BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-1402

20 JUNE 2018

Cyberspace

CLINGER-COHEN ACT (CCA) COMPLIANCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasibility restrictions on this publication

---

OPR: SAF/CIO A6XA

Certified by: SAF/CIO A6X, (Arthur G. Hatcher, SES)

Supersedes: AFMAN33-407, 24 October 2012

Pages: 15

This publication implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance, Governance, and Management*. It provides guidance for all Air Force military, civilians, and contractor personnel under contract by the Department of Defense (DoD) who are responsible for compliance and reporting for Subtitle III of Title 40 of the Clinger-Cohen Act (CCA) of 1996; Department of Defense Directive (DoDD) 5000.01, *The Defense Acquisition System* (12 May 2003); Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System*; DoDI 5000.74, *Acquisition of Services*; and DoDI 5000.75, *Business System Requirements and Acquisition*. This guidance clarifies the application of the CCA confirmation and compliance requirements to AF programs; delineates the AF CCA compliance and reporting process with clearly defined process steps; and provides the latest CCA requirements, guidance, and techniques for achieving CCA compliance.

This manual applies to all Air Force Active Duty Commands, Reserve, and Air National Guard units. This publication may not be supplemented or further implemented/extended Send recommended changes or comments to the Office of Primary Responsibility, Secretary of the Air Force, Chief, Information Dominance and Chief Information Officer, Policy and Resources Directorate, (SAF/CIO A6XA), 1800 Air Force Pentagon, Washington, DC 20330-1800, using AF Form 847, *Recommendation for Change of Publication*. Recommended changes or comments can also be sent via e-mail to **usaf.pentagon.saf-cio-a6.mbx.a6xa-workflow@mailbox.mil**. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS)

Records Disposition Schedule (RDS)". Tiering compliance requirements do not apply to this AFMAN 17-1402.

SUMMARY OF CHANGES

This rewrite incorporates the new CCA compliance requirements directed by the revised DoDI 5000.02, DoDI 5000.74, and DoDI 5000.75. The process for evaluating and reporting CCA compliance has been changed; the requirement for a CCA compliance report ("i.e., the narrative) has been eliminated; multiple memoranda signed by key managers associated with their respective area of authority for the program are to be submitted; and a Program Summary and memoranda signed by Program Managers are now required instead of a signature page in the CCA compliance report. Detailed information on compliance with the 11 CCA elements and updated guidance addressing cost, interoperability, cybersecurity, and the acquisition of services is presented in the Clinger-Cohen Act Implementation Guide.

1. Introduction.

1.1. This document provides guidance for compliance and reporting for the Clinger-Cohen Act (CCA) of 1996 (40 United States Code § 11101-11704, hereinafter referred to as "CCA"); DoDD 5000.01; DoDI 5000.02; DoDI 5000.74; and DoDI 5000.75. DoDI 5000.02 designates the Component CIO and the Milestone Decision Authority as the approval authorities for CCA. This AFMAN provides procedures for CCA implementation by AF Program Managers and the Chief, Information Dominance and Chief Information Officer of the Air Force (SAF/CIO A6) as directed in AFPD 17-1, *Information Dominance, Governance, and Management* (12 April 2016). The primary purpose of a successful CCA compliance review is to confirm for the Milestone Decision Authority that the program has successfully demonstrated compliance with the CCA. SAF/CIO A6XA records CCA compliance in the Air Force's Information Technology Investment Portfolio System which is then transmitted to the DoD Information Technology Portfolio Repository. A Glossary of References and Supporting Information is presented in **Attachment 1**.

1.2. The Clinger-Cohen Act is the principle Federal law on IT acquisition. Originally enacted as Public Law 104-106, *National Defense Authorization Act for Fiscal Year 1996,* Division E, Information Technology Management Reform, the law's primary purpose is to provide a framework for the role of the CIO in Federal agencies and describe how the CIO is to be involved in IT investments or IT acquisitions that support an agency's mission. The Clinger-Cohen Act directs the agency CIO to "advise the head of the agency regarding whether to continue, modify, or terminate a program or project" to ensure that IT is acquired and information resources are managed in a manner that implements the policies and procedures of CCA (40 USC § 1425, Agency Chief Information Officer). Implementation of CCA in the Air Force is the responsibility of the Chief, Information Dominance and Chief Information Officer of the Air Force (SAF/CIO A6). (The term "investment" is used here to identify an AF activity, product, or service that enables the acquisition, procurement, development, management, operation, lease, or closure of IT. Investment is used in the broadest sense, i.e., to include programs, projects, systems, business systems, family of systems, system of systems, and any other expenditures for IT or IT-related activities.)

1.3. CCA applies to all programs that acquire IT and/or IT Services. As a statutory requirement, CCA compliance is not subject to waiver. All programs acquiring IT (including technology refresh for programs in sustainment) need to undergo CCA compliance reporting (see Section 2.6 for further details on sustainment programs).

2. Roles and Responsibilities

2.1. Roles and responsibilities are delineated throughout the publication. Specific information on the roles of the Program Manager, SAF/CIO A6, and SAF/FM are embedded in specific sections throughout this publication.

3. CCA Coverage of Programs Acquiring IT.

3.1. DoDI 5000.02 directs that Enclosure 11 on "Requirements Applicable to All Programs Containing Information Technology (IT)" applies to IT, National Security Systems, and Information Systems as well as Automated Information Systems. The definitions of those terms are presented below.

3.1.1. IT " . . . is any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services, and related resources). IT is equipment used by the DoD directly or is used by a contractor under a contract with the DoD that requires the use of that equipment. IT does not include any equipment acquired by a federal contractor incidental to a federal contract."

3.1.2. National Security Systems ". . . as defined in 44 U.S.C. § 3552, are telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or, is critical to the direct fulfillment of military or intelligence missions. NSS do not include systems that are used for routine administrative and business applications (including payroll, finance, and personnel management applications)."

3.1.3. Information systems " . . . as defined in 44 U.S.C. § 3502, are a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

3.1.4. An Automated Information System, as defined in DoDI 5000.02, is "a system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. Excluded are computer resources, both hardware and software, that are an integral part of a weapon or weapon system; used for highly sensitive classified programs (as determined by the Secretary of Defense); used for other highly sensitive information technology (IT) programs (as determined by the DoD CIO); or determined by the Defense Acquisition Executive or designee to be better overseen as a non-Automated

Information System program (e.g., a program with a low ratio of research, development, and test and evaluation funding to total program acquisition costs or that requires significant hardware development)."

3.2. CCA is implemented through DoDI 5000.02, Tables 2 and 10 and Enclosure 11. CCA compliance is mandatory for "... all programs that acquire IT, including NSS, at any acquisition category (ACAT) level" per DoDI 5000.02, Enclosure 11, and for Defense Business Systems, per DoDI 5000.75, Table 1. Tables 2 and 10 in Enclosure 1 in DoDI 5000.02 lists the information requirements (statutory and regulatory) for all milestones and phases for all Acquisition Category programs and the basic requirements for CCA compliance, respectively.

3.3. Table 2 of DoDI 5000.02 directs that CCA compliance is statutory for all programs that acquire IT and regulatory for other programs. DoDI 5000.02 states that "For all programs that acquire IT, including NSS, at any acquisition category (ACAT) level, the Milestone Decision Authority will not initiate a program nor an increment of a program, or approve entry into any phase of the acquisition process that requires formal acquisition milestone approval, and the DoD Component will not award a contract for the applicable acquisition phase until: (1) The sponsoring DoD Component or program manager has satisfied the applicable acquisition phase-specific requirements of the CCA as shown in Table 10 in Enclosure 1 of this instruction; and (2) The Program Manager has reported CCA compliance to the MDA and the DoD Component Chief Information Officer (CIO), or their designee."

3.4. CCA compliance is undertaken when a program acquires IT. DoDI 5000.02 requires CCA compliance in time when a program is approaching its next Milestone Decision Review (Milestones A, B, and C, and Full Rate Production Decision/Full Deployment Decision or a major contract award consistent with DoDI 5000.02 and AFI 63-101/20-101, *Integrated Life-Cycle Management*). CCA compliance for Defense Business Systems occurs at the appropriate Authority to Proceed decision point, especially the Acquisition, Limited Deployment and Full Deployment Authority to Proceed decision points, as addressed in DoDI 5000.75, and in conjunction with specific processes designed for Defense Business Systems, such as the Organizational Execution Plan. There also may be inquiries or other processes that require the submission of CCA compliance documentation, such as AF Audit Agency or Inspector General requests.

3.5. DoDI 5000.02 (Table 2) states that "for IT programs employing an incremental development model (i.e., Model 3), the Program Manager will report CCA compliance at each Limited Deployment Decision Point." Program Managers managing Business Acquisition Category III Defense Business Systems can bundle selected Limited Deployment Decisions or releases into one CCA review in consultation with SAF/CIO A6XA and in conformance with the Model 3 approach described in DoDI 5000.02 (Sec 5c(3)(d)). The Program Manager may submit one CCA review package for all identified Limited Deployment Decisions or releases if the program maintains a stable schedule and all of the CCA documentation submitted in support of that approach addresses all activities associated with the multiple Limited Deployment Decisions.

3.6. AF programs in sustainment (not undertaking a technology refresh) are to be registered in the Information Technology Investment Portfolio System. A system or program in sustainment is one that spends Operations & Maintenance funds for continuing operations and current services, or sustainment-only activities. This type of system is not allocating or spending any funds on development, modernization and enhancement or for new capabilities, i.e., an activity that results in improved capability or performance of the baseline activity. The Office of Management and Budget refers to these systems or programs as steady-state.

3.7. Additional CCA guidance for programs that acquire contracted services is provided in DoDI 5000.74. Decisions on the approach taken for CCA compliance and whether an investment in IT services or the acquisition of contracted services is to be managed under DoDI 5000.74, DoDI 5000.75, or DoDI 5000.02 (as well as this AFMAN) are to be made in consultation with SAF/CIO A6. CCA compliance actions for the acquisition of contracted services should be conducted for entire programs rather than for each contract in an acquisition effort. Related contracts (such as software releases for a particular program) may be grouped together for CCA purposes.

3.8. Questions on the applicability of CCA compliance to a particular program or on statutory, regulatory, and milestone requirements for CCA are to be directed to the SAF/CIO A6XA Point of Contact. Although the Program Manager is responsible for implementing CCA compliance, the determination of whether CCA is applicable to a particular program is the responsibility of SAF/CIO A6.

4. CCA Compliance Reporting and Review.

4.1. CCA Compliance Reporting. CCA approval for Acquisition Category programs is achieved by verifying compliance with the 11 CCA elements that are identified in DoDI 5000.02, Table 10. For the purposes of reporting CCA compliance in the AF, the Program Manager will utilize the AF CCA Compliance Table in **Attachment 2** of this AFMAN to report CCA compliance. The Program Manager will list the documents that demonstrate compliance with the 11 CCA elements on the AF CCA Compliance Table. For most AF programs that acquire IT, the AF utilizes a two-track process for reporting CCA compliance, regardless of program size, Acquisition Category, or mission area (see paragraphs **3.2** and **3.3** below). The exceptions to this compliance requirement are:

4.1.1. Defense Business Systems that conduct CCA compliance per this AFMAN and DoDI 5000.75 guidance and Acquisition of Services programs that conduct CCA compliance per DoDI 5000.74;

4.1.2. Defense Business Systems designated as Joint systems, which are approved for CCA by both the AF CIO and the DoD CIO;

4.1.3. Special Access Program/Special Access required or other classified programs, for which the documentation for all 11 CCA elements is reviewed by SAF/CIO A6 and SAF/FM (cost only); and

4.1.4. IT Special Interest programs, that may be any AF program, project, or activity that the AF CIO designates as such, regardless of where that program is in its program lifecycle (including technology projects, service contracts, supply contracts, or other IT investments that have not been designated as an Acquisition Category program and may be considered acquisition programs), and for which the CCA compliance process determinations are made on a case-by-case basis.

4.2. The first track requires the Program Manager to report compliance for the documents listed as evidence of compliance with CCA elements 1, 2, 3, 4, 5, 7, and 10. The Program Manager shall assess the compliance documentation to ensure that it addresses the information requirements as described in the CCA Implementation Guide on the CCA SharePoint site. The Program Manager is responsible for ensuring that the program has met the requirements of CCA. Program Managers should be familiar with the statutory, regulatory, and milestone requirements for programs that acquire IT and IT-related investments in DoDI 5000.02, DoDI 5000.74, and DoDI 5000.75, as noted in paragraphs **2.1** and **2.2** of this AFMAN.

4.3. The second track is coordinated by SAF/CIO A6XA. Although the Program Manager sends the links or documentation for all 11 CCA elements to SAF/CIO A6XA so that it may be checked for due diligence, the SAF/CIO A6 CCA review process will address the compliance documentation for only CCA elements 6, 8, 9, and 11 (except the Information Support Plan, which is submitted to the Global Information Grid Technical Guidance Federation system). SAF/FM retains approval and policy responsibility for element 6 and SAF/CIO A6 retains approval and policy responsibility for elements 8, 9, and 11 of the CCA compliance table referenced in **Attachment 2** of this AFMAN. Please see the Clinger-Cohen Act Implementation Guide for more information on required documentation.

4.4. The Program Manager or the Program Management Office Point of Contact notifies the SAF/CIO A6XA Point of Contact that a CCA compliance package is forthcoming and then sends the following to SAF/CIO A6XA:

4.4.1. The AF CCA Compliance Table (**Attachment 2**);

4.4.2. Compliance documentation or links to compliance documentation for all CCA elements on the CCA Compliance Table (except for the Information Support Plan);

4.4.3. A CCA transmittal memorandum signed by the Program Manager (see the template in **Attachment 3**)

4.4.4. The CCA Program Summary Sheet (see the template in **Attachment 4**).

4.5. The SAF/CIO A6XA CCA Point of Contact and be contacted directly or through the CCA Workflow box **usaf.pentagon.saf-cio-a6.mbx.af-cio-clinger-cohen-compliance@mail.mil**. The *Defense Acquisition Guidebook* **https://dag.dau.mil/Pages/Default.aspx** and the *USAF Clinger-Cohen Act (CCA) Compliance Guidance Sharepoint Site* **https://cs2.eis.af.mil/sites/10774/default.aspx** contain authoritative sources, information, and templates to aid in preparing a CCA compliance package and in learning about DoDI 5000.02 and IT acquisition.

4.6. The CCA compliance documentation for CCA elements 6, 8, and 9 is reviewed by the CCA Subject Matter Experts and the program's registration in the Information Technology Investment Portfolio System registration is approved by SAF/A6X. SAF/CIO A6XA consolidates the Subject Matter Experts' comments and sends them to the Program Manager or Program Management Office Point of Contact if there are issues that require resolution. SAF/CIO A6XA employs a rigorous, consistent, and repeatable review protocol.

4.7. If a Program Manager does not use the documents listed in the Applicable Program Documentation column of the AF CCA Compliance Table (**Attachment 2**) to demonstrate compliance, the Program Manager may cite other documents, actions, or events as proof of compliance. Original reports, memoranda, spreadsheets, and architectural drawings may be used but the citation should be an original document, not a secondary source. For example, an answer to a question in the Information Technology Investment Portfolio System is not a compliant response.

4.8. The supporting documents that a program lists in the Applicable Program Documentation column shall be (1) supplemented by information about where to find the particular paragraph(s), section(s), figure(s), and/or table(s) in the referenced document; (2) stand-alone or self-contained documents (i.e., not embedded), to the extent possible; and (3) provided to SAF/CIO A6XA as part of the CCA compliance package. Documents in draft form may be sent to SAF/CIO A6XA at the start of the CCA review process but must be finalized before the Program Manager signs the CCA assertion memorandum (**Attachment 5**) and sends that memorandum to SAF/CIO A6XA.

4.9. Where applicable and relevant to the upcoming milestone or contract award, documents may be re-used. Re-used documentation should specifically address the program under CCA review. New or updated documentation may be needed when the (1) information in the original documentation needs to be updated; (2) when the information in the original document does not adequately address the current effort; or (3) original document did not adequately address the CCA requirement.

4.10. Although DoDI 5000.02 allows for some CCA supporting documents to be subsumed into alternate acquisition documentation (i.e., the Analysis of Alternatives and Economic Analysis for Milestone A), the Cybersecurity Strategy and the Information Support Plan, or alternate architecture documentation, are to be provided to SAF/CIO A6XA as stand-alone documents prepared in accordance with this AFMAN and other specialized guidance documents. DoDI 5000.75 allows for some flexibility in the Implementation Plan.

4.11. Programs that are applying to be National Security Systems should fill out the National Security Systems checklist (relying upon the guidance in NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*), and submit the signed checklist to SAF/CIO A6XA as soon as possible.

4.12. The Program Manager is responsible for ensuring that all CCA compliance documentation is submitted and approved in time for the scheduled milestone review or contract award. Program Managers are encouraged to contact the CCA Point of Contact in SAF/CIO A6XA as early in the process as possible before the next milestone review so they can develop an ongoing dialogue, increase and improve the opportunities for early feedback, and facilitate access to the Subject Matter Experts for assistance. The Program Manager should submit the CCA compliance documentation for CCA elements 6, 8, 9, and 11 to

SAF/CIO A6XA at least four months before the milestone review or contract award is scheduled to allow sufficient time for review and revisions. Documentation should be sent by e-mail to the SAF/CIO A6XA CCA Point of Contact or by using the U. S. Army Aviation and Missile Research Development and Engineering Center Safe Access File Exchange tool **https://safe.amrdec.army.mil/safe**.

4.13. At the completion of the CCA compliance review process, the Program Manager sends to SAF/CIO A6XA a CCA Assertion Memorandum that states that all 11 CCA elements are CCA compliant in accordance with this AFMAN and either DoDI 5000.02, DoDI 5000.74, or DoDI 5000.75 (Attachment 5).

4.14. The Chief, Information Dominance and Chief Information Officer will sign a CCA confirmation memorandum, signifying that the program is compliant with this AFMAN for the particular milestone, contract award, or Authority to Proceed decision point. SAF/CIO A6XA deposits the confirmation memorandum into the Information Technology Investment Portfolio System, wherein the approval is transmitted to the DoD Information Technology Portfolio Repository, completing the CCA compliance process for that particular milestone or contract award activity.

BRADFORD J. SHWEDO, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION.

References

Air Force Policy Directive (AFPD) 17-1, *Information Dominance, Governance, and Management*, April 12, 2016

Clinger-Cohen Act (CCA) of 1996, Title 40

Department of Defense Directive (DoDD) 5000.01, *The Defense Acquisition System* (12 May 2003)

Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System* (7 January 2015, Incorporating Change 3, August 10, 2017)

DoDI 5000.74, *Acquisition of Services* (January 5, 2016)

Air Force Manual (AFMAN) 33-363, *Management of Records*, 1 March 2008

DoDI 5000.75, *Business System Requirements and Acquisition* (2 February 2017)

CCA Implementation Guide, CCA SharePoint site

AFI 63-101/20-101, *Integrated Life-Cycle Management*, 9 May 2017

DoD Acquisition Guidebook

Federal Information Security Management Act (FISMA) Public Law (PL) 107-347

DoDI 8580.1, *Information Assurance in the Defense Acquisition System*, 9 July 2004

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*

Prescribed Forms

None

Adopted Forms.

AF Form 847, *Recommendation for Change of Publication*

Attachment 2

AIR FORCE CLINGER-COHEN ACT COMPLIANCE TABLE

Table A2.1. Air Force Clinger-Cohen Act Compliance Table.

(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 (Reference (p)))	**Applicable Program Documentation**
1. Make a determination that the acquisition supports core, priority functions of the DoD.	Initial Capabilities Document, IS Initial Capabilities Document, or urgent need requirements documents
2. Establish outcome-based performance measures linked to strategic goals.	Initial Capabilities Document, IS Initial Capabilities Document, Capability Development Document, Capability Production Document, Analysis of Alternatives, Acquisition Program Baseline
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
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	Component Cost Estimate, Component 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, Sec 9.4 Alternate Architecture Report (see 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, Risk Management Framework Security 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 Registration Number

Attachment 3

PROGRAM MANAGER CLINGER-COHEN ACT TRANSMITTAL MEMORANDUM TEMPLATE

Figure A3.1. Program Manager Clinger-Cohen Act Transmittal Memorandum Template.

_____
(date)

MEMORANDUM FOR SAF/CIO A6XA

SUBJECT: CCA Transmittal Memorandum for _____(Name of Program)_____

Attached to this memorandum is the Air Force Clinger–Cohen Act Compliance Table and supporting documentation for the ____(Name of Program)____ Program. I have reviewed the attached documentation and determined that it is ready for assessment and confirmation. Additional information on our program is provided in the attached CCA Program Summary Sheet. My Point of Contact for CCA compliance is (name, e-mail, phone number).

_____
(Signature of Program Manager)
(add signature block)

Attachment 4

AIR FORCE CLINGER-COHEN ACT PROGRAM SUMMARY SHEET

Table A4.1. Air Force 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)*	
For National Security Systems, National Security Systems Checklist (date approved or not approved)	
Period of Performance *(total lifecycle by FY)*	
Lifecycle funding *(in $, with breakout of Research, Development, Test, & Evaluation (RDT&E); Development/Modification (Dev/Mod); and Operation & Maintenance (O&M))*	
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/email/phone number)*	
Name of Program Executive Officer *(org/office symbol)*	
Name of Milestone Decision Authority *(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 5

PROGRAM MANAGER CLINGER-COHEN ACT ASSERTION MEMORANDUM TEMPLATE

Figure A5.1. Program Manager Clinger-Cohen Act Assertion Memorandum Template.

_____
(date)

MEMORANDUM FOR SAF/CIO A6XA

SUBJECT: CCA Assertion Memorandum for _____(Name of Program)_____

SUBJECT: Clinger-Cohen Act Compliance Assertion for ___(Name of Program)___

I have reviewed the Clinger-Cohen Act compliance documentation for all 11 Clinger-Cohen Act Elements for this Program and I assert that the documentation is compliant with AFMAN 17-1402 and DoDI (select 5000.02, 5000.74, or 5000.75).

_____
(Signature of Program Manager,
Name of Program Office,
Command, or Functional