility to deliver a solution in partnership with the Sponsor.

2.2.3. The six SDDP Steps are described in **Table 2.1**:

Table 2.1. SDDP Steps

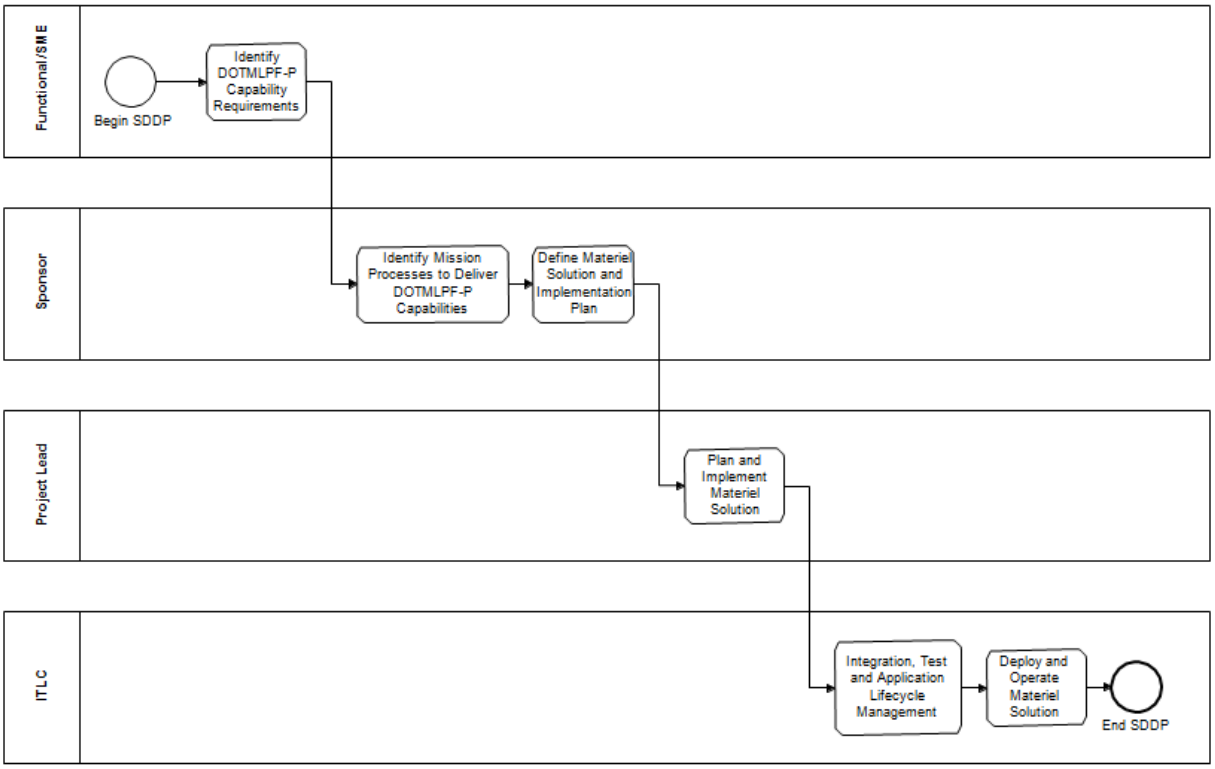
Step	Outcomes
Step 1 – Identify DOTMLPF-P Capability Requirements	Clear, concise statement of the user's needs and/or problems Delineation of a proposed set of capabilities that will solve the user's problem or meet the user's needs Documentation of relevant LRP requirements Generation of a set of performance measures that will indicate whether the capabilities, once implemented, actually solve the user's problem or meet the user's needs
Step 2 – Identify Mission Processes to Deliver DOTMLPF-P Capabilities	Re-engineered AF processes to improve effectiveness and efficiency Definition of the DOTMLPF-P executable actions and the implementation plan Sponsor approval to pursue the investigation of the materiel solution, if needed

Step 3 – Define Materiel Solution and Implementation Plan	Materiel Development Decision by Acquisition Authority Sponsor approval of the bounded user requirement, which includes definition of the materiel solution, information and data sources, and implementation plan Recommended implementation methods, e.g., web services code, systems and Commercial-Off-the-Shelf (COTS)/Government-Off-the- Shelf (GOTS) Optimizes reuse Approval by the AF Corporate Structure to fund and execute the implementation of the materiel solution
Step 4 – Plan and Implement Materiel Solution	IMS developed by Project Team from diverse organizations with a wide range of skill sets Delivered components of the materiel solution, accepted by the government
Step 5 – Integration, Test and Application Lifecycle Management	Validated solution that has been shown through test to satisfy the requirement and conform to security and configuration standards Definition of how the Platform is to be prepared to accept and manage the lifecycle of the deployed code
Step 6 – Deploy and Operate Materiel Solution and Measure the Success of the Capability Delivery	End user capability delivered/fielded in the Operational Environment and demonstrated to be successful Sustainment and, when appropriate, retirement of the materiel solution

2.2.4. The Steps of the SDDP generate products that are used in subsequent Steps. The products are continuously refined and detailed throughout the SDDP, as each activity builds upon the previous activities. Each of these Steps is decomposed into individual activities that will be completed by multiple supporting organizations and processes. Although the activities are depicted sequentially in the diagrams found in the appendices, they are executable in parallel. As a result, the SDDP is scoped to problems of different scope and complexity. For smaller problems or implementation of discrete components of a larger solution, the SDDP activities can be executed in parallel quickly; in some cases, the activities can be completed in very short spans of time. For example, in situations where the materiel solution addresses a need that is mission critical, the SDDP can be scoped as appropriate for the size and scale of the materiel solution, and tasks may be able to be accomplished in parallel to accelerate the activities in Step 3 to get to implementation more rapidly through parallel execution. If the mission need is so critical that there is no question that the materiel solution will be funded, the Information Analysis activities can be moved forward and executed in parallel with the Contextual Model and COA Development. In this situation, the SDDP can be scoped to generate the SRM and DRM information simultaneously. The

parallel activity can actually help inform the COA development and analysis for materiel solutions of smaller scope. The SDDP 6 Steps are depicted in **Figure 2.1**. Detailed versions of the process maps for all six SDDP steps are available at the SDDP SharePoint site at **https://cs.eis.af.mil/afdbt/SDDP/default.aspx**.

Figure 2.1. SDDP 6 Steps Official Flow Overview



2.3. Conditions for Executing the SDDP. The following conditions must be met to execute the SDDP:

2.3.1. The end users must obtain commitment from a Sponsor to manage the execution of the SDDP. If the end users are uncertain how to obtain a Sponsor's commitment, the end users should consult with their Functional organization at Headquarters Air Force, MAJCOM Leadership, or the AF Corporate Structure to obtain a Sponsor's commitment.

2.3.2. The end users' organization must commit SMEs to support the Sponsor in the execution of the SDDP.

2.3.3. The Sponsor must commit the resources necessary to assist the end users with completion of Steps 1 and 2 of the SDDP. These resources must provide the special skill sets required by Steps 1 and 2. The Sponsor may draw all resources from internal organizations, or may request assistance from other AF organizations to complete Steps 1 and 2.

2.3.4. If the decision is made to pursue a materiel solution, the Sponsor and Acquisition partners commit resources to continue the process in Steps 3 through 6. These resources must provide the special skill sets required by Steps 3 through 6. The Sponsor may draw all resources from internal organizations or may request assistance from other AF organizations.

2.4. Executing the SDDP. To initiate the SDDP, end users and Sponsors should refer to the detailed SDDP flow charts and the accompanying textual descriptions of each individual Step in the SDDP at **https://cs.eis.af.mil/afdbt/SDDP/default.aspx**. The product templates and examples will assist in explaining the work that needs to be completed in executing each Step in the SDDP. If either the end user's organization or the Sponsor is not completely confident in their ability to execute the SDDP without assistance, they can request support from the AF Deputy Chief Management Officer (DCMO). The AF DCMO's office can provide additional training and mentoring support to guide the end users and their Sponsor through the Steps of the SDDP.

2.4.1. **Step 1 – Identify DOTMLPF**-P **Capability Requirements**

2.4.1.1. **Purpose of the Step**. The purpose of Step 1 is to define the user's need/problem in sufficient detail such that a plan for implementing capabilities to solve the user's need/problem can be developed and implemented.

2.4.1.2. **Outcomes of the Step**. The expected outcomes of Step 1 are:

2.4.1.2.1. Clear, concise statement of the user's need/problem.

2.4.1.2.2. Delineation of a proposed set of capabilities that will solve the user's problem or meet the user's needs.

2.4.1.2.3. Generation of a set of performance measures that will indicate whether the capabilities, once implemented, actually solve the user's problem or meet the user's needs.

2.4.1.2.4. Documentation of relevant LRP requirements and constraints.

2.4.1.3. **Description of the Step**. The end user's organization works directly with the Sponsor to define the problem according to AF EA standards. The end users are represented by a set of SMEs who work with the Sponsor to define the problem. The Sponsor recruits assistance from the Architecture Team, with the Architecture Team either internal to the Sponsor's organization or recruited from outside the Sponsor's organization, from sources such as the AF Business Mission Area Directorate (SAF/CIO A6);. The Architecture Team works directly with the SMEs to elicit the nature of the problem as perceived by the SMEs and to capture the problem as part of the PRM information (**Figure 2.2**). The Sponsor approves/disapproves the outcomes of Step 1.

2.4.1.4. **Step 1 Activities**. The SMEs work with the Architecture Team and the Sponsor to define the problem by completing six major tasks within Step 1. The SMEs and the Sponsor can utilize different techniques and tools to execute Step 1 of the SDDP. However, the tools and techniques of the AFSO21 methodology are particularly useful in Step 1 and Step 2 of the SDDP and serious consideration should be given to the use of AFSO21 in these SDDP Steps. The activities in Step 1 are as follows:

2.4.1.4.1. **Define Need/Problem Statement.** The SMEs will work with the Architecture Team to state clearly and succinctly the problems identified during mission operations. Ideally, the problems should be stated in both qualitative and quantitative terms, providing the basis for defining performance measures that can be calculated to determine whether a potential solution actually meets the end user's needs or solves the problem. The SMEs document their needs in the PRM

information as part of the AF EA and then work with the Sponsor to develop a work plan to complete Steps 1 and 2. The work plan is based on the initial problem statement and will be updated and refined as the problem is better defined. The Sponsor reviews the work plan with the SMEs and either agrees to proceed with the SDDP or may decide that the need/problem statement is inadequate or is low priority and so may terminate the SDDP.

2.4.1.4.2. **List Relevant LRP Requirements.** The SMEs work with the Architecture Team to identify LRP requirements that must be addressed by any potential solution and the specific content within the LRP sources that affect any potential solution. The nature of the LRP requirements affects the scope of the problem, placing requirements on the implementation of any solution, and can either complicate or simplify the implementation. It may be determined that LRP requirements may need to be changed or waived in order to solve the user's need/problem. The LRP requirements are documented in the PRM information. The Architecture Team supports the SMEs with AF EA searches to locate candidate LRP requirements for consideration by the SMEs.

2.4.1.4.3. **Determine, Prioritize and Present DOTMLPF-P Capabilities to Sponsor.** The SMEs work with the Architecture Team to identify specific DOTMLPF-P capabilities that they believe are needed to solve the problem, as defined in the previous Step 1 activities. The SMEs consider the entire DOTMLPF-P spectrum in identifying the required capabilities. The capabilities are very high level statements at this Step and will be further refined and detailed as the SMEs and the Sponsor work through the Steps of the SDDP (see paragraph 2.4.1.5 below). The SDDP is designed to encourage the decomposition of warfighter needs into discrete and manageable capabilities, each of which is independently implementable and has standalone value to the warfighter. The SMEs prioritize these capabilities, so the Sponsor can consider resource limitations before deciding on whether to pursue any specific capability. Again, the Sponsor reviews the prioritized capabilities and decides either to continue the SDDP or halt the project. If the Sponsor decides to proceed, the capabilities are captured in the PRM information and linked to the user need/problem statement to maintain traceability between the original user need and the capability that will satisfy that need.

2.4.1.4.4. **Identify Performance Measures and Attributes.** The SMEs will work with the Architecture Team to identify performance measures and attributes that can be measured to determine the effectiveness of any potential implementation of the identified DOTMLPF-P capabilities. The performance measures and attributes are captured in the PRM information as part of the AF EA and are used as a foundation to define more system-specific performance measures and attributes during Step 3. **Note:** The Sponsor and SMEs may wish to consult with the Test Community in the capture of performance measures to assure that they are testable as the DOTMLPF-P Capabilities are implemented.

2.4.1.4.5. **Conduct EA Analysis.** The Architecture Team reviews the SME-defined needs/problems and capabilities to determine if some capability already exists within the Air Force, other Services, DoD/Federal Agencies and partner nations that may solve the SME defined problem. If a solution already exists, the Sponsor will direct

the SMEs to reuse the existing solution, and the SDDP will terminate. If there is no duplication, the Architecture Team will review the PRM information generated by the SMEs and ensure it aligns with AF strategy, and that all relevant LRP requirements have been identified and will be satisfied by the capabilities requested by the SMEs.

2.4.1.4.6. **Obtain Formal Review and Approval to Proceed.** The Sponsor reviews the PRM information generated by the SMEs, along with the Architecture Team's EA review and determines whether to proceed with the SDDP. This review is primarily a resource review, looking at the cost associated with completing Step 2 of the SDDP against the benefit of the capabilities and the Sponsor's other priorities. If necessary, the Sponsor obtains approval from the AF Corporate Structure to assure appropriate resource allocation. If all necessary approvals are forthcoming, the Sponsor and the SMEs will move to Step 2 of the SDDP.

2.4.1.5. One potential outcome of Step 1 is the decomposition of a problem that is very large and complex into discrete and modular capabilities that have standalone value to the warfighter, supported by IT capabilities developed in a way that maximizes the potential for reuse by other end users. In such cases, a single problem statement represented in the PRM information may spawn multiple SDDP Step 2s, where each Step 2 attacks a more discrete component of the problem documented in the PRM information. The resulting individual SDDP projects should be closely coordinated by the Sponsor(s) to assure that the resulting final solution sets resolve the original warfighter problem.

2.4.1.6. Given the results of several pilot activities used to build SDDP concepts and processes, the completion of Step 1 should be targeted to take no more than one month, depending on the resources available, scope and complexity of the problem that is being addressed by the SMEs.

2.4.1.7. **Products**. The primary output of Step 1 is the information listed in **Figure 2.2**, which is captured in the PRM of the AF EA. The PRM information documents the end user's needs and/or problems in the AF EA and provides the content necessary to complete the rest of the SDDP to help ensure that whatever solutions are implemented through the SDDP will solve the end user's problems and/or satisfy the end user's needs. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02 documents.

2.4.1.8. **Alignment with Governance Processes.** SDDP work will generate information needed to support the documentation requirements of JCIDS, DoDI 5000.02 or other applicable governance processes. For example, SDDP information captured in Steps 1 and 2 should support the population of an Initial Capabilities Document (ICD) format specified by JCIDS, an initial Problem Statement as required by DAS guidance, including Measures of Effectiveness (MOE) which validate outcomes to ensure the business need is satisfied and the necessary investment is justified, or the development of an initial CONOPS and architecture products as required by DoDI 5000.02. Some of this information is developed in Step 1.

Figure 2.2. PRM Information

PRM Information

Need/Problem Statement: A general statement that clearly describes the current situation causing inefficiencies and work delays. The need/problem statement includes an outline of what the need is, defines the problems that arise from the need, describes why the need is important, identifies the AF Senior Leadership that will support the initiative, details what improvements will result from the proposed changes and describes how the need is carried out.

LRP Requirements: All Federal laws and Federal, DoD and AF regulations and policies that affect or are affected by the identified need.

DOTMLPF-P Capabilities: A DOTMLPF-P capability is the ability of the AF to perform specific actions that, when taken together as a whole, will solve the end user's problem or satisfy the end user's need. When documenting possible DOTMLPF-P capabilities, a full and clear definition of the capability is required; what the capability does, what inputs and outputs are needed, and the anticipated outcomes to support the proposed changes must be included. It is important to note that a DOTMLPF-P capability refers to all possible solutions across the DOTMLPF-P spectrum, including Doctrine, Operations, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy.

Performance Measures: The establishment of a measurement of success, a target goal and a definition of how the improvements will be measured. Performance measures should be quantitative and testable. Understanding what the target goal is and measuring capability performance against the target goal provides verification that the capability is functioning as expected and that the end user's problem is solved or needs are met. A target goal can be established through the use of benchmark data. A benchmark is a standard of excellence or achievement that has been established, either from the commercial sector or by the government, as the optimum performance against which similar things can be measured or judged.

Performance Attributes: A description of the components that make up the successful delivery of capability (performance measure).

Note: For additional information on performance measurement within the SDDP, see https://cs.eis.af.mil/afdbt/SDDP/default.aspx.

Note: This information may support the generation of the following Acquisition Documents: Acquisition Strategy, Acquisition Program Baseline (APB), Market Research, System Engineering Plan (SEP), Life Cycle Sustainment Plan, Program Protection Plan, Problem Statement, AOA Study Plan, CDD, CPD, ICD. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoD.

2.4.2. **Step 2 – Identify Mission Processes to deliver DOTMLPF-P Capabilities**

2.4.2.1. **Purpose of the Step.** The purpose of Step 2 is to establish a plan to implement the capabilities across the DOTMLPF-P spectrum that are necessary to solve the end user's problems and/or satisfy the end user's needs.

2.4.2.2. **Outcomes of the Step.** The expected outcomes of Step 2 are:

2.4.2.2.1. Re-engineered AF processes to improve effectiveness and efficiency of those processes.

2.4.2.2.2. Definition of the DOTMLPF-P capabilities that need to be implemented to solve the user's problem and/or satisfy the user's needs.

2.4.2.2.3. Generation of a plan to implement the DOTMLPF-P capabilities as defined by the re-engineered business processes.

2.4.2.2.4. Sponsor approval to pursue the investigation of the materiel solution.

2.4.2.3. **Description of the Step**.

2.4.2.3.1. In Step 2, the primary activity is the generation of business process models that describe the mission processes. The mission process map will expand on the DOTMLPF-P capabilities identified in Step 1. The majority of the work is facilitated and captured by the Process Team, a group of business process engineers who specialize in designing and improving business processes. The Sponsor recruits the Process Team, again from either internal resources or from external sources. The Process Team works with the SMEs to re- engineer the mission processes and works with the Architecture Team to ensure that there is no duplication of mission processes.

2.4.2.3.2. Step 2 must result in re-engineered business process models that support Business Processing Re-engineering (BPR) assertions, as required by the Clinger-Cohen Act (CCA) and (in the case of DBS) National Defense Authorization Act (NDAA) 2010. Materiel solutions that will be implemented in Steps 3-6 of the SDDP are dependent upon the generation of the BRM information used to assert BPR in Step 2. As with Step 1, the AFSO21 tools and techniques are applicable in the re-engineering of the mission processes and should be considered seriously by the Sponsor for utilization in Step 2. For example, value stream mapping provides a valuable perspective prior to re-engineering the business processes. AFSO21 characterized countermeasures should help to inform the DOTMLPF- P Execution Plans that are an output of Step 2. The Sponsor approves/disapproves the outcomes of Step 2.

2.4.2.4. **Step 2 Activities**. Step 2 has six major tasks:

2.4.2.4.1. **Identify Mission Processes.** The SMEs identify those mission processes that must be engineered to deliver the DOTMLPF-P capabilities identified in Step 1. The mission processes could be processes that generate the DOTMLPF-P capability, or possibly could manage and control the DOTMLPF-P capability. The Architecture Team will look for potential reuse of mission processes that already have been modeled, thereby reducing the level of effort required to complete Step 2. The

Architecture Team will also consider what other AF mission processes may be affected by the mission processes Identified by the SMEs, and whether those processes will need to be included in the business process re-engineering.

2.4.2.4.2. **Update Work Plan.** Based on the number and complexity of the mission processes, the Sponsor will work with the SMEs to update the work plan from Step 1 and ensure the proper resources are available to complete Step 2 successfully. **Note:** See Glossary for typical content of work plans.

2.4.2.4.3. **Conduct Process Re-engineering.** The Process Team works with the SMEs to re-engineer the mission processes to meet the SME-identified needs and to deliver the DOTMLPF-P capabilities identified in Step 1. AFSO21 Rapid Improvement Events (RIEs) are particularly applicable during this task to elicit knowledge regarding the mission processes from the SMEs. The re-engineered mission processes are documented in the BRM component of the AF EA (**Figure 2.3**). The mission processes in the BRM information are traced back to the user needs and DOTMLPF-P capabilities identified in the PRM information from Step 1, and that traceability is maintained throughout the SDDP.

2.4.2.4.4. **Inform and Adjudicate Affected Processes.** The Sponsor works with the Architecture Team to detail what effect the re-engineered mission processes may have on other mission processes. The Sponsor notifies the owners of those other processes and works with those organizations to ensure that those other mission processes can accommodate the re-engineered mission processes without undue difficulty. The Sponsor may need to adapt the re-engineered mission processes in order to avoid major disruptions to other activities within the AF.

2.4.2.4.5. **Develop DOTMLPF-P Execution Actions and Plans.** The Sponsor uses the re- engineered mission processes and the DOTMLPF-P capabilities from Step 1 to develop a plan to implement the DOTMLPF-P capabilities as a set of solutions. The plan includes the materiel solution implementation through Steps 3-6 of the SDDP, as described in subsequent sections of this Manual. For the non-materiel/DOT-LPF-P) (Doctrine, Organization, Training, Leadership and Education, Personnel, Facilities, and Policy), the implementations are accomplished through other AF mechanisms, such as Organizational Change Requests. The results of this task are described in Task A4.2.3.5.2 at **https://cs.eis.af.mil/afdbt/SDDP/default.aspx**. Develop DOTMLPF-P Implementation Plan, which includes the different DOTMLPF-P solutions, characterized execution requirements, implementation work plans including schedules, resource allocations, anticipated ROI and investment auditability, and business case analysis supporting the solutions.

2.4.2.4.6. **Obtain Approvals and Validate BPR Sufficiency.** The Sponsor reviews the re- engineered mission processes in the BRM information, along with the DOTMLPF-P Implementation Plan, and determines whether to proceed with the SDDP. This review is primarily a resource review, looking at the costs associated with the implementation of the DOTMLPF-P solutions, at a very high level, against the benefit of the capabilities and the Sponsor's other priorities. If necessary to support resource allocation decisions, the Sponsor obtains approval from the AF Corporate Structure. If all approvals are forthcoming, the Sponsor and the SMEs will

move to Step 3 of the SDDP for a materiel solution identified in the DOTMLPF-P Implementation Plan.

2.4.2.5. **Products**. The primary output of Step 2 is the information described in **Figure 2.3**, which is captured in the BRM of the AF EA and **Figure 2.4**, the DOTMLPF-P Implementation Plan. The BRM information is generated throughout Step 2 and used in subsequent SDDP Steps. It also supports the BPR assertion required as part of Clinger-Cohen Act compliance or, in the case of some DBS, to satisfy the BPR requirements of NDAA 2010. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02 documents.

2.4.2.6. **Alignment with Governance Processes.** SDDP work will generate information needed to support the documentation requirements of JCIDS, DoDI 5000.02 or other applicable governance processes. For example, at the end of Step 2, SDDP information could support a Materiel Development Decision (MDD) documented by Acquisition Decision Memorandum (ADM).

Figure 2.3. BRM Information

BRM Information

Mission Process Map: Captures the description as a "picture" of the steps by which tasks are completed. The mission process map is a diagram that shows each process step, with a high-level description, and a description of how information flows from one step to the next within the process. The mission processes are identified as those processes that are necessary to deliver the capabilities identified in Step 1.

Auditable Mission Process Models: An in-depth description of a mission process from beginning to end. Each process is decomposed into its constituent activities or tasks, sometimes down to 2 or 3 levels of decomposition. The start event(s) that trigger the beginning of a process and the inputs provided at the start of the process are defined. The process steps are the actual activities performed by an AF resource that occur between the beginning trigger and the end output. The steps that trigger the end of the process and the work product (output) are clearly defined. Descriptive actions that take place at each step, along with an explanation why each step in the process is necessary, are included.

Information Flows: A description of how information assets move from one step to another in a process. An information asset flow begins with a description of who supplies the information and concludes with a description of the end product and identification of who the consumer is. Information flows are derived from the individual Information Puts and Gets included in the process models. Information Gets are information that is supplied to the task for consumption; Information Puts are information that is generated by the completion of the task.

Information Assets: The information that is consumed during a task within the Auditable Mission Process Model, as well as the information that is produced during completion of the task. An information asset is a definable piece of information, stored in any manner, which is recognized as valuable to an organization. Information assets are modeled within the process as individual Gets and Puts.

Business Rules: There are several types of business rules that are generated. Business rules define how a task identified in the Auditable Mission Process Model is completed; for example, defining how a specific output of a process is generated. Business rules can also define the constraints for a task, articulating how a task is completed in terms of performance, such as the time in which the task must be completed, or the scope of the information produced or consumed during the task; for example, all units that fall under the command of a specific commander. Business rules are also applied to the information flows and information assets associated with a specific Auditable Mission Process, such as restricting information about a specific Wing during a specific timeframe for a specific operation. The business rules also define access controls, such as providing only the information on personnel for those units under the direct command of the requesting personnel.

Enterprise-Level Dependencies: Process dependencies are enterprise-level associations (i.e., dependencies) among mission processes. Dependencies describe the interdependence among processes, are based on information, materials or other resources and describe the influence of time events on the execution of processes.

BPR Assertion: The documentation, presentation and AF Senior Leader validation of BPR, as required by the Clinger-Cohen Act and in the case of Defense Business System modernization with total cost of over $1M (NDAA 2010). The BPR Assertion is needed to implement an IT-enabled materiel solution beginning in Step 3. BRM information and the DOTMLPF-P Implementation Plan, generated in Step 2, are used to assert BPR sufficiency.

Note: This information may support the generation of the following Acquisition Documents: Acquisition Strategy, SEP, Program Protection Plan, Problem Statement, CDD and ICD. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02.

BRM (Part 2)

Figure 2.4. DOTMLPF-P Implementation Plan

DOTMLPF-P Implementation Plan

Characterized Execution Requirements: The execution requirements define what DOTMLPF-P actions need to be taken to implement the re-engineered mission processes characterized in the BRM. These requirements range from relatively straight forward actions such as modifications to Air Force Manuals to more complex structural changes such as new organizational structures or responsibilities.

ROI and Investment Auditability: The plan includes an estimate on the ROI for implementing the DOTMLPF-P actions embodied in execution requirements. The ROI includes methods to audit the costs and benefits of the DOTMLPF-P actions to ensure that the ROI is measurable and can be assessed by the Sponsor to ensure the success of the DOTMLPF-P Implementation Plan.

Work Plans: Each of the DOTMLPF-P actions will have a top level work plan described in terms of what steps will be taken to implement the DOTMLPF-P actions embodied in the execution requirements, the timeline for completing those steps and a rough order of magnitude resource estimates to complete the DOTMLPF-P actions.

Business Case Analysis : A business case analysis will be included that lays out the argument for proceeding with the DOTMLPF-P Implementation Plan. This includes analysis of the execution requirements scope and complexity, the risk associated with achieving the ROI and the feasibility of the work plans to implement the DOTMLPF- P actions successfully and achieve the ROI.

Note: This information may support the generation of the following Acquisition Documents: Acquisition Strategy, Program Protection Plan, Problem Statement, CDD, CPD, ICD and Requirements Strategy. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02.

2.4.3. **Step 3 – Define Materiel Solution and Implementation Plan**

2.4.3.1. **Purpose of the Step**: The purpose of Step 3 is to define the materiel solution component of the DOTMLPF-P capabilities and to plan the materiel solution implementation. Step 3 builds upon the products delivered in the first two Steps of the SDDP to generate the content that informs and guides the implementation of the materiel solution in the subsequent SDDP Steps. Step 3 is designed to support rapid acquisition of incremental capabilities by scoping the level of effort for each activity in SDDP Steps 3 through 6 to adapt to the size and scale of the materiel solution, and thus supports the mandates of NDAA 2010 Section 804. Step 3 is user-driven under Sponsor Leadership, drawing on the appropriate skill sets from other team members, including end user and SMEs during all the Step 3 activities. The Sponsor reviews and approves Step 3 products.

These two attributes of Step 3 enable the AF to meet the NDAA 2010 Section 804 mandate of user involvement.

2.4.3.2. **Outcomes of the Step**. The expected outcomes of Step 3 are:

2.4.3.2.1. Sufficient definition of a materiel solution, as identified in the DOTMLPF-P capabilities resulting from Step 2, such that the user's problem will be solved and/or the user's needs will be satisfied upon implementation of the materiel solution.

2.4.3.2.2. Definition of a materiel solution that considers all possible approaches to implementation, including web services, traditional systems and COTS/GOTS software, including modernization of legacy systems where appropriate under the business case, and leverages reusable components as much as possible. Reuse of existing solutions reduces implementation cost and time, simplifies the technical implementation of the materiel solution and simplifies the programmatic implementation by identifying existing architectural artifacts that, through reuse, can be inherited by subsequent activities in the SDDP. This inheritance simplifies and streamlines activities such as certification and governance, as well as the preparation of acquisition documentation to support the materiel solution.

2.4.3.2.3. Alternate COAs that incorporate multiple implementation approaches will be considered for selection as the implementation approach for the materiel solution to help achieve the mandates of NDAA 2010, Section 804, for modular, open systems as a key feature of the COAs that are proposed and evaluated. Alternate COAs should look first to COTS/GOTS reutilization, then to web services, and if those cannot satisfy the requirement, then to system implementation.

2.4.3.2.4. Generation of a plan to implement the selected materiel solution that is feasible, economical and can be executed within a schedule that will meet the user's time frame for success.

2.4.3.2.5. Approval by the AF Corporate Structure to fund and execute the implementation of the materiel solution.

2.4.3.3. **Description of the Step**. Step 3 of the SDDP consists of the seven major tasks described below. If Steps 1 and 2 were completed through an AFSO21 activity, artifacts derived in that activity, such as a future state map, should be used to help shape the materiel solution defined in Step 3. The Sponsor delivers the outcomes of Step 3, which are the final materiel solution requirements and funding, to the identified Product Lead/Project Center for implementation in Step 4. Through Step 3, the Sponsor partners with the Project Lead and starts to build a team with the appropriate skill sets to complete Step 3 work (SMEs, Architecture Team, System Engineering, Platform Engineering, Test Community and others) to assure that the requirement developed in Step 3 is sufficient to carry forward in the execution of the subsequent SDDP Steps.

2.4.3.3.1. **Design Contextual Model.** The Sponsor initiates Step 3 by forming a System Engineering/Design Team to assist in the development of the detailed requirements for the materiel solution, identified within the DOTMLPF-P Implementation Plan generated in Step 2. The System Engineering/Design Team may be available from a variety of places (e.g., Sponsor resources, ITLC). The first task for the System Engineering/Design Team is to bind the materiel solution to the

mission processes from Step 2 that will be addressed by the materiel solution. Not all the processes identified in the process models, generated during the BPR in Step 2, will have some automated capability to support the process. Thus, the first task of Step 3 is to identify those mission processes that will have support from the materiel solution. The processes that are selected compose the Contextual Model. The System Engineering/Design Team identifies the relevant information necessary to support the processes in the Contextual Model, how that information flows between the processes and any business rules derived from the mission processes that affect that information. The System Engineering/Design Team reviews the Contextual Model with the SMEs to ensure the materiel solution is addressing the most important mission processes, identifying, early on, any SME requirements for presenting information to the end user. After SME review, the Sponsor reviews the Contextual Model and either sends the model back for rework, or proceeds to the next task in Step 3. The Sponsor may wish to consult with appropriate skill sets, including the Project Lead, System Engineering and Test Community. An example of a Contextual Model is shown at **Figure 2.5**.

Figure 2.5. Contextual Model Example.

PROCESS	STEP	GET (INPUT)	PUT (OUTPUT)	SOURCE	DESTINATION
Develop Air Force Top Line	Get Top Line from OSC	Control Total (Air Force Top Line)		OSD	A8P
	Send Blue TOA to A8P		Control Total (Blue TOA)	FMB	A8P
	Inform AFCS of Bill to Pay		Bill to Pay (Initial Allocated Bill to Pay)	A8P	AF Board, AF Council Chairs
	Distribute Final Bill to Pay		Bill to Pay	A8P	Panels, FMBP

2.4.3.3.2. **Activities to Build Materiel Solution Implementation (M-Implementation) Plan.** This task selects an approach for implementation of the materiel solution development and generates the plan for completing that implementation successfully. The Sponsor's team identifies alternate COAs the Sponsor can take to implement the materiel solution. The COA can include different technology solutions, such as web services, traditional systems implementation, COTS/GOTS software or reused components already owned by the AF, other Services, DoD or Federal Agencies, or any combination of those technology solutions. The Sponsor reviews the developing M-Implementation Plan through the Sponsor Review Package, which captures the descriptions of the individual COAs

generated in Step 3. The development, evaluation and selection of the COAs include the following tasks:

2.4.3.3.2.1. The Sponsor works with the SMEs and the rest of the Sponsor's team to develop functional evaluation criteria for the COAs to ensure that each COA will meet the SME requirements as defined in the Contextual Model. This retains the emphasis on the end-user involvement to better assure successful implementation in accordance with NDAA 2010 Section 804.

2.4.3.3.2.2. Subsequently, for each COA, the Sponsor works with the Project Lead and other members of the team to capture the cost of implementation, including the cost of DOT-LPF-P change management needed to assure success of the deployed capability, and to capture any risks associated with the COA.

2.4.3.3.2.3. For each COA, the Sponsor asks the AF Governance Team to identify the compliance requirements. Compliance levies a wide range of requirements; including but not limited to: CCA, BPR, Privacy Impact Assessment (PIA), Federal Information Security Management Act (FISMA) and Federal Acquisition Regulation (FAR).

2.4.3.3.2.4. The Sponsor works with the members of their team to complete the description of each COA and with the team assesses each COA's ability to meet all the requirements for the materiel solution as defined in the Contextual Model.

2.4.3.3.2.5. The Architecture Team identifies possible reuse components where existing AF capabilities can satisfy some of the requirements in the Contextual Model. The reuse components are incorporated into the COAs.

2.4.3.3.2.6. The Architecture Team also looks for compliance requirements that can be satisfied by inheriting previous certifications from other implementations, such as those provided by the platform environment or from reused components. These inherited certifications have artifacts that the Architecture Team includes in the reuse components for each COA.

2.4.3.3.2.7. Next the Sponsor works with the members of the Sponsor's team to identify the DOT-LPF-P impacts of each COA and with the Architecture Team looking for reuse of other DOT-LPF-P implementations, the Sponsor assesses the scope, scalability and degree of difficulty in implementing the DOT-LPF-P requirements necessary to make the materiel solution fully operational.

2.4.3.3.2.8. The Sponsor's Team also works with a Platform Engineering Team to identify for each COA mission critical platform services requirements, platform compliance requirements such as standards that need to be met, infrastructure topological adjustments needed any new or additional services the platform environment may need to provide, including taking action necessary to engage with Target, Implementation or Operational Baseline (See AFPD 33-4) to initiate necessary change requests.

2.4.3.3.2.9. The Sponsor works with the members of their team to generate cost and risk estimates for each COA and using the evaluation criteria developed with the SMEs, assesses the COAs and selects one for implementation. The Sponsor

should address high- level development, acquisition and sustainment strategies for each COA and the cost of implementing those strategies.

2.4.3.3.2.10. The Sponsor considers the alternate COAs and selects the COA that seems best able to satisfy the initial user problem/need. The Sponsor reviews the selected COA with the AF Corporate Structure to assure appropriate resource allocation and alignment with AF strategic objectives and priorities, and proceeds to the appropriate AF and DoD governance bodies to obtain approval to expend funds and implement the materiel solution. If the COA selected is likely to result in the acquisition of a materiel solution, the COA analysis and selection will also support an MDD and selection of the preferred alternative.

2.4.3.3.3. **Onboarding Activities.** This task ensures the materiel solution will result in an implementation that can be onboarded (deployed, operated and maintained) by the AF enterprise. The Sponsor's team works with a Platform Engineering Team that consists of specialists from different organizations involved in the implementation, operation and sustainment of the AF platform environment. The platform environment consists of the physical infrastructure, middleware and enterprise services such as security and monitoring, and support functions such as Help Desk and configuration management, that are consistent across the AF enterprise. For more information on Platform Environments, see Attachment 3. The Platform Engineering Team supports the Sponsor's team during the COA development.

2.4.3.3.3.1. After the COA is selected by the Sponsor, the Platform Engineering Team identifies the technical requirements for connecting to the legacy systems and environments which, by their need to interface with the materiel solution, place requirements on the materiel solution implementation. The Platform Engineering Team identifies monitoring requirements for each of the components within the materiel solution as well as the Service Level Agreements (SLA) for the capabilities delivered by the materiel solution.

2.4.3.3.3.2. Finally, the Platform Engineering Team works with the Project Lead to develop an initial test strategy for the materiel solution, to test user interface, data exchange, and performance requirements—which include but are not limited to response time, availability (uptime)—as well as the accuracy of the business rules.

2.4.3.3.4. **Obtain Appropriate Governance Approvals.** SDDP generates information that is useful to support governance oversight in a consistent and coherent message. At appropriate points in the SDDP, the Sponsor will need to assure:

2.4.3.3.4.1. **Requirements Validation.** This task ensures that the identified requirements are validated by the appropriate approval authority. The Sponsor should consult with AF/A5R to assure appropriate requirements validation is accomplished.

2.4.3.3.4.2. **Compliance Governance**. This task ensures that the materiel solution development complies with all Federal, DoD and AF LRP requirements. The Sponsor prepares a Governance Package that addresses all the compliance

requirements for the COA selected for implementation and assesses the financial cost of compliance as part of the requirements definition. Note: Example content of a governance package for a DBS is captured in Figure 2.8 M-Implementation Plan (packages for other governance bodies may be different). The Sponsor takes the Governance Package through the appropriate governance reviews to obtain approval to proceed with the implementation of the materiel solution. For business systems, the package would be reviewed by the ESWG, the AF DCMO, the IRB and the DBC. For all IT capabilities, the Acquisition Authority and Platform provider will review the package.

2.4.3.3.4.3. **Acquisition Governance.** This task ensures that the appropriate acquisition oversight is maintained over the materiel solution development and delivery. The Sponsor should consult with the Acquisition community to assure the appropriate acquisition approvals are accomplished. **Note:** If the COA selected is likely to result in the acquisition of a materiel solution, the COA analysis and selection will also support an MDD and selection of the preferred alternative.

2.4.3.3.5. **Identify Project Lead.** At this point in Step 3, the leader/follower partnership between the Sponsor and Acquisition-selected Project Lead begins to shift, as work is increasingly performed by the acquisition partners. For the remainder of Step 3, more specific requirements related to the COA selected are derived.

2.4.3.3.6. **Information Analysis Activities.** This task completes the detailed information requirements that drive the materiel solution. The System Engineering/Design Team works from the Contextual Model and the selected COA to identify the initial requirements for the functions and/or services of the materiel solution, coupled with the information exchanges (flows of information between components of the materiel solution or other AF capabilities) that must occur in the materiel solution. The Architecture Team supports the documentation of the information requirements in the SRM information (**Figure 2.6**) and the DRM information (**Figure 2.7**). The Architecture Team identifies reusable information exchanges that may already be implemented. Each information exchange can consist of multiple information assets, which are discrete information products that are useful individually or collected into information exchanges. An information asset may support multiple information exchanges. The Sponsor charters a COI or uses an existing COI to define the information assets that are included in the materiel solution. The Architecture Team looks for reusable COI artifacts and provides that content to the COI to complete the information requirements. The COI defines the following information requirements:

2.4.3.3.6.1. The authoritative data that compose each information asset in each Information Exchange.

2.4.3.3.6.2. The authoritative data sources.

2.4.3.3.6.3. The roles and permissions associated with the information assets (derived from applicable enterprise architecture information) that enable users to access and manipulate the data within the defined processes (subject to approval of the appropriate functional leadership, and in consultation with the original

classification authority).

2.4.3.3.6.4. A vocabulary (based on the COI's ontology, semantic and structural metadata) that defines the assets, their authoritative and source data, and the roles and permissions in a machine-readable form.

2.4.3.3.7. **Prepare Bounded User Requirements for Implementation.** This task packages up the requirements for the materiel solution development and delivers them to the Program Office or appropriate PEO for full-scale implementation of the materiel solution development. The Sponsor works with the members of the Sponsor's team to develop a complete implementation plan, called the M-Implementation Plan that lays out the tasks, timelines and resource requirements to implement the materiel solution fully as defined by the selected COA and the detailed information and onboarding requirements generated in Step 3. The M-Implementation Plan is shown in **Figure 2.8**. All these requirements are packaged up into the bounded user requirements by the Sponsor, with assistance from the Architecture Team, and reviewed by the SMEs for agreement that this is the set of requirements that will deliver the materiel solution that solves the end user problems or satisfies the end user needs. After final review and approval of the bounded user requirement by the Sponsor and the SMEs, the Sponsor takes the bounded user requirement to the appropriate governance authority for review and approval. If needed to support resource allocation, the Sponsor takes the bounded user requirement to the AF Corporate Structure to ensure alignment with AF strategic objectives. Once the reviews are completed and approvals are forthcoming, the Sponsor moves to Step 4.

2.4.3.4. **Products**: The primary product of Step 3 is a bounded user requirement. The bounded user requirement consists of the SRM information, DRM information and the M- Implementation Plan. Each of these products is described below and depicted in an accompanying figure that contains the detailed content of each product. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02 documents.

2.4.3.4.1. **SRM Information**. The SRM information described in **Figure 2.6** is captured in Step 3 and contains the detailed requirements for the specific functions or services that the materiel solution must provide. The IT capability could consist of web services code, COTS/GOTS, traditional system implementation or any combination of these three, leveraging reusable components as much as feasible. The information should be sufficient to satisfy relevant compliance requirements as part of downstream governance activities. **Note:** The Sponsor and SME may wish to consult with IA SMEs during this Step to assure that IA requirements are designed into the materiel solution.

Figure 2.6. SRM Information (Parts 1-4)

SRM Information

The SRM Information captures a description of the functions and services that the materiel solution must deliver in order to solve the end user's problem and satisfy the end user's needs. The description of the functions and services within the materiel solution must be at a sufficient level of completeness, consistency and detail to prepare a bounded user requirement sufficient to select a satisfactory COTS product, web service, developed software code or combination of these, to deliver the materiel solution successfully.

Contextual Model: The Contextual Model bounds the materiel solution only to those specific mission processes within the BRM information that will be supported by the materiel solution. Other mission processes may be supported by other components of the DOTMLPF-P Implementation Plan. The Contextual Model adds context to each process step through more in-depth descriptions of the process step, how the user communicates, coordinates, utilizes and interacts with the information assets associated with each mission process, the flow of information between the mission processes in the Contextual Model and the business rules and access roles and permissions associated with each step of the process. Performance metrics and initial service descriptions for each mission process are also specified, derived from the performance measures from Step 1, and decomposed to align with each mission process step included in the Contextual Model.

Web Services Code Requirements: Description of the requirements to implement a web service or set of web services as part of the materiel solution.

- Information Exchange Requirements: Information exchange requirements are derived from the information flows (Step 2 Information Puts & Gets) in the Contextual Model. Information exchange requirements identify the information that flows between the materiel solution, as defined by the Contextual Model, and external sources and destinations of the information. The information exchange requirements also include exchanges between the processes within the materiel solution that are likely candidates for reuse by other materiel solutions. The inclusion of internal exchanges in the information exchange requirements ensures that those materiel solution components that can be reused are implemented in a manner that facilitates future reuse.
- Service Layering: Service Layering defines the individual services that will be implemented within the materiel solution. The individual services are derived from the mission processes included in the Contextual Model, identifying which activities within the mission processes will have automated support from the services and which functions those services need to perform in order to support the mission processes. Each service is linked to the information exchanges and/or the information assets that the service will consume or produce. The services can be decomposed into layers, showing the breakdown of a single service into multiple individual services or service operations that may be reusable on their own.

- Service Levels: Service Levels describe the technical performance parameters for each service, including the response times and availability, among other parameters. SLAs are derived from the Step 1 Performance Measures that are associated with the mission processes included in the Contextual Model.
- Reuse Components: Reuse Components include any existing web services that can supply all or portions of the services identified in the Service Layering, or information exchanges and information assets that are already defined and implemented through some other materiel solution that can meet the requirements for this particular materiel solution.
- Automated Information Assets: Information assets that are implemented electronically. The information assets are identified from the information exchange requirements to support interface implementation, as well as the Information Gets and Puts from the mission processes in the Contextual Model to identify information assets that will be managed in on-line repositories.

COTS/GOTS Requirements:

- Information Exchange Requirements: Information exchange requirements are derived from the information flows (Step 2 Information Puts & Gets) in the Contextual Model. Information exchange requirements identify the information that flows between the materiel solution, as defined by the Contextual Model, and external sources and destinations of the information. The information exchange requirements also include exchanges between the processes within the materiel solution that are likely candidates for reuse by other materiel solutions. The inclusion of internal exchanges in the information exchange requirements ensures that those materiel solution components that can be reused are implemented in a manner that facilitates future reuse.
- Functional Requirements: The Functional Requirements define the automated functions that will be implemented within the materiel solution. The automated functions are derived from the mission processes included in the Contextual Model, identifying which activities within the mission processes will have automated support from the COTS/GOTS solution and, specifically, which functions the COTS/GOTS solution needs to perform in order to support the mission processes. Each function is linked to the information exchanges and/or the information assets which the service will consume or produce. The functions can be decomposed into layers, showing the breakdown of a single function into multiple individual sub-functions that may be reusable on their own. The functional requirements serve as the basis for the blueprinting of the COTS solutions or tailoring of the GOTS solutions to meet the requirements of the materiel solution.
- Service Levels: Service Levels describe the technical performance parameters for each function, including the response times and availability, among other parameters. SLAs are derived from the Step 1 Performance Measures that are associated with the mission processes included in the Contextual Model.

SRM Information (Part 2)

- Reuse Components: Reuse Components include any existing COTS/GOTS components that can supply all or portions of the functional requirements, or information exchanges and information assets that are already defined and implemented through some other materiel solution that can meet the requirements for this particular materiel solution.
- Automated Information Assets: Information assets that are implemented electronically. The information assets are identified from the information exchange requirements to support interface implementation, as well as the Information Gets and Puts from the mission processes in the Contextual Model to identify information assets that will be managed in on-line repositories.

System Requirements:

- Information Exchange Requirements: Information Exchange Requirements are derived from the information flows (Step 2 Information Puts & Gets) in the Contextual Model. Information exchange requirements identify the information flows between the materiel solution, as defined by the Contextual Model, and external sources and destinations of the information. The information exchange requirements also include exchanges between the processes within the materiel solution that are likely candidates for reuse by other materiel solutions. The inclusion of internal exchanges in the information exchange requirements ensures that those materiel solution components that can be reused are implemented in a manner that facilitates future reuse.
- Functional Requirements: The Functional Requirements define the automated functions that will be implemented within the materiel solution. The automated functions are derived from the mission processes included in the Contextual Model, identifying which activities within the mission processes will have automated support from the system solution and, specifically, which functions the system solution needs to perform in order to support the mission processes. Each function is linked to the information exchanges and/or the information assets which the service will consume or produce. The functions can be decomposed into layers, showing the breakdown of a single function into multiple individual sub-functions that may be reusable on their own.
- Service Levels: Service Levels describe the technical performance parameters for each function, including the response times and availability, among other parameters. SLAs are derived from the Step 1 Performance Measures that are associated with the mission processes included in the Contextual Model.
- Reuse Components: Reuse Components include any existing system components that can supply all or portions of the functional requirements, or information exchanges and information assets that are already defined and implemented through some other materiel solution that can meet the functional requirements.

SRM Information (Part 3)

- Automated Information Assets: Information assets that are implemented electronically. The information assets are identified from the information exchange requirements to support interface implementation, as well as the Information Gets and Puts from the mission processes in the Contextual Model to identify information assets that will be managed in on-line repositories.

Compliance Requirements: The compliance requirements identify which certifications and accreditations are required for the materiel solution. The compliance requirements include those requirements that can be satisfied by inheriting certifications and accreditations from related components, such as inheritance from reuse components or inheritance from the platform environment.

Onboarding Requirements:

- Mission Critical Requirements: Identify which of the materiel solution components satisfy mission critical requirements. Mission critical components may require that the materiel solution meet specific requirements to deploy into and operate within the platform environment.
- Topology Requirements: Identify potential changes to the physical location of computers, network connections and core platform services, as well as changes to the capacity provided by the platform that will be required in order to deploy and operate the materiel solution.
- Additional Infrastructure Requirements: Description of any additional infrastructure capabilities or services that the platform environment requires in order to deploy and operate the materiel solution.
- Distributed Components Requirements: Description of any materiel solution requirements for components that are distributed to different locations to support warfighter needs or support performance requirements in order to meet the performance measurements, SLA or other mission critical service or function.
- Service Monitoring Requirements: Description of the levels of service monitoring required from the platform environment during the deployment and sustainment phases of the materiel solution.
- SLA: Description of the official Service Levels that the materiel solution will be able to meet once it is deployed, operated, and sustained within the platform environment.

Onboarding Compliance: Identification of any protocols, standards or other constraints, to which the materiel solution must adhere in order to be deployed, operated and sustained within the platform environment.

Note: This information may support the generation of the following Acquisition Documents: Acquisition Strategy, SEP, Program Protection Plan, and AoA Study Plan. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02.

2.4.3.4.2. **DRM Information**. The DRM information described in **Figure 2.7** is captured in Step 3 and contains the detailed information requirements for the materiel solution. The detailed information requirements include: the information that serves as input to the materiel solution; the information generated by the materiel solution; the sources for all that information and the access constraints for users desiring to utilize the information. The information should be sufficient to satisfy relevant compliance requirements as part of downstream governance activities.

Figure 2.7. DRM Information

DRM Information

DRM information provides an in-depth characterization of each information asset identified in the information exchange requirements in the SRM information.

COI Charter: A charter to establish a COI to generate the detailed information requirements for the materiel solution. The charter identifies the processes in the Contextual Model that the COI will support, the information assets that will serve as the starting point, stakeholders, deliverables, dependencies and a timeline for completion of the COI activity. More information on AF COIs is available at https://cs.eis.af.mil/afdbt/COI/default.aspx.

Vocabulary Package: The complete product of COI work that is made up of the Authoritative Data Source (ADS) mapping, roles and permissions, example data records and the ontology.

- Example Data Record: List of data elements that compose the information assets specified for detailing by the COI.
- Authoritative Data Source: The point at which information is first captured as data -- most current, reliable, highest-quality data that captures the information.
- ADS Mapping: List of the actual physical repositories of authoritative and source data that will deliver the data elements identified in the example data record.
- Roles and Permissions: Identification of who has access to each information asset and its authoritative and source data, and the criteria for assignment to access. Roles and permissions are defined for each information asset and its associated authoritative and source data to be exposed.
- Ontology: Semantic representation of the information assets, as well as the associated authoritative and source data to ensure understandability and discoverability of the information asset, associated authoritative and source data.

Reusable Artifacts: Products generated by previous COIs that can be reused by the COI for this materiel solution. A key component of the reuse is ensuring that COIs do not define duplicate or potentially conflicting ontologies for the same information assets or authoritative data. The reusable artifacts include ontologies that represent other problem domains and can reduce or eliminate work of a specific COI addressing the requirements for the materiel solution.

Note: This information may support the generation of the following Acquisition Documents: Acquisition Strategy, SEP, Program Protection Plan, Economic Analysis, ICD and Requirements Strategy. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02.

2.4.3.4.3. **M-Implementation Plan**. The M-Implementation Plan lays out the plan for the selected COA for implementing the materiel solution according to the requirements detailed in the SRM information and DRM information. The COA specifies how the requirements will be implemented from a technology basis, with components of the materiel solution delivered through web services, COTS/GOTS,

traditional system implementation or any combination of those three. The scoping of the individual activities in Step 3 through Step 6 to the specifics of the materiel solution is included in the M- Implementation Plan, which captures DOT-LPF-P activity dependencies to the materiel solution. Specifics of the materiel solution delivery are captured in the M-Implementation Plan, which serves as the basis for the acquisition strategy and the development of the detailed IMS in Step 4. The content of the M-Implementation Plan is shown in Figure 2.8.

2.4.3.5. **Alignment with Governance Processes.** SDDP work will generate information needed to support the documentation requirements of JCIDS, DoDI 5000.02 or other applicable governance processes. For example, at the end of Step 3, SDDP could support the development of documentation such as a Service Requirement Document (SRD), Information Support Plan (ISP), Analysis of Alternatives (AoA), Capability Development Document (CDD) or updated Problem Statement, or reviews such as the Preliminary Design Review (PDR) as required by the applicable process and MDA. Information captured at Step 3 should also support the Milestone A/B decision. It is the responsibility of the Project Lead to assure that the appropriate documentation, reviews and decision gates are included in the IMS.

Figure 2.8. M-Implementation Plan

M-Implementation Plan

Work Breakdown Structure / Requirements Traceability Matrix (WBS/RTM): The WBS/RTM identifies the tasks necessary to implement the materiel solution based on the selected COA, maintaining traceability to the original requirements defined in the Contextual Model. The WBS focuses on delivery of capability rather than a detailed technical implementation plan. The detailed technical implementation plan is the core of the IMS developed in Step 4. The M-Implementation Plan provides the basic framework for the IMS.

Cost Estimate: The M-Implementation Plan includes a detailed cost estimate, identifying the financial resource requirements to implement the components of the COA selected by the Sponsor and approved by the AF Corporate and governance structures.

DOT-LPF-P Change Management Plan: Includes all the DOT-LPF-P actions necessary to make the materiel solution operational and sustainable. Includes actions such as training to operate and maintain the materiel solution, assignment of new organizational responsibilities, development of new process-based policy documents to institutionalize the mission processes re-engineered in Step 2 and the means by which the materiel solution will be used to support those re-engineered processes.

Compliance Governance Package: Provides all the documentation to acquire the certifications and accreditations necessary for the Sponsor to obtain authorization to proceed to implement the materiel solution as required by the appropriate governance bodies. For example, DBS modernizations with a total cost of over $1M (NDAA 2010) going to the DBC for ultimate approval must submit assertions, certifications and accreditations including the following. **Note:** Other governance paths may require different assertions, certifications and accreditations.

- IT Dashboards
- Funding Profile
- Compliance Completion Plan
- Chief Management Officer (CMO) Determination Memo
- BPR Assertion
- Compliance Approvals

Onboarding Plan: Defines actions to be completed to bring the materiel solution onboard into the platform environment for operation and sustainment, including the following:

- Distributed Computing Requirements
- Monitoring Requirements
- SLAs
- Legacy System Requirements

Resourcing: Identifies the requisite organizational, personnel, facility and funding resources necessary to implement the materiel solution successfully.

Test Strategy: Sets the solution-level test requirements that will be captured in the test plan and decomposed into specific test procedures and parameters for the individual design components of the materiel solution.

Note: This information may support the generation of the following Acquisition Documents: Acquisition Strategy and Life Cycle Sustainment Plan. See Reference *SDDP Acquisition Alignment Document* for a mapping of SDDP to DoDI 5000.02.

2.4.4. **Step 4 – Plan and Implement Materiel Solution**

2.4.4.1. **Purpose of the Step**: The purpose of Step 4 is to implement the components of the materiel solution.

2.4.4.2. **Outcomes of the Step**. The expected outcomes of Step 4 are:

2.4.4.2.1. Formation of a team from across a wide range of skill sets to support the detailed planning and execution of the implementation of the materiel solution components.

2.4.4.2.2. Generation of a detailed, program-level schedule for (1) implementation, (2) assignment of responsibilities for implementation and (3) allocation of resources to implement the materiel solution successfully.

2.4.4.2.3. Implementation of the materiel solution components.

2.4.4.2.4. Preparation of materiel solution components for testing and certification. **Note:** appropriate tests (functional, integration, security, networthiness and others) should be determined by the ITT and included in the IMS.

2.4.4.3. **Description of the Step**. Step 4 consists of the following four major tasks:

2.4.4.3.1. **Generate Integrated Master Schedule.** In Step 4, the primary responsibility shifts from the Sponsor to the acquisition-selected Project Lead, who then works with the Sponsor to execute the M-Implementation Plan from Step 3. The Sponsor retains customer oversight of the materiel solution implementation through the IMS. The Project Lead obtains Points of Contact (POC) to serve as members of the Project Team (**Table 2.2**) responsible for executing the M-Implementation Plan. The Sponsor tasks the Project Lead to work with the POCs from each of the stakeholder groups to develop a detailed IMS (team may be tasked to assure that all required skill sets are represented on the Project Team). The IMS includes the detailed tasks, timelines and resource allocations from each of the stakeholder groups that must be completed to deliver the materiel solution and should capture necessary reviews, tests, and compliance and certification activities. IMS activities should be scoped as much as possible for the specific materiel solution to expedite development/delivery of the capability. The IMS is at a sufficient level of granularity to enable the Project Lead to manage the project according to AF program management standards and guidelines.

Table 2.2. Skill sets included on Project Team

Functional/SMEs
Sponsor
Project Lead
Architecture
System Engineering/Design
Acquisition Authority
Platform Engineering
Contracting
Finance

ITLC
Associated PEOs/Program Management Office (PMO)
Testing
Governance; for example, IA/FISMA Certification

2.4.4.3.2. **Approve Integrated Master Schedule.** After the IMS is completed and agreed upon by the members of the Project Team, the Project Lead takes the IMS to the Sponsor for review and approval. As required, the Sponsor takes the IMS to the PEO, Acquisition Decision Authority, and/or AF Corporate Structure for further review and approval. Once approved, the Project Lead initiates the execution of the IMS.

2.4.4.3.3. **Execute Integrated Master Schedule.** The Project team executes the IMS to implement the components of the materiel solution. Only the portion of the IMS relevant to the actual development of the materiel solution components is completed at this point in the SDDP. The portions of the IMS associated with testing, deployment and sustainment of the materiel solution are completed in Steps 5 and 6 of the SDDP, but there may be activities in Step 4 to assure that the materiel solution being developed is integratable, networthy and deployable. Each POC in the Project Team ensures that their respective teams complete their assignments in the IMS in order to deliver the components of the materiel solution on time and within budget.

2.4.4.3.4. **Deliver Deployable Components of the Materiel Solution.** Upon the completion of the development portion of the IMS, the Project Lead and the Project Team deliver the components of the materiel solution to the ITLC for testing and preparation for deployment.

2.4.4.4. **Products**. The primary products of Step 4 are the developed components of the materiel solution that are ready for integration and testing. These will include the test plans and procedures, development test and evaluation results, the DOTMLPF-P Change Management Plan, contractual products and other products developed by the team members in order to accomplish their IMS tasks.

2.4.4.5. **Alignment with Governance Processes.** SDDP work will generate information needed to support the documentation requirements of JCIDS, DoDI 5000.02 or other applicable governance processes. For example, at the end of Step 4, SDDP could support the development of documentation to support mandatory design (i.e. Critical Design Review (CDR)) or test readiness reviews or other requirements of the applicable process and MDA (i.e. Milestone (MS) C, etc). It is the responsibility of the Project Lead to assure that the appropriate documentation, reviews and decision gates are included in the IMS.

2.4.5. **Step 5 – Integration, Test and Application Lifecycle Management**

2.4.5.1. **Purpose of the Step**. The purpose of Step 5 is to prepare the components of the materiel solution for deployment into the platform environment. The Project Lead assures the Step 5 activities are completed as captured in the IMS.

2.4.5.2. **Outcomes of the Step**. The expected outcomes of Step 5 are:

2.4.5.2.1. Successfully tested components of the materiel solution that demonstrate networthiness, functionality and satisfy the performance measures from Step 1.

2.4.5.2.2. Platform environment prepared to accept and manage the components of the materiel solution throughout the lifecycle of the materiel solution, including sustainment functions such as monitoring and Help Desk support.

2.4.5.3. **Description of the Step.** Step 5 integrates the components of the materiel solution developed in Step 4 with the platform environment for full-scale testing and certification. Step 5 consists of seven major tasks:

2.4.5.3.1. **Develop Initial Build and Deployment Packages.** The ITLC commences Step 5 by tasking resources both within the ITLC and outside the ITLC to prepare for testing and certification.

2.4.5.3.1.1. The ITLC starts development of Help Desk documentation for the materiel solution, while System Engineering generates compliance packages for C&A, instructions for monitoring the materiel solution and the required configurations of the Integration/Test Environment necessary to test the materiel solution. System Engineering also generates the instructions and procedures for provisioning the security services of the platform environment with the roles, permissions and credentials for the end users to obtain access to the materiel solution. The ITT updates the test plans and procedures to support the integration of the materiel solution and the independent testing of those components once integrated into the Platform Environment. Network Operations develops training materials for the operators in how to monitor and measure the performance of the materiel solution.

2.4.5.3.1.2. The ITLC completes the preparation of the Help Desk by collaborating with the Sponsor SMEs for Tier 3 support and with Network Operations for Tier 1 support, with the ITLC providing the content for Tier 2. System Engineering conducts an engineering review of the Help Desk content to ensure that Tiers 1, 2 and 3 will integrate sufficiently to address all likely user problems and issues. In addition, System Engineering conducts a similar review of the training material produced by Network Operations to verify the operators are monitoring all the appropriate materiel solution components in a manner that ensure availability of the materiel solution to the end users. Finally, Platform Engineering provisions the integration/test environment to support testing of the materiel solution, functioning of the Help Desk, and operations of the monitoring functions in support of the Network Operators.

2.4.5.3.1.3. With the provisioned integration/test environment, the ITLC, in conjunction with the ITT, tests the build of the materiel solution and finalizes the Build Packages. Any errors that occur during the build of the materiel solution are then fixed through adaptation of the Build Package and documented further in the Deployment Package. The Build Package describes how to install and connect the components of the materiel solution such that the materiel solution will operate correctly. The Build Package includes source code, compilation instructions, development and test environment descriptions necessary to support the build, integration/test environment characteristics required to complete the build, test

data, as well as reference documentation for testing, deficiencies and prioritization of deficiency reports. The Deployment Package describes how, where and when to deploy the materiel solution across the platform environment using the Build Package. The Deployment Package includes the Platform Service Order, readiness, standards, user evaluation, functional and performance assertion, networthiness assertion and other compliance assertions.

2.4.5.3.2. **Perform Integration of Materiel Solution: Services, COTS, and Systems**. The Project Lead, leveraging the ITLC skill sets, commences the integration of the materiel solution components (Services, COTS/GOTS and Systems). As directed by the Project Lead, System Engineering performs the actual integration with support from the ITLC, connecting the components of the materiel solution with the appropriate infrastructure services within the platform environment as well as with all required external interfaces. Testing conducts a static analysis and tabletop review of the testing procedures, to ensure that all components are installed, integrated and linked to monitoring and operations support capabilities. Test support personnel will participate in the analysis to ensure they are familiar with the components and the planned test activities, and are prepared to conduct the testing.

2.4.5.3.3. **Conduct User Evaluation.** Once the materiel solution is installed and integrated, a formal limited user evaluation is conducted. This evaluation is intended to determine if the materiel solution meets the end user needs prior to extensive expenditure of resources on testing and deployment of the materiel solution. The rationale behind this testing is that the AF does not want to spend the resources to test and deploy a materiel solution that does not improve the mission operations of the end users. The Project Lead works with the ITLC and the Sponsor to identify a set of SMEs to serve as the end users for this testing, with the ITLC and ITT providing technical support as needed during the testing. Once the user testing is completed, the Sponsor reviews the results with the ITLC and the Project Lead to determine what action is required. The Sponsor, in coordination with the PEO, may choose to have the ITLC make simple fixes to the materiel solution. More significant fixes may need to go back to the Development Team. Alternatively, the Sponsor may decide that major changes require a return to earlier Steps in the SDDP. If the Sponsor determines that the materiel solution cannot meet its objectives, the Sponsor may decide to terminate the initiative. Once changes are implemented and the Sponsor is satisfied with the results of the user testing, the materiel solution moves to the Independent Testing.

2.4.5.3.4. **Conduct Independent Testing.** In accordance with current Air Force policy and guidance, the Project Lead oversees independent testing, which is full testing of the materiel solution in the platform environment, including all operational support. The Lead Developmental Test and Evaluation Organization (LDTO) and Participating Test Organization (PTO) conduct the independent testing and generate test results for analysis. LDTO is responsible for distributing test results to the PM, PEO, and other stakeholder in support of decisions reviews. System Engineering works with the Project Lead to assess the test results and determines what action, if any, is required to fix any discrepancies in the performance of the materiel solution. Again, if the fixes are minor, the ITLC could undertake the implementation of those

fixes at the direction of the Project Lead. If the fixes are major, the Project Lead works with System Engineering to determine the impacts of implementing the fixes, with a particular focus on the cost and schedule impacts of those fixes. The Project Lead and System Engineer then review the proposed fixes and their impacts with the Sponsor, who will decide how to proceed with the fixes. The Sponsor will determine the point in the SDDP to which the materiel solution must return in order to implement the fixes. In the most extreme cases, the Sponsor may decide to terminate the initiative. Once the fixes are implemented, the materiel solution is retested to verify the fixes resolved the problems and the deficiencies can be closed. Then the materiel solution moves to the next activity.

2.4.5.3.5. **Networthiness Review.** The results of the test and integration activities are captured for the Project Lead, who generates the compliance and certification packages for the materiel solution, with assistance from Platform Engineering to ensure the materiel solution complies with the Platform Infrastructure standards and procedures prior to connection to a DoD network. The compliance and certification packages are then submitted to the appropriate governance bodies for review and approval. The PEO, Project Lead, ITLC and Platform Engineering work with the governance bodies to modify and adapt the compliance and certification packages until the governance bodies sign off the packages with their approval.

2.4.5.3.6. **Deployment Readiness.** After signoff on the compliance and certification packages, the Sponsor does a final readiness check on the materiel solution for deployment. If there are fixes needed to the Deployment Package, the Project Lead will direct necessary changes be made to the materiel solution, leveraging the ITLC as needed. These fixes are not changes to the materiel solution, but rather changes to the procedures, directions and possible resource assignments associated with the deployment. The Sponsor also checks to ensure the DOT-LPF-P actions necessary to support the materiel solution, such as training or policy updates, have also been completed as appropriate. If the Sponsor chooses, the deployment may be postponed until those DOT-LPF-P actions have been completed. Upon successful Deployment Readiness review, deployment of the materiel solution can commence.

2.4.5.3.7. **Deployment Initiation.** Deployment commences with the issuance of the Platform Service Order. System Engineering produces the Platform Service Order to give instructions and directions to Platform Engineering and Network Operations to deploy the materiel solution. Architecture updates the architectural artifacts for the materiel solution to ensure those artifacts accurately reflect the actual, deployed materiel solution. The Platform Service Order is then delivered for execution, and the materiel solution moves into Step 6.

2.4.5.4. **Products**. The primary products of Step 5 are the integrated components of the materiel solution, captured in the Build Package, and the Deployment Package that includes the instructions and material within the Platform Service Order that informs the Platform Engineers how to deploy the materiel solution and when specific activities within the deployment need to be complete.

2.4.5.5. **Alignment with Governance Processes.** SDDP work will generate information needed to support the documentation requirements of JCIDS, DoDI 5000.02 or other

applicable governance processes. For example, at the end of Step 5, SDDP could support the development of documentation to support mandatory reviews or other decisions as required by the applicable process and MDA (i.e. full deployment decision (FDD)). Information captured at Step 5 should also support an MS C decision to approve initiation of deployment processes. It is the responsibility of the Project Lead to assure that the appropriate documentation, reviews and decision gates are included in the IMS.

2.4.6. **Step 6 - Deploy and Operate Materiel Solution and Measure the Success of the Capability Delivery**.

2.4.6.1. **Purpose of the Step**: The purpose of Step 6 is to deploy the materiel solution, deliver capabilities that solve the user's problem and satisfy the user's needs, support the operation and sustainment of the materiel solution and measure success.

2.4.6.2. **Outcome of the Step**. The expected outcomes of Step 6 are:

2.4.6.2.1. Fully operational materiel solution that meets the user's needs and achieves the performance measures identified in Step 1.

2.4.6.2.2. Platform environment prepared to operate and sustain the materiel solution for the duration of the useful life of the materiel solution, and to retire it when directed by the Sponsor.

2.4.6.3. **Description of the Step**: In Step 6, a target set of users from the broader community of AF users (different from those users involved in the design of the capability) are given their first look at the fully functional materiel solution, which essentially serves as the success prototyping required by DAS and NDAA 2010. This limited deployment allows the Sponsor and Project Lead to evaluate the successful performance of capability in terms of functionality, performance levels and service levels. Positive assessment of the materiel solution and verification that change management was adequate leads to full-scale deployment to the entire targeted user community, and Step 6 closes the SDDP with an assessment of how well the DOTMLPF-P implementation, including the materiel solution, meets the users' needs or solves the users' problem. Step 6 consists of four major tasks:

2.4.6.3.1. **Initiate Deployment Activities for Limited Deployment.** The ITLC commences the deployment activities by updating their tasks within the IMS and allocating sufficient resources to conduct the final testing and deployment. The Project Lead works with the Sponsor, ITLC and ITT to recruit the users who will act as SMEs for the limited deployment testing. In parallel, the Project Lead, in partnership with the Sponsor, acquires the Authorization to Test (ATT) while the ITLC trains Help Desk personnel who will support the limited deployment testing. Platform Engineering defines for Network Operations the changes needed to provision the Operational Environment with the IT resources necessary to support the materiel solution and then installs the materiel solution across the Operational Environment to support the limited deployment testing. The Sponsor completes the test preparation by training the end users on the materiel solution, and Network Operations provisions the Operational Environment to provide access to the limited deployment to the selected and trained users. Network Operations/Platform Engineering conducts a final assessment of the limited deployment. Based on this

final check, the Sponsor makes a decision to proceed to the limited deployment testing or, if additional work is required to prepare for testing, the Sponsor may choose to have some of the activities in this Step repeated. In the final assessment Network Operations/Platform Engineering checks that:

2.4.6.3.1.1. All components of the materiel solution are properly installed and operating.

2.4.6.3.1.2. End users are adequately trained.

2.4.6.3.1.3. Help desk is operational.

2.4.6.3.1.4. Platform environment is prepared to support the testing.

2.4.6.3.2. **Perform User Evaluation of Limited Deployment.** The User Evaluation of the limited deployment is a full-scale test of the complete materiel solution by a limited subset of the user community in live operations. The user community, selected in the previous activity, provides a sufficient breadth of experience to test all aspects of the materiel solution. The test is conducted in the Operational Environment with live data during the actual mission operations, defined in Step 2, which the materiel solution is intended to support. This activity begins with two parallel testing threads. The Testing Community conducts standard Operational Test and Evaluation (OT&E) to ensure the limited deployment materiel solution functions as it was intended to do within the Operational Environment. The Independent Testers also ensure that the materiel solution meets the DoD and AF mandated performance measures. Simultaneously, the selected end users use the materiel solution during their mission operations to assess how well the materiel solution meets their needs and solves their problems. The Sponsor observes the User Evaluation and may, in some cases, actually participate to obtain first-hand knowledge of the performance of the materiel solution in meeting its objectives. The Sponsor assesses the results of the Independent Test and User Evaluation to determine if the materiel solution should be deployed across the Operational Environment. The Sponsor, in consultation with the project team, assesses whether the DOT-LPF-P capabilities necessary to support the materiel solution are sufficient, or whether additional effort is needed. The Sponsor takes these factors into account in determining whether to deploy the materiel solution. If additional work is required, the Sponsor determines where in the SDDP to return the materiel solution for rework. If the Sponsor decides the test results meet the requirements and support a deployment decision, the ITLC completes any final Help Desk training, and the Product Lead, in partnership with the Sponsor, obtains the Authorization to Operate (ATO).

2.4.6.3.3. **Conduct Phased User Deployment of Materiel Solution.** The actual deployment of the materiel solution to the entire targeted user community is accomplished in phases, with different subsets of the user community trained and brought on-line with the materiel solution in sequence. The Sponsor trains each set of users in each phase, Platform Engineering provisions the Operational Environment to support each group of users in each phase, and Network Operations provisions the Operational Environment and the materiel solution to provide access to each group of users in each phase. Once access is granted, each group of users commences utilizing the materiel solution during mission operations. Once all phases are complete, the

Sponsor updates the IMS to show completion of the implementation of the materiel solution.

2.4.6.3.4. **Conduct Post Implementation Review (PIR).** After a 6-12 months period of use of the materiel solution by the targeted user community, the Sponsor conducts a review to determine the success of the DOTMLPF-P solution and the materiel solution associated with the DOTMLPF-P Implementation Plan. The PIR addresses the overall performance in the areas of user satisfaction, business process improvements, cost improvements, technical evaluation and other factors as specified by the Sponsor. This performance is compared with the intended results of the DOTMLPF-P Implementation Plan developed in Step 2 to achieve the mission performance measures defined in Step 1. The Sponsor assesses the impact of each component of the DOTMLPF-P Implementation Plan and determines whether it meets its objectives. The Sponsor may determine that additional actions are required, including commencing a new SDDP to solve new problems or improve certain aspects of the DOTMLPF-P implementation. If the Sponsor is satisfied with the DOTMLPF-P implementation, the SDDP terminates and future assessments occur at the determination of the Sponsor.

2.4.6.3.5. Alignment with Governance Processes. SDDP work will generate information needed to support the documentation requirements of JCIDS, DoDI 5000.02 or other applicable governance processes. For example, during Step 6, SDDP could support the declaration of Initial Operational Capability (IOC) or Full Operational Capability (FOC), as required by the applicable process and MDA. It is the responsibility of the Project Lead to assure that the appropriate documentation, reviews and decision gates are included in the IMS.

MICHAEL J. BASLA, Lt General, USAF
Chief, Information Dominance and
Chief Information Officer

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

NDAA 2005, *Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*

NDAA 2010, *National Defense Authorization Act for Fiscal Year 2010*

NDAA 2012, *National Defense Authorization Act for Fiscal Year 2012*

NDAA 2014, *National Defense Authorization Act for Fiscal Year 2014*

Subtitle III of Title 40 of the Clinger-Cohen Act of 1996, 10 February 1996

10 USC 2222, *Defense Business Systems: architecture, accountability and modernization,* 7 Jan 2011

44 USC 3542(b) (2), *Coordination of Federal Information Policy,* 7 Jan 2011

Federal Enterprise Architecture

OMB Circular A-11, Section 53, *Information Technology and E-Government,* 26 Jun 2008

DoDD 4630.05, *Interoperability and Supportability of Information Technology (IT) and*

National Security Systems (NSS), 5 May 2004, Certified current as of 23 Apr, 2007

DoDD 5000.01, *The Defense Acquisition System,* 12 May 2003, Certified current as of 20 Nov 2007

DoDI 5000.02, *Operation of the Defense Acquisition System,* 25 Nov 2013

DoDI 5010.43, *Implementation and Management of the DoD-Wide Continuous Process Improvement/Lean Six Sigma (CPI/LSS) Program,* 17 Jul 2009

DoD Guidance for the Implementation of Section 1072, Business Process Reengineering, 30 Apr 2011

JCIDS Manual, 19 Jan 2012

JP 1-02, *DoD Dictionary of Military and Associated Terms,* 15 Nov 2011

AFPD 10-6, *Capability Requirements Development,* 6 Nov 2013

AFPD 33-4, *Information Technology Governance,* 17 Jan 2013

AFI 10-601, *Operational Capability Requirements Development,* 6 Nov 2013

AFI 16-501, *Control and Documentation of Air Force Programs,* 15 Aug 2006

AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review,* 23 Dec 2008

AFI 33-210, *Air Force Certification and Accreditation Program,* 23 Dec 2008

AFI 33-401, *Air Force Architecting,* 17 May 2011

AFI 63-101/20-101, *Integrated Life Cycle Management,* 7 Mar 2013

AFI 99-103, *Capabilities-Based Test and Evaluation,* 16 Oct 2013

AFMAN 33-363, *Management of Records*, 01 Mar 2008

Air Force Enterprise Architecture Framework

Air Force Communities of Interest Panel Charter

Air Force Enterprise Senior Working Group Charter

Air Force Requirements Oversight Council Charter

ISO/IEC/IEEE 42010, *Recommended Practice for Architectural Description of Software-Intensive Systems*, 7 Dec 2011

ISACA, October 15, 2004, IS Auditing Guidelines Post-Implementation Review

Prescribed Forms

No prescribed forms are implemented by this publication.

Adopted Forms

AF 847, *Recommendation for Change of Publication*, 22 Sep 2009

Abbreviations and Acronyms

ADS—Authoritative Data Source

AF—Air Force

AFB—Air Force Board

AFC—Air Force Council

AFG—Air Force Group

AF EA—Air Force Enterprise Architecture

AFIT—Air Force Institute of Technology

AFLCMC—Air Force Life Cycle Materiel Center

AFMC—Air Force Materiel Command

AFOTEC—Air Force Operational Test and Evaluation Center

AFROC—AF Requirements Oversight Council

AFSO21—Air Force Smart Operations for the 21st Century

AF/CV—Air Force Vice Chief of Staff

AoA—Analysis of Alternatives

APB—Acquisition Program Baseline

ATO—Authorization to Operate

ATT—Authorization to Test

AT&L—Acquisition, Technology and Logistics

BEA—Business Enterprise Architecture

BMA—Business Mission Area

BO—Business Outcome

BPR—Business Process Re-engineering

BRM—Business Reference Model

C&A—Certification and Accreditation

CCA—Clinger-Cohen Act

CCB—Configuration Control Board

CDD—Capability Development Document

CDR—Critical Design Review

CEIB—Consolidated Engineering IT Baseline

CFLI—Core Function Lead Integrator

CM—Configuration Management

CMO—Chief Management Officer

COA—Course of Action

COI—Community of Interest

COTS—Commercial Off-the-Shelf

CPD—Capability Production Document

CPI/LSS—Continuous Process Improvement/Lean Six Sigma

DAA—Designated Accrediting Authority

DAU—Defense Acquisition University

DBC—Defense Business Council

DBS—Defense Business Systems

DCMO—Deputy Chief Management Officer

DCR—DOTMLPF-P Change Recommendation

DISA—Defense Information Systems Agency

DISR—Defense Information Technology Standards and Profile Registry

DoD—Department of Defense

DOT&E—Director, Operational Test and Evaluation

DOTMLPF-P—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy

DOT-LPF-P—Doctrine, Organization, Training, Leadership and Education, Personnel, Facilities, and Policy

DRM—Data Reference Model

DT&E—Development Test and Evaluation

EA—Enterprise Architecture

EDR—Example Data Record

ESWG—Enterprise Senior Working Group

FAR—Federal Acquisition Regulation

FDD—Full Deployment Decision

FEA—Federal Enterprise Architecture

FISMA—Federal Information Security Management Act

FOA—Field Operating Agency

FOC—Final Operational Capability

FYDP—Future Years Defense Program

GAO—Government Accountability Office

GOTS—Government Off-the-Shelf

HAF—Headquarters Air Force

HIPAA—Health Insurance Portability and Accountability Act

HLO—High Level Outcome

IB—Implementation Baseline

ICD—Initial Capabilities Document

IMS—Integrated Master Schedule

IOC—Initial Operational Capability

IRB—Investment Review Board

ISACA—Information Systems Audit and Control Association

IT—Information Technology

ITLC—Information Technology Lifecycle Capability

iTRM—Infostructure Technology Reference Model

ITT—Integrated Test Team

JCIDS—Joint Capabilities Integration and Development System

JROC—Joint Requirements Oversight Council

LDTO—Lead Developmental Test and Evaluation Organization

LRP—Legal, Regulatory and Policy

MAJCOM—Major Command (USAF)

MAIS—Major Automated Information System

MDA—Milestone Decision Authority

MDAP—Major Defense Acquisition Program

MDD—Materiel Development Decision

MOE—Measure of Effectiveness

MOP—Measure of Performance

MS—Milestone

NDAA—National Defense Authorization Act

NETOPS—Network Operations

NSS—National Security System

OASIS—Organization for the Advancement of Structured Information Standards

OB—Operational Baseline

OMB—Office of Management and Budget

OT&E—Operational Test and Evaluation

OPR—Office of Primary Responsibility

PEO—Program Executive Officer

PIA—Privacy Impact Assessment

PII—Personally Identifiable Information

PIR—Post Implementation Review

PM—Program Manager

PMO—Program Management Office

POC—Point of Contact

POM—Program Objective Memorandum

PTO—Participating Test Organization

PRM—Performance Reference Model

RACI—Responsible, Accountable, Consulted or Informed

RDT&E—Research, Development, Test and Evaluation

REST—Representational State Transfer

RIE—Rapid Improvement Event

ROI—Return on Investment

ROM—Rough Order of Magnitude

RTM—Requirements Traceability Matrix

SAF—Secretary of the Air Force

SDDP—Service Development and Delivery Process

SDF—Standard Deployment Folder

SEP—Systems Engineering Plan

SLA—Service Level Agreement

SMART—Specific, Measureable, Actionable, Relevant and Timely

SME—Subject Matter Expert

SRM—Service Reference Model

TB—Target Baseline

TCO—Total Cost of Ownership

TEMP—Test and Evaluation Master Plan

TRM—Technical Reference Model

T&E—Test and Evaluation

UDM—Unit Deployment Manager

UI—User Interface

URL—Uniform Resource Locator

USAF—United States Air Force

WBS—Work Breakdown Structure

WIP—Work in Progress

W3C—World Wide Web Consortium

Terms

Accreditation—Certification of a capability to be compliant with technical, security and interoperability standards is assured.

Air Force Corporate Structure—Embodies the corporate review process for HQ USAF. It does not replace the functional staff but, rather, enhances it by allowing time critical or time limited functional reviews at the appropriate levels. The deliberative components of the Corporate Structure are the AFC, the AFB, the AFG and the thirteen Mission and Mission Support Panels. This structure increases management effectiveness and improves cross-functional decision-making by providing a forum in which senior AF Leadership can apply their collective judgment, experience and analysis to major programs, objectives and issues. This process balances programs among mission areas, between force structure and support, and between readiness, modernization and transformation. Additionally, this approach ensures the AF program is capabilities-based and supports the Joint warfighter. Only military or DoD civilian personnel assigned to the Air Staff or Office of the Secretary of the Air Force may serve as members of the corporate structure.

Air Force Enterprise—All MAJCOMs, HQ USAF offices, agencies, installations, forces, and all operational mission and support activities that those organizations perform; represents the Air Force as a corporate entity and reflects the way the Air Force accomplishes its missions.

Air Force Enterprise Architecture (AF EA)—An architecture that describes the Air Force Enterprise. The AF EA includes internal Air Force elements and processes and their relationships. The AF EA also defines external relationships between the Air Force Enterprise and external enterprises (such as DoD, US Navy, etc.) (AFPD 33-4)

Architecture—A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. (JP 1-02, *DoD Dictionary of Military and Associated Terms*). The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. (*ISO/IEC/IEEE 42010)* It is the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. (*Federal Enterprise Architecture)*

Auditable Mission Process Model—An in-depth description of a mission process from beginning to end. Each process is decomposed into its constituent activities or tasks, sometimes down to two or three levels of decomposition. The start event(s) that trigger the beginning of a process and the inputs provided at the start of the process are defined. The process Steps are the actual activities performed by an AF resource that occur between the beginning trigger and the end output. The Steps that trigger the end of the process and the work product (output) are clearly defined. Descriptive actions that take place at each Step, along with an explanation why each Step in the process is necessary, are included.

Authoritative Data Source (ADS)—The point at which information is first captured as data. The most current, reliable, highest-quality data that captures the information.

Authoritative Data Source (ADS) Mapping—A list of the actual physical repositories containing the ADS and source data that deliver the data elements identified in the EDR.

Automated Information Asset—An electronically implemented information asset.

Business Case Analysis—Assessment, analysis and recommendation regarding the reasoning for and viability (financially, technically, practically) of pursuing a specific project or business opportunity. The logic of the business case is that, whenever resources such as money or effort are consumed, they should be in support of a specific business need (e.g., improved customer satisfaction, reduced task time or reduced maintenance costs). A compelling business case adequately captures both the quantifiable and unquantifiable characteristics of a proposed project.

Business Enterprise Architecture (BEA)—The enterprise architecture for the DoD that reflects the DoD business transformation priorities.

Business Process Re-engineering (BPR)— The fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical contemporary measures of performance, such as cost, quality, service, and speed. (DoDI 5010.43)

Business Process Re-engineering (BPR) Assertion—The documentation, presentation and AF Senior Leader validation of BPR, as required by the Clinger- Cohen Act and, in the case of Defense Business System modernization with total cost of over $1M, by NDAA 2010. The BPR

Assertion is needed to implement an IT-enabled materiel solution beginning in Step 3 of the SDDP. BRM information and the DOTMLPF-P Implementation Plan, generated in Step 2, are used to assert BPR sufficiency.

Business Reference Model (BRM)—A function-driven framework used to describe the lines of business and sub-functions performed by the federal government independent of the agencies that perform them. IT investments are mapped to the BRM to identify collaboration opportunities. (OMB Circular A-11, Section 53)

Business Rule—A definition of how a task identified in the Auditable Mission Process Model is completed. Business rules can also define the constraints for a task, articulating how a task is completed in terms of performance, such as the time in which the task must be completed, the scope of the information produced or consumed during the task.

Capability—The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways across the full spectrum of DOTMLPF-P to perform a set of tasks to execute a specified COA. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a DOTMLPF-P change recommendation.

Capability Need—A capability identified through a capabilities-based assessment required to be able to perform a task within specified conditions to a required level of performance.

Certification—A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process.

Certification and Accreditation (C&A)—A process for implementing information security. It is a systematic procedure for evaluating, describing, testing and authorizing systems prior to or after a system is in operation.

Clinger- Cohen Act (CCA)—This statute is the principal federal law on information technology (IT). Originally enacted as the Information Technology Management Reform Act, Division E of Public Law 104-106, the law's primary purpose is to provide a framework for the role of the CIO in federal agencies and how the CIO should be involved in IT investments or IT acquisitions that support an agency's mission.

Community of Interest (COI) Charter—A project charter to establish a COI to generate detailed information requirements for the materiel solution.

Compliance Completion Plan—A plan that sets out how the compliance requirements for the materiel solution will be satisfied, either through assertion, review or test.

Compliance Requirement—An identification of the certifications and accreditations required for the materiel solution.

Constraint—An external restriction or mandate that must be considered when defining and developing a solution.

Contextual Model—A description of the specific mission processes within the BRM that will be supported by the materiel solution. Context is added to each process Step through more in-depth descriptions of the process Steps, end user design concept, the flow of information between the mission processes and the business rules and access roles/permissions associated with each Step

of the process. Initial service descriptions for each mission process are specified as derived from the Step 1 performance measures and decomposed to align with each mission process Step.

Contracting—The skill set needed to capture a specific requirement or deliverable into a contract assigned to a specific vendor for delivery. The authority to enter into contracts on behalf of the Government is restricted to a Contracting Officer with an appropriate warrant.

Cost Estimate—Cost estimates, as captured in the AFMAN, are initially very rough, high- level estimates of resources needed to delivery described capability. Over the course of the SDDP process those cost estimates are informed and become more and more precise.

Course of Action—A planning and decision process that culminates in a sponsor decision. It principally refers to the decision whether to proceed with development of one or more prospective materiel solutions.

Critical Design Review (CDR)—A multi-disciplined technical review to ensure that a system can proceed into fabrication, demonstration, and test and can meet stated performance requirements within cost, schedule, risk, and other system constraints.

Data Validation—The process of ensuring that a capability has correct and useful data required by the information flows supporting the processes enabled by the capability.

Data Reference Model (DRM)—A framework used to promote the common identification, use and appropriate sharing of data/information across the federal government. It provides standards and guidelines to help agencies structure, categorize, exchange and manage their data to improve the ability of government to perform cross- agency information sharing. (OMB Circular A-11, Section 53)

Defense Business System—An information system, other than a national security system, operated by, for or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (NDAA 2005 and NDAA 2012)

Distributed Computing Requirement—A description of the materiel solution's requirement to have components distributed to different locations to support warfighter needs, performance requirements, service level agreements or other mission critical service or function.

Defense Information Technology Standards and Profile Registry (DISR)—Online repository of IT standards formerly captured in the Joint Technical Architecture.

DOT-LPF-P Change Management Plan—A description of all DOT-LPF-P actions necessary to make the materiel solution (the M within DOTMLPF-P) operational and sustainable.

DOTMLPF-P Capability—A specific action or portion of a DOTMLPF-P solution that, when completed or deployed, has standalone value to the warfighter. A collection of DOTMLPF-P capabilities, within the context of the SDDP, will solve the end user's problem or satisfy the end user's need.

Enterprise Architect—A person responsible for developing the enterprise architecture and often called upon to draw conclusions from it. By producing enterprise architecture, architects provide

a tool for identifying opportunities to improve the enterprise, in a manner that more effectively and efficiently pursues its purpose.

Enterprise Architecture (EA)—A management practice for aligning resources to improve business performance and help agencies better execute their core missions. An EA describes the current and future state of the agency and lays out a plan for transitioning from the current state to the desired future state. (FEA Practice Guidance dated Nov 2007, **http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_Practice_Guidance_Nov_2007.pdf)**

EA Analysis—An activity whereby the EA is referenced to inform a decision. An EA analysis can identify opportunities for reuse, inform legal, regulatory and policy constraints, identify dependent or tangential process and help to capture impacts to those processes caused by changes to a specific process.

Enterprise- Level Dependency—An association among mission processes that (1) describe the interdependence between process Steps, (2) are based on information, materials or other resources, and (3) describe the influence of time events on the execution of processes.

Example Data Record (EDR)—A list of the data elements that compose the information assets specified for detailing by the COI.

Federal Enterprise Architecture (FEA)—Enterprise architecture of the federal government that provides a methodology for IT acquisition, use and disposal. FEA includes in its reference models the PRM, BRM, SRM, TRM and DRM.

Finance—The skill set needed to assure that funding is available to support the implementation of a materiel solution. The Finance Team will assist with characterization of funding profile (what type of money is needed when), as well as verify that the business case supporting a materiel solution is adequate to justify the expenditure of resources.

Functional Organization—A domain focused on a specific type of mission activity or process (i.e., Logistics or Acquisition). Typically represented by a Headquarters Air Force office (AF/A4 or SAF/AQ).

Functional Requirements—A definition of the automated processes that will be implemented within the materiel solution.

Funding Profile—A description of what type of funding (i.e., procurement, research and development, operations and maintenance) is needed when (year and quarter) in order to satisfy the implementation requirements for the materiel solution.

Governance—The management activity of overseeing a capability implementation to assure that the capability delivered meets legal, regulatory and policy compliance criteria, that the delivery of the capability makes sense in terms of return against the requested investment funding, and that the implementation plan is sufficient to deliver the capability within the time-to-need specified by the user.

Governance Package—The documentation required for the certifications and accreditations necessary for the Sponsor to obtain authorization to spend funds on implementing the materiel solution as required by the appropriate governance bodies.

Information Asset—The information that is consumed during a task within the Auditable Mission Process Model, as well as the information that is produced during the completion of the task. An information asset is a definable piece of information, stored in any manner, which is recognized as valuable to an organization.

Information Exchange Requirement—An identification of the information that flows between the materiel solution, as defined by the Contextual Model, and the external sources and destinations of the information. The information exchange requirements also include internal exchanges between the processes within the materiel solution that are likely candidates for reuse by other materiel solutions.

Information Flow—A description of the manner in which information assets move from one step to another in a process. An information flow begins with a description of who supplies the information and concludes with a description of the end product and identification of the consumer.

Information Get—A description of the information needed to support a specific step or task in a mission process. For example, training status information would be an Information Get needed to determine whether an Airman needs training. The contents of the information (course information, date completed, etc.) are captured in the Information Asset that describes the Information Get.

Information Put—A description of the information generated as a result of a specific Step or task in a mission process, which is passed along the process to support other down- stream steps/tasks. For example, an Information Put may be a report of an Airman's training status. The contents of the information (training requirements, dates on which requirements were met and how, etc.) are captured in the Information Asset that describes the Information Put.

Information Technology Lifecycle Capability (ITLC)—The set of capabilities needed to provide 1) development and test environments to support the delivery of capability within the SDDP, 2) enterprise-level Help Desk, and 3) enterprise-level system engineering and software sustainment support.

Infrastructure Requirement—A description of capabilities or services that the platform environment requires in order to deploy and operate the materiel solution.

Integrated Master Schedule (IMS)—The schedule of all activities, across all skill sets, needed to implement a materiel solution. A baselined schedule is used to assess progress against the planned delivery of capability.

Integrated Test Team (ITT)—A cross-functional team of representatives from multiple disciplines and organizations responsible for developing the test and evaluation strategy.

IT Dashboard—A specific format requested by the DBC that presents certain information regarding a system and the status of its implementation.

IT Service—An automated capability that employs web-based technology to deliver information and functionality to requesters. The service is reusable and can be accessible to either human or automated requesters, or both. A service can consist of the following:

- One or more web services
- One or more web services with a web application

- One or more web services with a persistent data repository
- One or more web services with a web application and a persistent data repository
- Legacy web application (interacts directly with a non-web service application) with or without a repository.

Legal, Regulatory and Policy (LRP) Requirements—All Federal laws and Federal, DoD and AF regulations and policies that affect or are affected by the identified need.

Materiel Implementation (M-Implementation) Plan—The plan for developing/acquiring and delivering the materiel solution. The plan should include all activities needed across skill sets (e.g., architecture, system engineering, acquisition, funding, contracting, governance, testing and evaluation, and compliance).

Materiel Solution—Correction of a deficiency, satisfaction of a capability gap, or incorporation of new technology that results in the development, acquisition, procurement or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related software, spares, repair parts and support equipment, but excluding real property, installations and utilities) necessary to equip, operate, maintain and support military activities without disruption as to its application for administrative or combat purposes. (DoDD 4630.05) Within the context of the SDDP, the materiel solution is focused on the acquisition or development of Information Technologies, specifically software.

Measure of Effectiveness (MOE)—Metrics that are used to measure mission success and are specific to the conditions under which a mission will be executed.

Measure of Performance (MOP)—Measure used to determine task performance and the conditions under which the tasks are performed. Static MOPs include metrics that can be measured through simple observation. Dynamic MOPs are metrics that are measured during actual operation of the IT Capability.

Milestone—Date for completion of activities or deliverables.

Milestone Decision Authority—The designated individual with overall responsibility for a program who has authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting. (DoDD5000.01)

Mission Critical Requirement—A characterization of criticality and priority of need from a warfighter or user perspective.

National Security System (NSS)—Any telecommunications or information system operated by the US Government, the function, operation or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications). (44 USC 3542(b)(2))

Need/Problem Statement—A general statement that describes clearly the situation causing inefficiencies and work delays. The need statement includes an outline of what the need is, defines the problems that arise from the need, describes why the need is important, identifies the

AF Senior Leadership that will support the initiative, details what improvements will result from the proposed changes and describes how the need is carried out.

Network Operations—The operation and monitoring of platform and applications deployed onto the platform.

Onboarding—The capture of activities necessary to prepare the platform environment to receive a new capability. Onboarding activities are captured within the IMS.

Onboarding Compliance—An identification of any protocols, standards or other constraints, to which the materiel solution must adhere in order to be deployed, operated and sustained within the platform environment.

Onboarding Plan—A definition of the actions to be completed to onboard the materiel solution into the platform environment for operation and sustainment.

Ontology—A semantic representation of the information assets, as well as the associated authoritative and source data, to ensure the understandability and discoverability of the information asset and its associated authoritative and source data.

Performance Attribute—A description of the components that make up the successful delivery of capability (performance measure).

Performance Measure—A description of the successful delivery of capability in terms of desired outcomes. Performance Measures are sometimes referred to as Measures of Success.

Performance Metric—A point at which performance attributes are monitored. A metric is a quantitative measure of the degree to which a capability possesses a given attribute.

Performance Parameters—Acceptable boundary conditions for the performance metrics.

Performance Reference Model (PRM)—The PRM is a framework to measure the performance of major IT initiatives and their contribution to program performance. The PRM will help agencies: produce enhanced performance information; improve the alignment and better articulate the contribution of inputs, such as technology, to outputs and outcomes; and identify improvement opportunities that span traditional organizational boundaries.

Persistent Data Repository—A database, XML repository, file directory, flat file or other such data structure that maintains data either consumed or generated by the web services at the behest of a requester.

Platform Engineering—Engineering activities to prepare the platform environment to receive a materiel solution or to inform the technical implementation of the materiel solution to assure that it deploys successfully into the platform environment.

Platform Environment—The hosting environment into which the capability will be deployed. The platform environment includes the IT infrastructure, computing resources and facilities, and enterprise services such as security and monitoring, that are necessary to deploy, operate and sustain the materiel solution. The platform environment includes the Development, Testing and Operational Environments.

Platform Service Order—Platform Service Order gives instructions and directions to Platform Engineering and Network Operations and includes those orders to take those actions necessary to configure the Platform in order to deploy the IT capability successfully.

Process Team—The team responsible for understanding, explaining and capturing their mission processes and identifying areas where processes could be improved.

Program Executive Officer (PEO)—An individual within the AF Acquisition community assigned responsibilities for a specific program or a portfolio of programs and projects that together provide a specific capability set.

Program Office—The organization or team responsible for the delivery of a specific warfighter capability.

Project Lead—Individual with responsibility for the planning, execution and closing of the materiel solution. The project lead is responsible to track process against cost, schedule and performance and to manage resources (money and manpower) assigned to the project.

Prototype—An early sample or model built to test a concept or process and specifically to test the design of an IT capability to assure it functions correctly and delivers the required capabilities.

RACI Matrix— Listing of roles/responsibilities in terms of Responsible, Accountable, Consulted or Informed; and other items necessary to manage the activity effectively.

Representational State Transfer (REST)—A type of web service where each unique URL is a representation of some object.

Resource—An individual with specific skill sets to help conduct the work.

Resourcing—An identification of the requisite organizational, personnel, facility and funding necessary to implement the materiel solution successfully.

Responsible, Accountable, Consulted or Informed (RACI) Matrix—Listing of who is Responsible, Accountable, Consulted or Informed of various activities within the set of work. It is especially useful in clarifying roles and responsibilities in cross-functional/ departmental projects and processes.

Reusable Artifact—A product generated by previous COIs that can be reused by a COI for a materiel solution.

Reuse—Identifying and incorporating into a materiel solution capabilities already owned or operated within the DoD or AF, in order to same time, money and inherit compliance against the reusable capability.

Reuse Component—An existing web service, COTS/GOTS component or system component that can supply a proposed materiel solution with all or portions of a service layering, functional requirements, information exchanges or information assets that are already defined and implemented through some other materiel solution.

Requirements Traceability Matrix (RTM)—A document that provides alignment from the original statement of a requirement to the delivery of capability. A requirements trace is bi-directional between various associated requirements and the implementation of those requirements.

Roles and Permissions—Identification of personnel who have access to each information asset, the authoritative and source data, and the criteria for assignment to access.

Service—The means by which the needs of a consumer are brought together with the capabilities of a provider. (**http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.html**)

Service Development and Delivery Process (SDDP)—the end-to-end process by which capability-supporting mission processes are identified, described, developed and deployed.

Service Layering—A definition of the individual services that will be implemented within the materiel solution.

Service Level—A description of the technical performance parameters for each service, including response times and availability. Service Levels are derived from the Step 1 performance measures that are associated with the mission processes included in the Conceptual Model.

Service Level Agreement (SLA)—A description of the official service levels that the materiel solution will be able to meet once it is deployed, operated and sustained within the platform environment.

Service Monitoring Requirement—A description of the levels of service monitoring required from the platform environment during the deployment and sustainment phases of the materiel solution.

Service Reference Model (SRM)—A description of the functions and services that the materiel solution must deliver in order to solve the end user's problem and/or satisfy the end user's needs. The SRM information must be at a sufficient level of completeness, consistency and detail to prepare a bounded user requirement sufficient to select a satisfactory COTS product or develop software code to deliver the materiel solution successfully.

Skill Set—Each swim lane within the SDDP process charts captures tasks done by a specific skill set. The charts do not identify the organizations that may be responsible to bring those skill sets to the AF user.

Sponsor—The individual or organization responsible for documentation, periodic reporting, and funding actions necessary to support the delivery of needed capabilities (e.g., MAJCOM, FOA).

Subject Matter Expert (SME)—An individual that has actual experience in the mission or process being defined; typically, the warfighter.

System Engineering—The skill set needed to design the materiel solution. System engineering must address architectures, design, technical management, test and evaluation, verification and validation, environment, safety, and occupational health, and human systems integration. These fundamental elements must be accomplished.

Task—A work item that must be completed by identified resources.

Technical Reference Model (TRM)—A foundation used to describe the standards, specifications and technologies supporting the delivery, exchange and construction of business (or service) components and E-Government solutions. The TRM unifies existing agency TRMs and E-Government guidance by providing a foundation to advance the re- use of technology and component services from a government-wide perspective. (OMB Circular A-11)

Test and Evaluation Master Plan (TEMP)—A document detailing the overall structure and objectives of the enterprise T&E program. The TEMP provides a framework within which to

generate detailed T&E plans and documents schedule and resource implications associated with the T&E program.

Testing—The skill set needed to assure that a capability as implemented functions as designed and satisfies the user's need/problem statement.

Timeline—Length of time allocated for the tasks to be completed by the resources.

Topology Requirement—A modification to the physical location of computers, network connections or core platform services, or a modification to the capacity provided by the platform environment that is required in order to deploy and operate the materiel solution.

Vocabulary Package—A complete product of COI work that is made up of the ADS mapping, roles and permissions, example data records and ontology.

Web Application—A Java-based or other type of application that provides a human-user interface to the capabilities delivered by a set of web services. The web application includes user interface screens and presentation services generally delivered through HTML or other similar protocol standard.

Web Service—Either a SOAP-based or REST service that delivers information and functionality at the request of a consumer.

Web Services Code Requirements—A description of the requirements to implement a web service or set of web services as part of the materiel solution.

Work Breakdown Structure (WBS)—A tool used to define and group a project's discrete work elements in a way that helps organize and define the total work scope of the project.

Work Plan—A charter or plan to perform specific work. Within the SDDP, a work plan is often focused on completing a single Step of the SDDP and typically consists of Tasks, Resources, Timelines, Milestones, RACI Matrix and other items necessary to manage the activity effectively.

Tasks – List of work items that must be completed by identified resources; Resources – List of individuals with specific skill sets to help conduct the work; Timelines – Length of time allocated for the tasks to be completed by assigned resources;
Milestones – Dates for completion of actions or deliverables;
*****RACI Matrix – Listing of roles/responsibilities in terms of Responsible, Accountable, Consulted or Informed; and
Other items necessary to manage the activity effectively.

Attachment 2

PERFORMANCE MEASUREMENT WITHIN THE SDDP

A2.1. Introduction. Performance Measurement within the SDDP is an iterative decomposition of the initial Step 1 Performance Measures used to define the successful delivery of DOTMLPF-P capabilities to solve the sponsor's problem. These measures can then be used as testable performance requirements for the Materiel Solution. The performance requirements can be used in both Operational Test and Evaluation (OT&E) and in Development Test and Evaluation (DT&E). Performance Measurement is accomplished through the specification of categories of performance indicators that are associated directly with specific products generated during an SDDP Initiative.

A2.2. Performance Indicator Definitions.

A2.2.1. **Performance Measures.** A Performance Measure is a description of the successful delivery of capability in terms of desired outcomes. The Performance Measures are linked to the DOTMLPF-P Capabilities to indicate when each of those capabilities has been successfully implemented. These Performance Measures serve as the basis for all subsequent Measures. Since SDDP DOTMLPF-P Capabilities are synonymous to the High Level Outcomes that are defined in acquisition policy, Performance Measures are also directly linked to the High Level Outcomes. These measures are sometimes referred to as Measures of Success, not to be confused with Measures of Suitability.

A2.2.2. **Measures of Effectiveness (MOE).** The **JCIDS Manual 19 Jan 2012 Appendix F to Enclosure B** defines a Measure of Effectiveness as metrics that are used to measure mission success and are specific to the conditions under which a mission will be executed. Within the SDDP, a Measure of Effectiveness indicates when a re-engineered business process is being executed optimally. Measures of Effectiveness can be time-oriented or capacity-based, such as volume of transactions through a process. Measures of Effectiveness are used to describe Business Outcomes (BO) in acquisition guidance.

A2.2.3. **Measures of Performance (MOP).** The **JCIDS Manual 19 Jan 2012 Appendix F to Enclosure B** defines a Measure of Performance as a measure used to determine task performance and the conditions under which the tasks are performed. Within the Materiel Solution of the SDDP, these MOPs view the tasks to be performed as the IT Performance Requirements that the Materiel Solution must perform and that are included in the IT Capability specifications. Performance requirements are attributes of IT requirements, specifically IT Functional Requirements and Information Assets that indicate when an IT Capability is performing optimally and meeting its end user needs. Performance requirements are two types, static and dynamic MOPs. Static MOPs include metrics that can be measured through simple observation, such as information storage capacity represented by a specific number of documents that an IT Capability must be able to store online. Dynamic MOPs are metrics that are measured during actual operation of the IT Capability, such as response times or availability measures.

A2.3. Relationships among Performance Indicators. Performance indicators, including Performance Measures, MOEs, and MOPs, do not exist as individual requirements within the SDDP. Each of these types of performance indicators is actually an attribute of another type of requirement. Performance Measures are attributes of the DOTMLPF-P Deployable Capabilities.

MOEs are attributes of the re- engineered business processes resulting from Step 2. MOPs are attributes of the IT Functional Requirements and Information Asset Requirements identified in Step 3. These relationships are depicted in **Table A2.1**.

In addition to these relationships, there is an inherent relationship between the different types of performance indicators. Since certain aspects of the DOTMLPF-P Capabilities are delivered through re-engineered business processes, the MOEs associated with each business process are also associated with the Performance Measures for the DOTMLPF-P Capabilities that each business process supports. Similarly, each MOP is associated with each MOE for the business process to which each IT Functional Requirement or Information Asset must provide support.

Table A2.1. Mapping of Performance Measures.

SDDP Step	SDDP Product	Performance Indicator	Acquisition Policy
Step 1	DOTMLPF-P Capabilities	Performance Measures	High Level Outcomes (HLO)
Step 2	Re-engineered Business Processes	Measures of Effectiveness (MOE)	Business Objectives (BO)
Step 3	IT Functional Requirements/Information Assets	Measures of Performance (MOP)	N/A

A2.4. Applicability. Performance measurement supports multiple activities within an SDDP Initiative.

A2.4.1. The Performance Measures are used at the enterprise level to determine whether the execution of the DOTMLPF-P Implementation Plan resulted in the targeted improvements to the performance of the Sponsor's organization that was driving the SDDP effort. The Sponsor's organizational performance may be measured at individual organizational units or at the Air Force enterprise level.

A2.4.2. MOEs can be used to derive the Operational Test and Evaluation (OT&E) test procedures and scripts. The MOEs enable the Independent Test Team to define OT&E test procedures and scripts that determine how well the Materiel Solution support the work that is being done by the end users, as represented by the re-engineered business processes to which the MOEs apply.

A2.4.3. The MOPs are used to generate the test procedures and scripts for Development Test and Evaluation (DT&E). The MOPs assist the Independent Test Team in evaluating the successful implementation of each of the IT Functional Requirements and Information Asset Requirements associated with each MOP.

A2.5. Example. **Table A2.2** depicts an example of the derivation of performance measurement in an SDDP Initiative. In the example, the DOTMLPF-P Capability identified in the PRM is the Lifecycle Case Management, providing greater management control over the cases that are presented to Review Boards within the USAF. The current situation is marked by a large backlog of cases and cases that take longer to adjudicate than what is mandated by legal and statutory requirements. A performance measure indicating that the Lifecycle Case Management DOTMLPF-P Capability has been implemented successfully is that there is less than 5% of the

total number of cases that exceed the legal or statutory deadlines for adjudication. Ideally there would never be a case that took longer than the mandated statutory requirements, but it is unrealistic to set a target which cannot be guaranteed to be met. The re-engineered business process necessary to deliver this DOTMLPF-P Capability is the Case Adjudication Process. That process has a MOE of 8 months to adjudicate each case which is less than the statutory requirement of 10 months. Finally the MOP for the ITFR is that the Materiel Solution must be able to rapidly ingest the case documentation for 10,000 cases in a year. This would most likely not be the only MOP for that ITFR, as there will likely be an MOP that dictates how quickly the ITFR must ingest each set of case documentation. The example shows the derivation of a MOP in support of the MOE to complete adjudication of a case within 8 months.

Table A2.2. Example of SDDP Performance Measurement.

Requirement	Performance Indicator
DOTMLPF-P Capability: Lifecycle Case Management	**Performance Measure:** Fewer than 5% of cases take longer to adjudicate than mandated by legal or statutory requirements
Business Process: Case Adjudication	**MOE:** Complete Case Adjudication in 8 months, instead of statutory requirement of 10 months
ITFR: Ingest Case Documentation	**MOP:** Ingest 10,000 cases per year. Given a 40 hour work week for 50 weeks this equates to ingesting one case every 12 minutes, so the ITFR must be completed in 12 minutes.

Attachment 3

PLATFORM ENVIRONMENT AND BASELINES

A3.1. The SDDP is enhanced by, but not dependent upon, a centrally managed and configuration-controlled platform environment. The AF Chief Information Officer (CIO)/A6, Air Force Materiel Command (AFMC) through the AFLCMC, and Air Force Space Command (AFSPC) are working to provision this platform environment. The platform environment will comprise any number of different platform service implementations and components, including AF, DoD or commercial platform services, as provided by AFSPC, either organically or through agreement or contract. In order to facilitate the SDDP reader in understanding the capabilities the platform environment will bring, the following terms are defined, refer to AFPD 33-4 for additional details:

Table A3.1. Term Definition (AFPD 33-4).

Baseline	Description	Governance
Target **CIO/CTO** Phase The "To Be"	The TB specifies the standards, protocols, guidelines and implementation constraints for the future state of the AF IT infrastructure. It is used to inform the development of the implementation baseline. The TB is thoroughly documented and continually updated based upon emerging industry standards and the evolving AF EA.	The AF CEIB CCB will be the controlling body for all changes to AF CEIB documentation. This CCB reviews and approves/ disapproves configuration item instantiations and change requests to existing configuration items. Approved items are submitted to the AF CIO Council by the AF Chief Technology Officer (CTO) for validation.
Implementation **ACQUISITION** Phase	The IB is the associated baseline of acquisition selected products and their target baseline informed/ allowed configurations that implement the architecture, standards, protocols and guidelines specified in the TB. The IB informs the OB of the acquisition selected products and how they are to be configured to support deployment of user applications across the infrastructure topology. The IB governs the implementation of the Development and Integration/Test environments.	The IB is governed by the ITLC or Enterprise System Engineering function and validated by the CTO.

Operational **RUN TIME** Phase The "As Is"	The OB is the set of components of the IB appropriately configured and deployed across the topology of the AF IT infrastructure that implements the architecture, standards, protocols and guidelines specified in the TB and provide the required warfighter capabilities and performance. It specifies the exact lay-down and configurations of hardware and software within all facilities in the AF infrastructure topology.	The OB is managed by the 24th AF validated by the ITLC or Enterprise System Engineering function and validated by the CTO.

The figure below depicts the relationship between the baselines as described in AFPD 33-4.

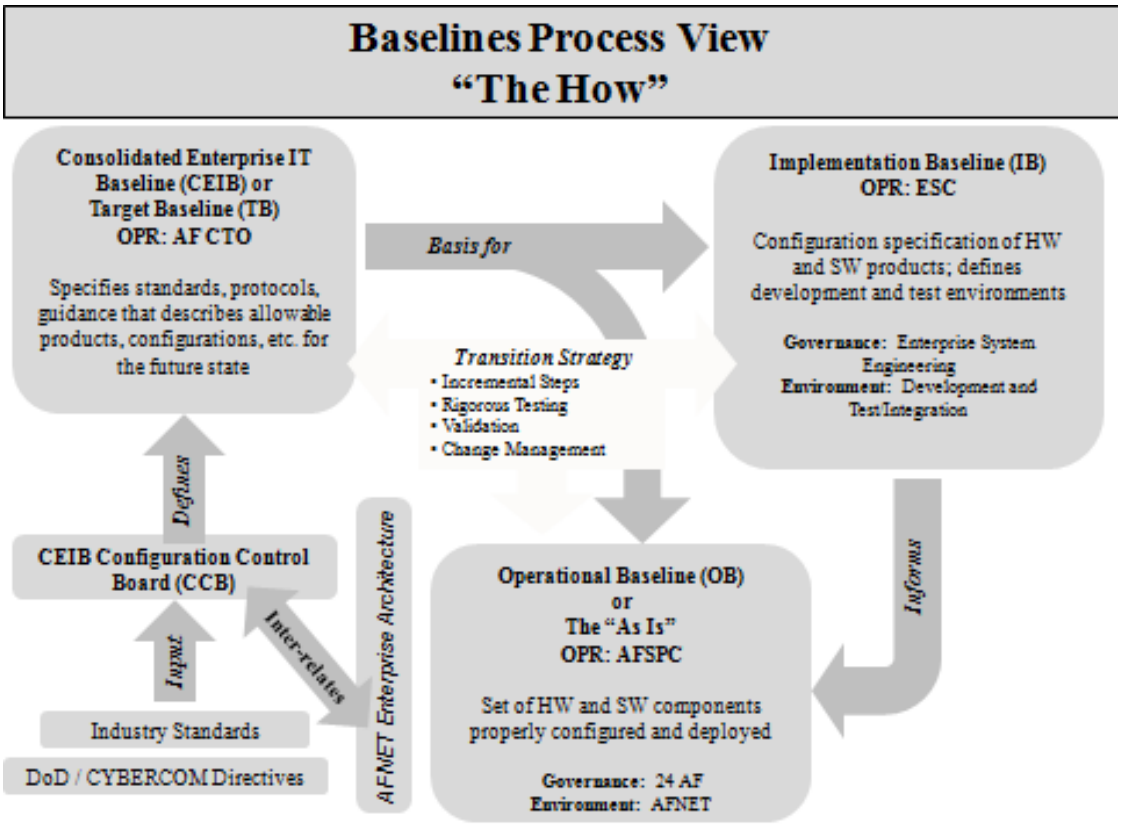



Figure A3.1. Baseline Process View.