United States Air Force

Clinger-Cohen Act Implementation Guide



**AS OF OCTOBER 18, 2022**

Please contact Neal S. Zank, SAF/CNZA, 703-695-6102,

if you have questions about Clinger-Cohen Act compliance or the CCA Implementation Guide

**INTRODUCTION**

The United States Air Force Clinger-Cohen Act Implementation Guide is a supplement to AFMAN 17-1402, *Clinger-Cohen Act (CCA) Compliance*, 20 June 2018. As noted in AFMAN 17-1402, implementation of CCA in the Air Force is the responsibility of the Chief Information Officer of the Air Force, represented by SAF/CN. AFMAN 17-1402 will be revised after a new version of DoDI 5000.82 is approved by the DoD CIO.

This Guide is designed to clarify the application of the CCA confirmation and compliance requirements to AF programs and provide the latest CCA requirements, guidance, and techniques for achieving CCA compliance. It provides detailed direction for addressing the 11 CCA elements listed on the Air Force Clinger-Cohen Act Compliance Table (Attachment 1).

The SAF/CNZA CCA Point of Contact can be contacted directly at [neal.zank.1@us.af.mil.](mailto:neal.zank.1@us.af.mil) The *Defense Acquisition Guidebook*, [https://www.dau.edu/tools/dag,](https://www.dau.edu/tools/dag) and the *USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site,* <https://usaf.dps.mil/sites/10774/default.aspx> contain authoritative sources, information, and templates to aid in preparing a CCA compliance package and in learning about CCA compliance and IT acquisition.

The acquisition processes followed by DoD have evolved over the years. After several years of consolidation and relying largely on one acquisition approach, DoD adopted a new Adaptive Acquisition Framework (AAF). The AAF incorporates a series of overarching policies, acquisition pathways, and functional policies that provide opportunities to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired. The relevant policies and pathways are listed below.

Overarching Policies

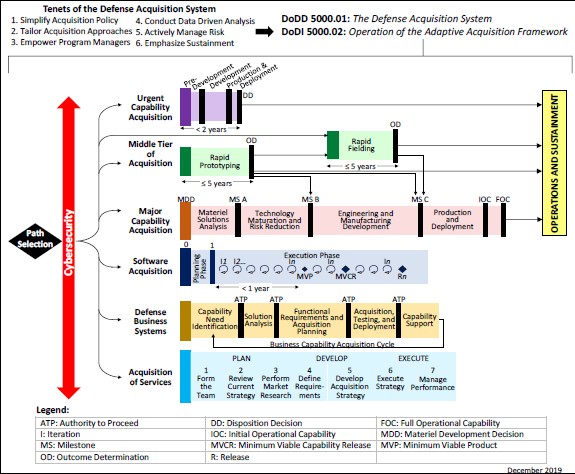
* *The Defense Acquisition System*, [DoDD 5000.01](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf?ver=2020-09-09-160307-310), September 9, 2020
* *Operation of the Adaptive Acquisition Framework*, [DoDI 5000.02](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093), January 23, 2020
* *Operation of the Defense Acquisition System (Change 10)*, [DoDI 5000.02T](https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002T.PDF?ver=oDQmg66hNAl51QOELK18UQ%3d%3d), December 31, 2020

Acquisition Pathway Policies

* *Defense Acquisition of Services – Change 1*, DoDI 5000.74, June 24, 2021
* *Business Systems Requirements and Acquisition – Change 2*, DoDI 5000.75, January 24, 2020
* *Operation of the Middle Tier of Acquisition (MTA),* DoDI 5000.80, December 30, 2019
* *Urgent Capability Acquisition*, DoDI 5000.81, December 31, 2019
* *Major Capability Acquisition*, DoDI 5000.85, August 6, 2020
* *Operation of the Software Acquisition Pathway*, DoDI 5000.87, October 2, 2020 Functional Policies
* *Acquisition of Information Technology*, DoDI 5000.82, April 21, 2020
* *Analysis of Alternatives*, DoDI 5000.84, August 4, 2020

Statutory and regulatory information requirements for CCA compliance, for all milestones and phases for all acquisition pathways, can be found at the Acquisition Framework Document Identification Tool (AAFDID) at the Defense Acquisition University portal and is available at [https://www.dau.edu/aafdid/Pages/About.aspx.](https://www.dau.edu/aafdid/Pages/About.aspx) Those tables also provide information on when CCA compliance should be accomplished for each acquisition pathway.

The Adaptive Acquisition Framework is shown below in Figure 1.



**FIGURE 1: The Adaptive Acquisition Framework**

Among the benefits of employing the Adaptive Acquisition Framework are the ability to simplify acquisition policy and tailor acquisition approaches to different types of investments. In that context, we continue to apply a CCA compliance approach that is flexible but that meets the requirements of both statute and DoD policy. Although the CCA compliance process is generally the same for all types of acquisitions, it is flexible enough to accommodate the differences among ACAT programs, Sec 804 programs, As a Service programs, and Defense Business Systems. Examples of those types of flexibility are:

* Documents used as evidence of compliance for CCA Elements 1, 2, 3, 4, 5, 6, 7, & 10 are approved by the Program Manager, not by SAF/CN. The Program Manager is responsible for determining that the documents listed as evidence of compliance with CCA elements 1, 2, 3, 4, 5, 7, and 10 are CCA compliant. SAF/CN will address the compliance documentation for CCA elements 8, 9, and 11. Starting in FY 20, the local cost centers approve the CCA element 6 submissions for less than ACAT I programs (see Section 7.0 below).
* CCA approvals are granted at milestones, Authority to Proceed (ATP) events, or contract awards, depending upon the pathway being followed.
* Each pathway has a different entry point for CCA compliance based upon the unique characteristics of that acquisition. For example, MTA programs do not use traditional milestones; therefore, CCA compliance is accomplished with the contract award associated with the start of the rapid prototyping phase and the contract award associated with the start of the rapid fielding phase. The primary difference between those two phases is that there is usually a solution associated with the latter phase.
* A broad range of documents may be used to demonstrate proof of compliance for the CCA elements, and these may differ by pathway.

Please contact SAF/CNZA for additional information on how CCA applies to your specific program (entry points, schedule, documentation, etc.).

The AF also provides guidance in the form of AFIs, AFMANs, Air Force Guidance Memoranda, and other Air Force Memoranda that address those acquisition approaches.

* Traditional programs generally include the warfighting systems that were addressed in DoDI 5000.02 and are ACAT Is, IIs, and IIIs. They are sometimes referred to as Major Capability acquisitions or MDAPs. They operate under the Defense Acquisition System.
* Middle Tier Acquisition includes Rapid Prototyping and Rapid Fielding programs commonly referred to as Section 804 programs. Section 804 programs are generally exempt from DoDI 5000.02 regulatory requirements and are not ACAT programs.
* Defense Business Systems (DBSs) follow the Business Capability Acquisition Cycle (BCAC) process and are referred to as BCAT programs. SAF/CN will work closely with DBSs undertaking the BCAC process.

The foundation of CCA compliance is built upon the use of existing documents, most of which are prepared at earlier stages of the program lifecycle development process. For most Acquisition Category programs, those processes are the Joint Capabilities Integration and Development System and Defense Acquisition System. For Defense Business Systems, some of the documentation may be prepared under the Business Capability Acquisition Cycle and the Defense Acquisition System processes.

The sections below describe the type of information that Program Managers and SAF/CN look for in the documents submitted to demonstrate compliance with the 11 CCA elements as listed in Table 10 from DoDI 5000.02 and for Post Implementation Reviews.

# CCA Compliance Element 1. Make a determination that the acquisition supports core, priority functions of the DoD.

* 1. Documents submitted to comply with this element should validate and explain the rationale supporting the relationship between the AF's mission (i.e., core/priority functions) as found in AF mission and strategy documents, and the IT function supported by the investment or acquisition. Is the function that the proposed IT acquisition supports central to or priorities for the AF’s mission, or something the Federal Government actually needs to perform? Is the function one that DoD and/or its Components have to perform to accomplish the military missions or business processes of the Department? What are the linkages among the mission, the function supported, the capability gap, and potential solutions?
  2. For Warfighting Mission Area programs, this question is usually answered in the Joint Capabilities Integration and Development System (JCIDS) process. The JCIDS analyses should demonstrate that the acquisition supports core/priority functions that should be performed by the Federal Government. Examples of a valid mission need include a combat or weapon system or an integral part of a weapons system, Joint operations in support of the warfighter, or designation as a National Security System (NSS). The supporting documentation for this element might include mission and strategy documents like the Quadrennial Defense Review, Strategic Planning Guidance, Joint Operating Concepts, Joint Functional Concepts, the Universal Joint Task List, mission area statements, or Service mission statements.
  3. For Business Mission Area programs, this question may be answered in the BCAC process. Information Environment Mission Area programs may rely upon the DoD Enterprise Service Management Framework for this information.

# CCA Compliance Element 2. Establish outcome-based performance measures linked to strategic goals.

* 1. Outcome-based performance measures (OBPMs) assess the actual results, effects, contributions, accomplishments, or impacts of a program compared to its intended purpose. OBPMs represent the mission outcomes that would fill a functional gap identified as the need for a program and would be used in justifying the program. They measure the ability of the delivered system to achieve a need, requirement, or capability based on an established baseline previously identified by the user. OBPMs also serve as the basis for developing the program’s Post-Implementation Report (see Section 12.0 of this Guide).
  2. OBPMs for the capabilities of warfighting systems are generally developed during a Capabilities-Based Assessment and recorded in a validated Initial Capabilities Document. In older programs, the OBPMs related to the achievement of a needed capability (rather than actual system performance) might be found in a Mission Need Statement or an equivalent document. Business Mission Area programs identify OBPMs in the Problem Statement.
  3. OBPMs should be established before the Concept Decision that starts the acquisition process or at the pre-Milestone A stage and validated at Milestone A. If that has not occurred in an

existing program, the OBPMs should be developed before Milestone B. There should be a statement in the program documentation about the desired outcome and how the program would develop and deploy the solution to achieve that outcome (an outcome is the resulting effect of an IT investment on an organization). The OBPMs should be determined prior to the selection of a particular alternative approach or contractor, be independent of any solution, and not specify system performance or criteria.

* 1. The OBPMs should measure the value-added contribution of the IT investment to missions, goals, and objectives and provide a clear basis for assessing accomplishment and aiding decision-making. This requires the collection of performance data and comparing actual to projected performance from carrying out a program or activity, thereby determining an investment's efficiency and effectiveness in meeting cost, benefit, schedule, risk, mission, documentation, and performance objectives.
  2. Examples of OBPMs could be measuring the number of enemy submarines sunk or enemy tanks destroyed may be satisfactory OBPMs if the objective is to destroy such weapons systems, or (b) measuring the reduction in operating or manpower costs or the replacement of multiple legacy systems with a new single system, or facilitating command decision-making.
  3. When formulating OBPMs, it is important to differentiate between OBPMs, and output measures, Key Performance Parameters, and acquisition performance measures. Outputs are defined as “the level of activity that will be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity.” For example, in the case of the learning management system, output measures could be the number of courses delivered on relevant topics or the number of instructors hired. Key Performance Parameters are those attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability and those attributes that make a significant contribution to the key characteristics as defined in the Joint Operations Concept. Key Performance Parameters and other performance measures may be used to satisfy CCA Element 7 (see Section 7.0 of this document).

# CCA Compliance Element 3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of commercial off-the-shelf technology.

* 1. Documentation submitted for this element should demonstrate how the investment reduces costs and improves performance. Does the program’s Business Process Reengineering (BPR) optimize process performance by streamlining procedures, eliminating redundant or unnecessary tasks, optimizing resource allocations, and reducing risk and development time? The Program should revise its mission-related processes and administrative processes as appropriate before making significant investments in IT.
  2. Information supporting this element should describe the actions taken to streamline, reengineer, or redesign existing processes to reduce costs, improve effectiveness, and maximize the use of COTS or tailored versions of Government off-the-Shelf technology that better support the organization’s mission. In the absence of a total COTS solution, the program should

endeavor to utilize COTS technology as part of an overall solution and approach to reducing costs, etc., while maintaining vision on any operational risks or second-order effects of using a product from a commercial vendor. For DBSs, the requirement may be met by the BPR analysis prepared for and approved by SAF/MG.

# CCA Compliance Element 4. Determine that no private sector or government source can better support the function.

* 1. Documentation submitted for this element should demonstrate that the acquisition is being undertaken by the AF because it requires unique capabilities that are not found in the private sector or elsewhere in the public sector in a way that can support the function more effectively or at less cost. Program Managers should determine that the proposed function does not duplicate or overlap with an existing function being performed elsewhere by the Federal Government, DoD, or AF entities.
  2. Depending on the project’s current milestone review, some questions to be considered are:
     1. Does the proposed investment in IT support core mission or inherently governmental functions that need or have to be performed by the Government?
     2. Can the functions be accomplished more efficiently (reduced cost and/or improved effectiveness) by another federal organization?
     3. Does the proposed IT investment fall under Office of Management and Budget Circular A- 76, *Performance of Commercial Activities, May 29, 2003* (Outsourcing policy)

# CCA Compliance Element 5. Conduct an analysis of alternatives.

* 1. The Analysis of Alternatives (AoA) or market research conducted for the investment should address whether the program prepared a thorough AoA and considered enough reasonable alternatives. DoDI 5000.84 indicates that the AoA identify a wide range of solutions that have a reasonable likelihood of providing the needed capability); the alternatives examined (including the pros and cons of each alternative); and why the selected alternative was chosen and why the remaining alternatives were not chosen.
  2. A frequent question is whether an AoA should be updated as the Program goes through the milestone process. The answer depends upon whether the Analysis of Alternatives was written in a way that addresses changes to the program occurring after the AoA was approved. An update is not required if the AoA was specific enough to address the changes; however, the Program Manager should consider revising the AoA if, for example, it specified the use of software ABC V.1.0 and the contemplated contract and/or Milestone decision brief intends to procure software XYZ V.5.0.

# CCA Compliance Element 6. Conduct an Economic Analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a life-cycle cost estimate.

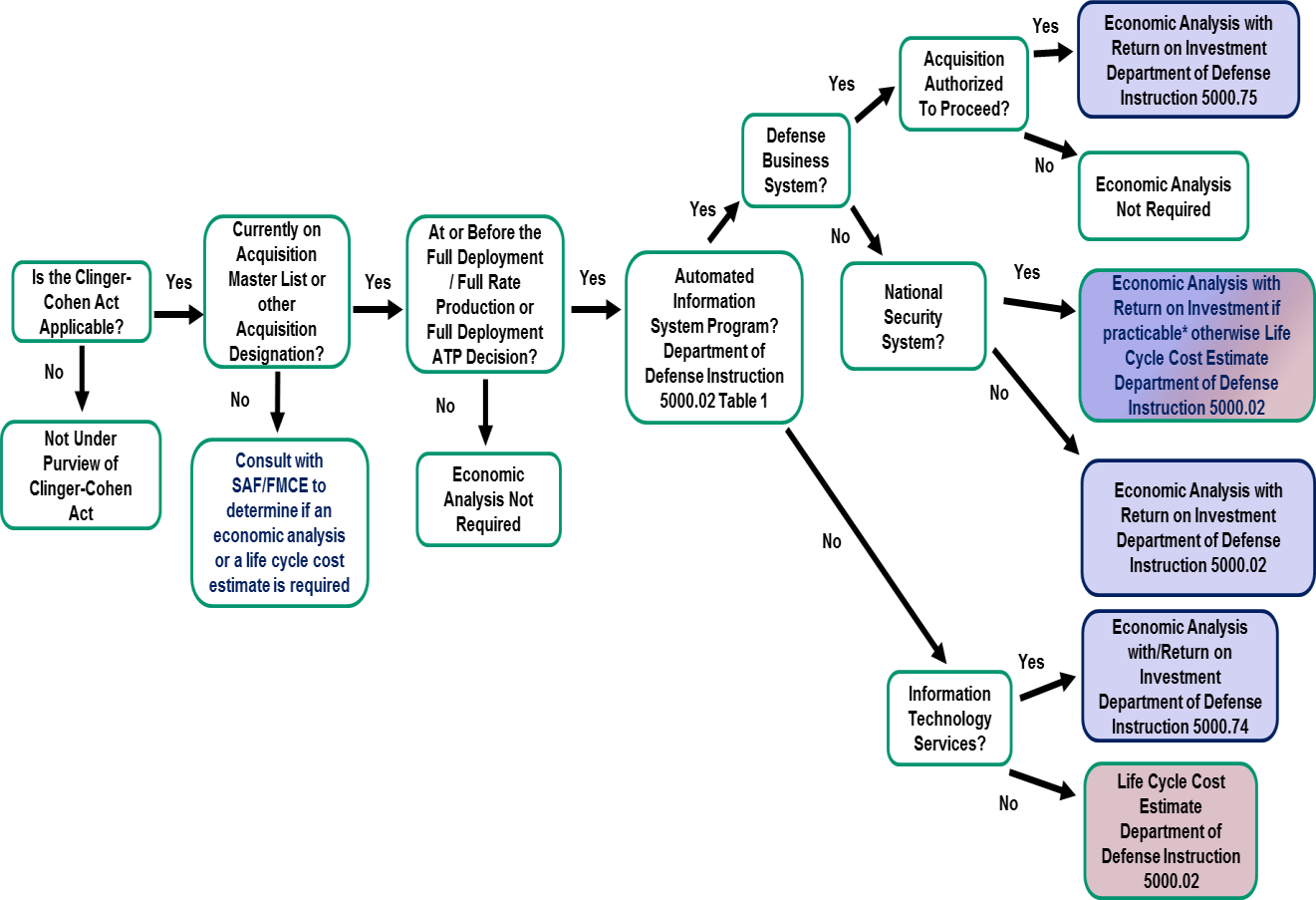
* 1. CCA requires an Economic Analysis with a calculated Return on Investment (ROI) or a Life-Cycle Cost Estimate (LCCE) depending on the type of system being acquired. Program cost analysts and Program Management Offices (PMOs) are encouraged to coordinate early in the Economic Analysis and LCCE development processes with SAF/FMCE (the Directorate of Economics and Business Management) or the analysts at the local cost centers.
  2. Cost analysts should rely on the policy direction contained in AFMAN 65-506, *Economic Analysis*, 6 September 2019 and AFI 65-501, *Economic Analysis*, 29 October 2018. AFMAN 65-506 includes an Attachment 13 on “Clinger-Cohen Act Economic Analyses” that provides information that can be used to determine which type of analysis is required, when in the acquisition life cycle the analysis is required, and information specific to preparing CCA economic analyses.
  3. An Economic Analysis is a systematic approach to the problem of choosing how to use scarce resources to meet a given objective. It includes consideration of costs, benefits, and uncertainties associated with all alternatives under consideration. At times, the term economic analysis is used in reference to the product/document that results from applying the economic analysis systematic approach. Economic Analyses are produced and documented in accordance with AFI 65-501 and AFMAN 65-506.
  4. A LCCE provides a structured accounting of all resources and associated cost elements required to develop, produce, deploy, and sustain a particular program. The LCCE encompasses all past (or sunk), present, and future costs for every aspect of the program, regardless of funding source. The LCCE should represent a realistic appraisal of the level of cost most likely to be realized, reflect the most up-to-date programmatic information, and be the estimate most recently reviewed by an independent cost oversight office. The LCCE will be performed according to the requirements of AFI 65-508, *Cost Analysis Guidance and Procedures*, 6 December 2018.
  5. Type Of Analysis Required. CCA requires an ROI calculation for automated information systems. These systems can either be wholly automated information systems such as a business system or they can be part of another weapon system or product such as software inside an aircraft. To satisfy CCA requirements, DoD requires an Economic Analysis or a LCCE depending on the type of system being procured. The following rules apply.
     + Acquisition Phase: In general, an economic analysis or LCCE is required for CCA purposes during the development and production or deployment acquisition phases. A program/ system at any phase after the full deployment decision (or equivalent) in its acquisition lifecycle is not required to update its economic analysis or LCCE for CCA purposes. DBSs are required to prepare an Economic Analysis at either a Contract Award decision or an ATP decision, depending upon how the program is following the BCAC process. Modification programs to the parent program require an independent economic analysis or LCCE for CCA purposes if that modification is treated as an acquisition program in its own right regardless of the acquisition phase of the parent program.
     + If the system under consideration is not an Automated Information System under DoDI 5000.02 Table 1 Note 4, then a LCCE is required for CCA purposes unless the program is an IT Services Contract. If a program is an IT Service Contract, then an Economic Analysis with a Return on Investment is required for CCA purposes.
     + If the program/system under consideration is an Automated Information System, but not a NSS and not a Defense Business System, then perform an Economic Analysis with an ROI.
     + If the program/system under consideration is an Automated Information System and also a NSS, then the ROI required for CCA purposes will be met using an economic analysis with return on investment if practicable; otherwise, a LCCE is required.

The initial determination of whether an economic analysis is practicable is made by the program office. The final determination is made by the highest level of Financial Management concurrence required for the analysis (Economic Analysis or LCCE). This will be either the Product Center Cost Chief, the Sustainment Center Cost Chief, the MAJCOM Cost Chief, or SAF/FMC, and is determined by acquisition category level. The program office may consult with the appropriate center level Cost Chief or SAF/FMC in advance when making an initial determination on whether an Economic Analysis is practicable. A list of local FM cost chiefs is provided on the *USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site*.

For acquisition programs, lack of time is rarely an acceptable reason for determining that accomplishing an Economic Analysis is not possible.

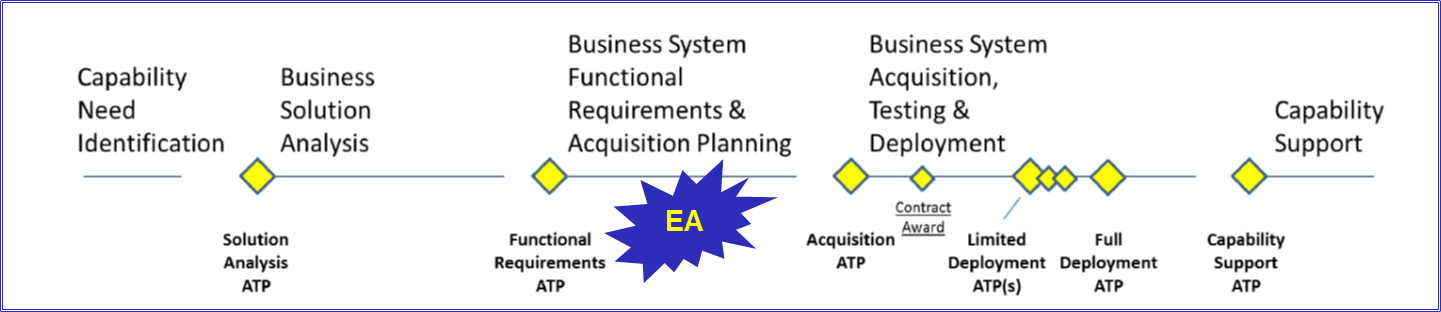
The requirements associated with conducting the Economic Analysis or LCCE is presented in the figure below.

# FIGURE 2: CCA Economic Analysis and Life Cycle Cost Estimate Requirements



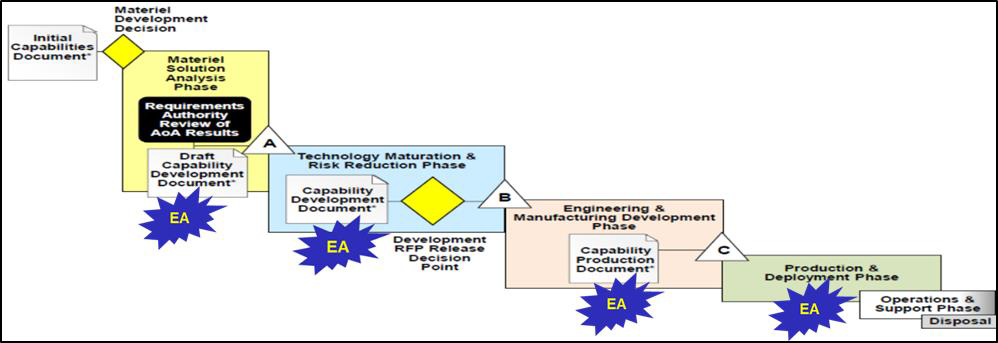
* 1. Timing of the Requirement for an Economic Analysis or Life Cycle Cost Estimate.
     + For DBSs, the Economic Analysis is required at the Contract Award decision or an ATP decision, depending upon how the program is following the BCAC process as described in DoDI 5000.75 and as shown in the figure below.

# FIGURE 3: Timing of Economic Analysis Requirement for Defense Business Systems



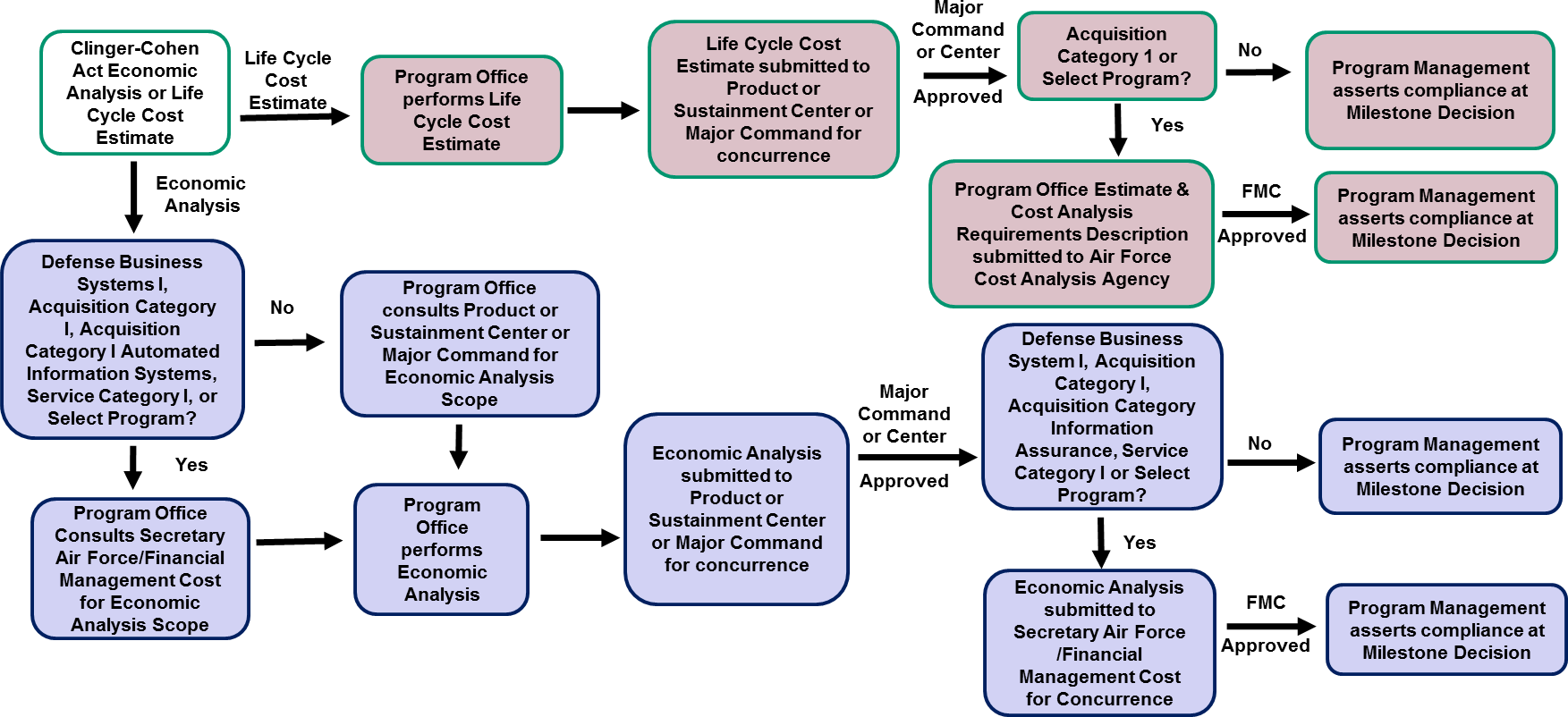
* + - For non-Defense Business Systems Automated Information Systems requiring an Economic Analysis, the Economic Analysis is required for Milestone A, B, C and Full Rate Production/Full Deployment decisions (or equivalent), as prescribed in the Defense Acquisition System in DoDI 5000.02 and as shown in the figure below.

# FIGURE 4: Timing of Economic Analysis Requirement for Non-Defense Business Systems



* 1. Coordination Process. If an Economic Analysis is required for CCA compliance, the Economic Analysis will be developed by the Program Office and submitted to the appropriate Cost Chief for concurrence and further reviews.
     + For DBSs that are Category I; non-Defense Business Systems that are ACAT I; and select programs as identified by the SecAF and/or Milestone Decision Authority, the Economic Analysis and associated documentation (including coordination by the appropriate Cost Chief’s office) will be submitted to Secretary of the Air Force/Financial Management Cost for review. The reviewing offices within the Secretary of the Air Force/Financial Management Cost are SAF/FMC and AFCAA/FMCI.
     + For non-select Defense Business Systems that are category II and III, the highest level of concurrence required is the Product Center Cost Chief, Sustainment Center Cost Chief, or MAJCOM Cost Chief. Similarly, for ACAT II and III systems that are non-select and non- Defense Business Systems, the highest level of concurrence required is the Product Center Cost Chief, Sustainment Center Cost Chief or MAJCOM Cost Chief. These cost offices’ coordination will serve as evidence of CCA compliance for category II and III non-select programs. A list of local FM cost chiefs is provided on the *USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site*. The coordination process is shown in the figure below.

# FIGURE 5: CCA Element 6 Process Flow and Coordination Requirements



* 1. **CCA Compliance Element 7. Develop clearly established measures and accountability for program progress.**
  2. Compliance documents should describe the process reporting, tools, and metrics for measuring program progress and post-deployment evaluation to include cost, schedule, and technical performance. Clearly established measures and accountability for program progress should be linked to strategic goals. The respective roles and responsibilities for the PMO and the contractors involved in the program in enforcing program control and Milestone Decision Authority-level directions to ensure accountability for program progress should be described.
  3. At milestone reviews, comparisons are made between the expected costs, risks, and benefits of earlier phases with the actual costs incurred, risks encountered, and benefits realized to date.
     1. Cost measures should reflect realistic cost estimates of the total program and/or increment. Budgeted amounts should never exceed the total cost thresholds (i.e., maximum costs) in the Acquisition Program Baseline (APB).
     2. Schedule parameters should include, as a minimum, the projected dates for program initiation, other major decision points, and Initial Operational Capability.
     3. KPPs and other measures of program performance should be identified and linked to strategic DoD and AF goals, periodic program management reviews, and quarterly metrics reviews.
  4. Among the documents that might provide information for this element are the APB (establishing program goals – thresholds and objectives – for the minimum number of cost, schedule, and performance parameters that describe the program over its life cycle); the AS (providing entrance and exit criteria in order to proceed into the next phase of the lifecycle); and the System Engineering Plan (SEP) that describes the system’s overall technical approach, including systems engineering processes; resources; and key technical tasks, activities, and events along with their metrics and success criteria? The APB, AS, and SEP should integrate or provide linkage with other program management control efforts that establish measures of accountability, such as [integrated master plans,](https://akss.dau.mil/dag/GuideBook/IG_c4.5.2.asp) [integrated master schedules,](https://akss.dau.mil/dag/GuideBook/IG_c4.5.3.asp) [technical](https://akss.dau.mil/dag/GuideBook/IG_c4.5.5.asp) [performance measures,](https://akss.dau.mil/dag/GuideBook/IG_c4.5.5.asp) [risk management](https://akss.dau.mil/dag/GuideBook/IG_c4.2.3.5.asp), PIR Plan, and [earned value management](https://akss.dau.mil/dag/GuideBook/IG_c11.3.1.asp) (EVM).

# CCA Compliance Element 8. Ensure that the acquisition is consistent with the DoD Information Enterprise policies and architecture, to include relevant standards.

* 1. CCA Element 8 requirements may be satisfied through (1) an Information Support Plan (ISP) with the required architecture; (2) an approved Joint Capability and Integrated Development System (JCIDS) capability development document with the required architecture;

(3) required architecture identified in Attachment 3 for systems not required to do an ISP; or (4) answers to the questions in Attachment 4 for closed systems that do not have architecture because the system has no interfaces (both AF and Joint). SAF/CNZA utilizes the checklist in Attachment 5 to assess the architecture for CCA compliance.

* 1. The requirements and procedures for developing an ISP are located in DoDI 8330.01 and the Joint Interoperability Test Command Interoperability Process Guide. If an ISP is required, preparation of the document should take place early in the program development process to meet the program schedule. Guidance on ISP preparation and requirements at each milestone and review protocols may be found at the Interoperability SharePoint site <https://cs2.eis.af.mil/sites/13157/default.aspx>.

**NOTE:** A Net-Ready Key Performance Parameter (NR KPP) Table is required when an ISP or JCIDS document is submitted for Element 8. In the CCA Compliance Table for Element 8, the Program Office must cite the document(s) used as proof of compliance with this element and its associated approval memorandum (e.g., JROCM or JCIDS approval memorandum; ISP approval memorandum; architecture and NR KPP Table; or questions answered from Attachment 4).

* 1. All DoD programs use one of the acquisition models identified in the Adaptive Acquisition Framework (Figure 1) of DoDI 5000.02. DoD Acquisition Executive Office (OSD Acquisition and Sustainment) developed separate instructions for each acquisition model. The instructions detail requirements for interoperability and CCA.
     1. For programs required to complete an interoperability certification in accordance with the DoD acquisition models, an ISP along with the required architecture (Attachment 3) is required for approval of CCA Element 8. Depending on the milestone of the program, the ISP can either be a draft or must be the final ISP. The final ISP is required during the milestone before the final decision to deploy the capability.
     2. For programs not required to complete an ISP for interoperability certification, development of the required architecture (identified in Attachment 3) along with the approved requirements document is the requisite submission. SAF/CNZA will review the architecture and ensure compliance with DoDAF 2.02 and make the final decision for approval of Element 8 of CCA.
     3. Programs that are not required to complete an ISP for interoperability certification and are self-contained (meaning no interfaces or connections to any other program) are not required to develop architecture for CCA Element 8. The PMO will submit the answer to the questions in Attachment 4 and provide a copy of its approved requirements document. SAF/CNZA will review the answers to the questions and make the final decision for approval of Element 8.
     4. Presented below is a breakdown of CCA Element 8 requirements for the different adaptive acquisition frameworks.
        1. Urgent Capability. There is no Element 8 requirement for these programs. Once a decision is made to make this capability a program of record, the program office will follow the guidance in accordance with its acquisition model.
        2. Middle Tier of Acquisition. A program’s architecture is the only requirement for Rapid Prototyping. An ISP (for programs that have interoperability certification requirements) and architecture are required for Rapid Fielding. If no ISP is required, architecture is required along with the program’s approved requirements document.
        3. Major Capability. An ISP and architecture is required at Milestone B and Milestone C submission for CCA for ACAT I, II, and III acquisition programs (non-DBS) with milestones (e.g., A, B, C) and interoperability certification requirements. Architecture and the program’s approved requirements document is required for CCA for programs without interoperability requirements.
        4. Software Acquisition. CCA will occur at Minimum Viable Capability Release (MVCR) for programs that will employ an agile software development strategy. During this stage, a program will provide architecture and complete an ISP (if there are interoperability certification requirements) for its submission. If an ISP is not required, architecture is required along with the program’s approved requirements document.
        5. Defense Business Systems. DoDI 5000.75 states that business systems are not required to complete an ISP, but are required to provide architecture and a NR KPP Table (for programs required to get an interoperability certification) along with an approved requirements document for Element 8 of CCA.

# CCA Compliance Element 9. Ensure that the program has a Cybersecurity Strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

* 1. A Cybersecurity Strategy (CSS) is required to address how cybersecurity is implemented in a program acquiring IT. The CSS is appended to the Program Protection Plan after its approval by the Component CIO or DoD CIO as applicable. In order to address the new DoD CIO cybersecurity guidance and template issued on July 8, 2021, the DAF CIO has revised the Air Force cybersecurity guidance and template (Version 3.0, September 2021). The complete template and guidance for preparing a CSS, a CSS Annex, a CSS Progress Summary, and other cybersecurity documentation is located on the *USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site,* [https://cs2.eis.af.mil/sites/10774/default.aspx.](https://cs2.eis.af.mil/sites/10774/default.aspx)
  2. A CSS is not required for Material Development Decisions. Cybersecurity requirements are addressed throughout the program life cycle, beginning pre-Milestone A, and incorporated into program design activities. A CSS developed in preparation for Milestone A is more general and contain a lesser level of detail than a CSS submitted to support subsequent Milestone decisions.
  3. The Program Manager, in accordance with DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014, assembles an RMF Team consisting of an Authorizing Official, Security Control Assessor, Information System Security Manager, and User Representative. Roles and responsibilities are outlined in AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)* 2 February 2017.
  4. The CSS describes how the program’s cybersecurity features comply with applicable DoD and AF policies, standards, and architectures, and describes the program’s Assess and Authorize approach. Describe the security features, practices, procedures, controls, and architecture of the system that enforce the Risk Management Framework.
  5. The requirements for a CSS (including NSSs) appear in:
     + 40 U.S. Code § 11302. Capital planning and investment control.
     + DoDD 5000.01, *The Defense Acquisition System*, November 20, 2007
     + DoDD 8500.1, *Cybersecurity*, 14 March 2014
     + DoDI 8510.01, *DoD Risk Management Framework (RMF) for DoD Information Technology*, 12 March 2014
     + DoDI 8580.1, *Information Assurance in the Defense Acquisition System*, 9 July 2004
     + DoDI 5000.02, *Operation of the Defense Acquisition System*, 7 January 2015, Incorporating Change 5, Effective October 21, 2019
     + DoDI 5000.75, *Business System Requirements and Acquisition*, 2 February 2017
     + Chairman of the Joint Chiefs of Staff (CJCSM) 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 9 February 2011
     + *DoD Acquisition Guidebook*
     + Federal Information Security Modernization Act (FISMA) of 2014, P.L. 113-283
     + AFPD 17-1, Information Dominance Government Management
     + AFI 17-130, Cybersecurity Program Management
     + AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)* 2 February 2017
     + AFMAN 17-1402, *Clinger-Cohen Act (CCA) Compliance*, 20 June 2018
  6. Program Managers should proactively monitor and address cybersecurity issues in the early stage of a program. Examine program and system characteristics to determine whether compliance with DoDI 8500.01 (*Cybersecurity*, 14 March 2014) is recommended or required and whether a CSS is required. Programs that do not involve the use of IT in any form have no cybersecurity requirements. However, Program Managers should examine programs carefully because many programs have IT embedded in the product or its supporting equipment, such as automatic test equipment. Programs that include IT always have cybersecurity requirements, and need to comply with DoDI 8510.01 if they are categorized as Air Force IT.
  7. Acquisitions of IT below the system level (e.g., IT products, IT services, Platform IT Components, Subsystems, etc.) are not subjected to the full process described in this Guide. However, IT below the system level has to be securely configured (in accordance with applicable DoD policies and security controls), documented in an assessment package and reviewed by the responsible Information System Security Manager (under the direction of the Authorizing Official) for acceptance or connection into an authorized computing environment (i.e., an authorized Information System or a Platform IT system). A CSS is required whether an investment is categorized as an IS or as Platform IT.
  8. All ACAT/BCAT Category I CSSs are approved by SAF/CNZ Chief Information Security Officer. For the Acquisition Category programs, the Program Manager submits the CSS for review and approval by the Authorizing Official/Authorizing Official Designated Representative at Milestone A; and updates and re-submits for review and approval at development request for proposal release decision, MS B, MS C, and Full Rate Production/Full Deployment Decision. Defense business systems submit the CSS for review and approval by the Authorizing Official/Authorizing Official Designated Representative prior to ATP decision points or contract awards. For Acquisition Category ID, IAM, IAC and Business Acquisition Category I submissions the DoD CIO is the approval authority, and the process for Acquisition Category/Business Acquisition Category I programs is provided on the *USAF Clinger-Cohen Act (CCA) Compliance Guidance SharePoint Site* [https://https://usaf.dps.mil/sites/10774/SitePages/Home.aspx.](https://https/usaf.dps.mil/sites/10774/SitePages/Home.aspx) The CSS and CSS approval memorandum should be cited on the final AF CCA Compliance Table.

# 10.0 CCA Compliance Element 10. Ensure, to the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments.

* 1. Under modular contracting, a system is acquired in successive acquisitions of interoperable increments that allow for the following: easier to manage, address complex IT objectives, not dependent of subsequent increments, take advantage of technology advancements and reduces risk through avoidance of custom-designed components. Documentation submitted for this element should describe the acquisition approach being followed and the relationship between each increment and the mission need and benefit associated with that increment. Program schedule and milestones should reflect phased successive implementation approaches. Each increment results in stand-alone functional capability; development in iterations or spiral development methodology, phased implementations, use of multiple contracts, and identification of “usable assets.”
  2. Office of Management and Budget Memoranda M-10-26 (“Immediate Review of Financial Systems IT Projects” dated June 28, 2010) recommends that agencies split projects into smaller, simpler segments with clear deliverables. Project segments should generally take no longer than 90 – 120 days to achieve specific project milestones. Although all specific milestones may not deliver functionality, all such milestones have to support the delivery of well-defined functionality. This approach simplifies planning, development, project management and oversight, and training. It reduces risk and allows changes in technology to be incorporated into later phases at lower costs.
  3. PMOs should seek to award contracts competitively, and ensure a "full and open" competition process as part of the Acquisition Strategy. If a sole source or limited competition is utilized, the PMO should (1) provide documentation that demonstrates why a full and open competition is not viable and (2) ensure that it adheres to Federal Acquisition Regulation Subpart 6.3, Defense Federal Acquisition Regulation Supplement Subpart 206.3, and Air Force Federal Acquisition Regulation Supplement 5306.3.

# 11.0 CCA Compliance Element 11. Register Mission-Critical and Mission-Essential systems with the DoD CIO.

* 1. Information Technology Investment Portfolio Suite (ITIPS) is the enterprise AF system of record for IT management data, and serves as the single AF repository for AF IT with the exception of Special Access Program/Special Access Required and other classified programs, which are addressed in sec 11.4 below. Information entered into ITIPS is migrated, if applicable, to the DoD Information Technology Portfolio Repository (DITPR). Once the registration process is completed, ITIPS and DITPR registration numbers are assigned if applicable to the investment. If possible, the ITIPS number should be obtained before the CCA package is submitted to the SAF/CNZA for Subject Matter Expert review. Please contact the ITIPS help desk for ITIPS registration assistance.
  2. Program Managers are responsible for ensuring that their programs are registered in ITIPS, and verifying the information in ITIPS is complete, current, and accurate. In order to register a program in ITIPS, a user account must be requested/established. To obtain access to ITIPS, program personnel have to complete DD Form 2875. The required forms, user guides, and additional information on the registration process may be found on the ITIPS SharePoint located at [https://cs2.eis.af.mil/sites/13057/ITIPS/default.aspx.](https://cs2.eis.af.mil/sites/13057/ITIPS/default.aspx)
  3. Once access is established and the registration process begins, there are several basic sets of registration and reporting requirements to be followed. All programs follow an initial registration process that addresses basic program information such as program name, certification and accreditation status, and project description in order to be assigned an ITIPS Registration Number. In the Core Data section of ITIPS, please ensure that the correct response is entered for Question Z11, Primary Mission Area. The entry on this question may impact some of the documentation required for CCA compliance. Guidance on Mission Area determination can be found in DoDI 8115.0, *Information Technology Portfolio Management*; AFI 17-110*, Information Technology Portfolio Management and Capital Planning and Investment Control;* and the Defense Acquisition Guidebook. In the Core Data section of ITIPS, also please ensure that the correct information is entered for IT Budget. Incorrect budget information will delay ITIPS approval.
  4. Programs undertaking CCA compliance must address the three questions located under Section 2 of the CCA tab. The three questions are G57 (IT Acquired), C23 (CCA Cert Required), and Q2 (Acquisition Category).
  5. Depending upon the nature of the program being registered, one might have to address other compliance areas such as Federal Information Security Management Act, Records Management, Information Support Plan, and Section 508. After the Program Manager has verified the information in ITIPS, the registration is reviewed and approved by the program’s Portfolio Manager, SAF/CNZA, and SAF/CNSG.
  6. Special Access Program/Special Access Required programs should be registered in the SAP registry. Please contact the Special Program Oversight Office in SAF/CNZC for SAP registry assistance.

# 12.0 Post-Implementation Review.

* 1. DoDI 5000.82 directs the Program Manager, in coordination with the IT functional sponsor and DoD Component CIO, is responsible for developing a plan and conducting a PIR for all fully deployed digital capabilities, including NSS. The PIR is to report the degree to which doctrine, organization, training, materiel, leadership, education, personnel, facilities, and policy changes have achieved the established measures of effectiveness for the desired capability. The PIR should be used to evaluate systems for effectiveness and efficiency and decide whether continuation, modification, or termination of the system is necessary to meet mission requirements. Lesson learned should be documented. The PIR documents may be submitted separately from the CCA compliance package. The documentation for PIRs for the six acquisition pathways are listed in DoDI 5000.82.
  2. Four activities are part of a successful PIR implementation.
     1. A draft plan for conducting the PIR is developed and then submitted to the SAF/CN at Milestone B, and a final plan is due at the last acquisition milestone – either MS C or Full Rate Production Decision Review/Full Deployment Decision Review (FRPDR/FDDR). The PIR itself is held after Initial Operational Capability but prior to Full Operational Capability.
     2. Conducting the PIR involves collecting measurement data, performing measurement analysis, and presenting the results so that the results of the review can be used to make decisions. Analysis, in the form of quantitative and qualitative indicators against the OBPMs, should be based on answering the question, "Did we get what we needed?"
     3. The PIR team should assess the extent to which the investment decision-making process was able to capture the warfighter's initial intent. The outputs of the analysis become the PIR findings. The findings should clearly identify the extent to which the warfighters received what was expected.
     4. Based on the PIR findings, the PIR team prepares a report and makes recommendations that can be fed back into the capabilities and business needs processes. The primary recipient of the report is the Sponsor who articulated the original objectives and OBPMs on which the program or investment was based. The results of the PIR can aid in refining requirements for subsequent increments. Recommendations may be made to correct errors, improve user satisfaction, or improve system performance to better match warfighter/business needs.

**ATTACHMENT 1**

**(NAME OF PROGRAM)**

**AIR FORCE CLINGER-COHEN ACT COMPLIANCE TABLE**

|  |  |
| --- | --- |
| **Actions Required to Comply With the CCA (Subtitle III of title 40 of U.S. Code** | **Applicable Program Documentation\*** |
| 1. Make a determination that the acquisition supports core, priority functions of the DoD. | * Initial Capabilities Document * IS Initial Capabilities Document * Urgent needrequirements documents * Business Plan or Capability Implementation Plan (for Defense Business Systems) |
| 2. Establish outcome-based performance measures linked to strategic goals. | * Initial Capabilities Document * IS Initial Capabilities Document, * Capability Development Document * Capability ProductionDocument * Analysis of Alternatives * Acquisition Program Baseline * AF Form 1067 |
| 3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of commercial off-the-shelf  technology. | * Initial Capabilities Document * IS Initial Capabilities Document * Concept of Operations * Analysis of Alternatives * Business Process Reengineering |
| 4. Determine that no private sector or government source can better support the function. | * Acquisition Strategy * Analysis of Alternatives |
| 5. Conduct an analysis of alternatives. | * Analysis of Alternatives * Market Research |
| 6. Conduct an Economic Analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a life-cycle cost  estimate | * Program Office Estimate * Service Cost Position * Program Economic Analysis with an ROI for Automated Information System Programs |
| 7. Develop clearly established  measures and accountability for program progress. | * Acquisition Strategy * Acquisition Program Baseline * Testing and Evaluation Master Plan |
| 8. Ensure that the acquisition is consistent with the DoD Information Enterprise policies and architecture, to include relevant standards. | * Capability Development Document Net-Ready Key Performance Parameters * Capability Production Document Net-Ready Key Performance Parameters * Information Support Plan * Attachment 3 and 4 of the Clinger-Cohen Act Implementation Guide |

|  |  |
| --- | --- |
| 9. Ensure that the program has a Cybersecurity Strategy that is consistent with DoD policies, standards  and architectures, to include relevant standards. | * Cybersecurity Strategy * Program Protection Plan |
| 10. Ensure, to the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future  increments. | * Acquisition Strategy |
| 11. Register Mission-Critical and Mission-Essential systems with the DoD  CIO. | * Information Technology Investment Portfolio Suite (ITIPS) Number * Special Access Program Registration Number |

\*The Applicable Program Documentation cited are examples of the most likely but not the only references for the required information. Other references may be used if they are more appropriate in addition to or instead of those cited. Include page(s) and paragraph(s), where appropriate. Urgent needs may cite the associated urgent needs documentation to demonstrate CCA compliance, e.g., the Course of Action and/or the network connection documentation.

**ATTACHMENT 2**

**CLINGER-COHEN ACT PROGRAM SUMMARY SHEET**

|  |  |
| --- | --- |
| **(NAME OF PROGRAM)** | |
| **INFORMATION REQUEST** | **RESPONSE** |
| Name of Program |  |
| Acquisition Category or Business Acquisition Category Designation  *(see DoDI 5000.02, Table 1 or DoDI 5000.75)* |  |
| Mission Area *(Warfighting, Defense Intelligence, Enterprise Information Environment, or Business)* |  |
| National Security Systems, National Security Systems Checklist *(If NSS, date approved or not approved)* |  |
| Special Access Program/Special Access Required (SAP/SAR) identification *(respond Yes or No)* |  |
| Period of Performance *(total lifecycle by FY)* |  |
| Lifecycle funding *(in $, with breakout of dev/mod and O&S)* |  |
| Milestone schedule *(denoting each program milestone, the dates for milestones already attained, and the dates for future milestones)* |  |
| Upcoming Milestone or Contract Award and Date |  |
| Name of Program Manager *(org/office symbol/ AFB/email/phone number)* |  |
| Name of Program Executive Officer *(org/office symbol)* |  |
| Name of Milestone Decision Authority *(title/org/ office symbol)* |  |
| Command or Functional Office *(org/office symbol)* |  |
| Program Description *(one to two paragraphs)* |  |
| Description of IT Capability or Modernization Effort  *(one to two paragraphs)* |  |

**ATTACHMENT 3**

**REQUIRED AND CONDITIONAL ARCHITECTURE VIEWPOINTS FOR CCA COMPLIANCE**

|  |  |
| --- | --- |
| ***REQUIRED* ARCHITECTURE VIEWPOINTS** | |
| **VIEWPOINT** | **DESCRIPTION** |
| **AV-1** | “Executive Summary” of the architecture. It will describe the Purpose, Scope, Perspective, etc. of the effort. It is not precisely tied to the architecture’s data elements, as are the other views. |
| **AV-2** | Data Dictionary. Purpose is to expand on the brief description of data elements used throughout the architecture. |
| **OV-1** | A graphical depiction of what the architecture is about and an idea of the performers and operations involved. |
| **OV-2** | Describes the Operational Performers within the scope of the architecture, and their need to communicate. |
| **OV-3** | Resource exchange between the Operational Performers. |
| **OV-5b** | Describes the Operational Activities within the scope of the architecture, the Operational Resources those Activities require, and what Operational Resources are created by the Activities. |
| **OV-6c** | Provides a time-ordered examination of the Resource Flows as a result of a particular scenario. |
| **SV-1** | Addresses the composition and interaction of System Performers. The SV-1 links together the operational and systems architecture models. |
| **SV-2** | Describes the precise specification of physical connections between systems. In network-centric environments, this will also describe the networks utilized by the systems. |
| **SV-5a** | Maps system functions (activities) to operational activities. |
| **SV-6** | Definition of the Resource exchanges between the System Performers. The SV-6 specifies the characteristics of the System Resource Flows with emphasis on resources crossing the system boundary. |
| **SV-7** | Set of system performance parameters (measures). |
| **StdV-1** | Standards Profile - list of implemented technical standards, rules, and guidelines.  *Note: If implemented standards appear in the StdV-2 and not the StdV-1 (e.g., as some have done for emerging standards that are currently implemented), then this information is also required.* |

|  |  |
| --- | --- |
| ***CONDITIONAL* ARCHITECTURE VIEWPOINTS** | |
| **VIEWPOINT** | **DESCRIPTION** |
| **DIV-2** | Logical Data Model. Documentation of the data requirements and structural business process (activity) rules.  *CONDITION: REQUIRED when critical Operational Resources are not clearly defined in the StdV-1, or when a standard Resource is used in a non-standard way.* |
| **DIV-3** | Physical Data Model. Physical implementation format of the Logical Data Model entities, e.g., message formats, file structures, physical schema.  *CONDITION: REQUIRED when critical System Resources are not clearly defined in the StdV-1, or when a standard Resource is used in a non- standard way.* |
| **SvcV-1** | Services Context Description – identifies services and their interconnections.  *CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.* |
| **SvcV-2** | Specifies resource flows exchanged between services, and may list protocol stacks.  *CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.* |
| **SvcV-4** | Depicts allocation of service functions and data flows between service functions (activities).  *CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.* |
| **SvcV-5** | Maps services (activities) to operational activities.  *CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.* |
| **SvcV-6** | Maps service data exchanges with associated measures and metrics. *CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.* |
| **SvcV-7** | Complete set of performance parameters (measures) of the services. *CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.* |

**ATTACHMENT 4**

**QUESTIONS TO BE ANSWERED FOR NON-ARCHITECTURE SYSTEMS**

|  |
| --- |
| **QUESTIONS** |
| 1. What does the system need to do? |
| 2. Who has the information needed by the system and to whom does the system need to give information? |
| 3. When does the system need to have those communications? |
| 4. What systems have the information in them? |
| 5. How is the system going to move the information? |
| 6. What system characteristics are needed to support the communications and what does the  system need to do? |
| 7. What are the data formats of the systems with which the system needs to exchange  information? |
| 8. What specs and standards is the system using to assure the systems can interoperate? |

**ATTACHMENT 5**

**ARCHITECTURE ASSESSMENT CHECKLIST FOR CCA COMPLIANCE**

|  |  |
| --- | --- |
| **QUESTIONS** | **EXPLANATION** |
| 1. Does the system require architecture development? | Architecture development is required for new capability development and modernization of capabilities that have been deployed. Legacy systems are not required to develop architecture for legacy capabilities, but are required to develop architecture for their new capabilities. (Reference DoDI 5000.02,  DoDI 8330.01, CJCSI 5123.01H, and AFI 17-140) |
| 2. Are the required architecture models provided? | Ensure the architecture artifacts are provided in accordance with Interoperability Process Guide v2.0 (required architecture in Attachment 3). (AV-1, AV- 2, OV-1, OV-2, OV-3, OV-5a/B, OV-6c, SV-1, SV-2,  SV-5a, SV-6, SV-7, StdV-1) (SvcVs required if a program has services) |
| 3. Are the architecture views consistent with the program’s DoD lifecycle stage in accordance with the Adaptive Acquisition Framework? | As the program progresses during their acquisition lifecycle, the architecture artifacts become more detailed with specific information for interfaces, security, and information attributes. The architecture is developed from the start of the program and  updated throughout the acquisition lifecycle. |
| 4. Is the architecture compliant with DoD and AF policies to interoperate with other systems  / services? If interoperability certification is required, is the program on track for certification? | The architecture contains enough data to define the characteristics the system needs to interoperate with other systems/services to achieve its required mission. The architecture must describe the required interfaces and the data and quality of service needed. This is used to create the development and operational test plans used by AF and Joint testers. If interoperability certification is required, the program must have an Information Support Plan that has started or  completed joint coordination. |
| 5. Does the architecture meet the DoDAF requirements in producing integrated  architecture views? | Architectural data elements are uniquely identified and consistently used across all products and views within the architecture. |

|  |  |
| --- | --- |
| 6. Are the technical architecture standards found in the StdV- 1 correct and current (mandated or active) in DoD  Information Technology Standards Registry (DISR)? | All standards come from approved standards depicted in DISR. Any deviation to use a retired or unapproved standard must be approved by the Air Force Chief Technology Officer. In other words, the current  technical standards should come from the set of “mandated” standards in DISR. |
| 7. If applicable, are the program’s emerging standards found in the StdV-  2? | Emerging standards are identified when a program utilizes newer standards during the development lifecycle. These standards should come from the set of  “emerging” standards found in DISR. |
| 8. Is the architecture consistent with the system/application description provided by the AV-1 and OV-1? | Compare the system’s/application’s supporting requirements document with the narrative of the OV-1 and information in the AV-1. Basically, are the high- level operations shown in the OV-1 and AV-1 reflected throughout the architecture and consistent with the  program’s requirements? |