DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 630-225-9*

INFORMATION SERVICES

Clinger-Cohen Act (CCA) Compliance for Information Technology (IT)

1. **Purpose.** This Instruction prescribes policy and assigns responsibilities and duties for Clinger-Cohen Act (CCA) compliance for information technology (IT). It also provides procedures for CCA compliance confirmation for full and abbreviated levels of IT acquisition.

2. **Applicability.** This Instruction applies to all DISA activities and the Joint Force Headquarters - Department of Defense Information Network (JFHQ-DODIN).

3. **Scope.** This Instruction applies to DISA and JFHQ-DODIN IT programs, initiatives, and services.

4. **Authority.** This Instruction is published in accordance with the authority contained in the Clinger-Cohen Act (CCA) of 1996; DoD Directive (DoDD) 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), 17 March 2016, as amended; DoD Instruction (DoDI) 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004; DoDI 5000.02, Operation of the Defense Acquisition System, 7 January 2015, as amended; DoDI 5000.75, Business Systems Requirements and Acquisition, 2 February 2017; and DoDD 5105.19, Defense Information Systems Agency, 25 July 2006.

5. **Background.** The Clinger-Cohen Act (CCA) of 1996 is the United States Federal Law that increases the roles and responsibilities of an agency Chief Information Officer (CIO) and provides the foundation for the acquisition, use, and disposition of information technology (IT). The CCA, which encompasses the Information Technology Management Reform Act (ITMRA) of 1996, Division E of Public Law 104-106, and the Federal Acquisition Reform Act (FARA) of 1996, provides the framework for the role of a CIO in federal agencies and their involvement in IT investments or IT acquisitions that support an agency's mission. The compliance of CCA is governed under the laws, rules, and policies of the Clinger-Cohen Act of 1996 and DoDI 5000.02, Operation of the Defense Acquisition System (authority documents).

6. **Objective**. This Instruction serves to institutionalize and streamline the Agency's review and oversight process for confirming CCA compliance of IT programs.

7. **General**. The CCA mandates the Federal Government improve the acquisition and management of IT resources. It also gives agencies the responsibility for making improvements in mission performance and service delivery to the public by strategically applying IT. Procedures for verifying compliance with the CCA are provided in the DISA Clinger-Cohen Act Compliance Guide. (Information as to how to locate the guide is provided in paragraph 13.)

8. **Definitions**. Definitions are provided in the enclosure.

9. **Policy**. In accordance with DoDI 5000.02, Operation of the Defense Acquisition System, and DoDD 8000.01, Management of the Department of Defense Information Enterprise (DoD IE) (authority documents), CCA compliance is required for all DISA IT acquisitions including acquisition of IT services. The IT programs that are required to be CCA compliant are defined in Enclosure 1, Table 2, and Enclosure 11, Section 3, of DoDI 5000.02. The programs include all IT acquisition programs, Major Defense Acquisition Programs (MDAP), Major Automated Information Systems (MAIS), and all Acquisition Category (ACAT) IT programs.

9.1 An IT program must have an Agency-signed CIO CCA Confirmation Memorandum before seeking acquisition Milestone Decisions. Program initiation or entry into any phase of the acquisition process that requires formal milestone approval will not be approved by the Milestone Decision Authority (MDA), and the Agency will not award a contract for the applicable acquisition phase until the CIO provides confirmation of CCA compliance.

9.2 A full or abbreviated review of a program with IT acquisition requirements will be required depending on the estimated cost for the life cycle and the fiscal year. (Refer to paragraph 10 for the procedures for CCA confirmation for full and abbreviated levels of IT acquisition.)

9.3 An IT program and its component systems or subprograms may be covered by the higher-level program's CIO CCA Confirmation Memorandum.

9.4 An IT program and/or acquisition of service (AoS) requiring frequent acquisition actions should request from the CIO a Blanket Waiver Memorandum for the program or contract to avoid having each acquisition action go through a complete CCA validation. (Renewal of the Blanket Waiver Memorandum from the CIO is to be requested annually by the Program Manager (PM) before the beginning of the next fiscal year.)

9.5 The Management Information Decision Support (MIDS) tool, or subsequent Agency-approved tool, shall be used by all Agency personnel responsible for IT programs to document CCA compliance of programs.

10. **Procedures for CCA Confirmation for Full and Abbreviated Levels of IT Acquisition.**

10.1 Programs with IT acquisition requirements of $10 million or more for the life cycle or $5 million or more for any fiscal year require a full review. The full review will involve the following actions:

10.1.1 Submission of a completed Clinger-Cohen Act (CCA) Compliance Checklist by the IT PM to the DISA CCA Compliance Office. (Refer to paragraph 13 as to location of the checklist.)

10.1.2 Submission of supporting documentation by the PM to a folder or location designated by the CCA Compliance Office.

10.1.3 Review and assessment of supporting documentation by the office of the CIO with the support of appropriate subject matter experts (SMEs).

10.1.4 Review of SME assessment results by the PM and submission of a signed CCA cover letter signed by the CCA Compliance Officer and the IT PM.

10.1.5 Review of a completed CCA assessment package by the CIO and a signed CIO CCA Confirmation Memorandum.

10.2 Programs with IT acquisition requirements estimated to be less than $10 million for the life cycle of the requirement and less than $5 million each fiscal year will follow an abbreviated review process. The review will involve the following actions:

10.2.1 Submission of a completed CCA Compliance Checklist by the PM to the CCA Compliance Office. (Refer to paragraph 13 as to location of the checklist. The program office is to make available any document referenced in the checklist to the CCA Compliance Office, if audited.)

10.2.2 Review of the program's CCA Compliance Checklist by the CCA Compliance Officer and a signed CIO CCA Confirmation Memorandum.

11. **Responsibilities.**

11.1 **Chief Information Officer (CIO).** The CIO serves as the office of primary responsibility to provide oversight and ensure CCA compliance within the Agency, in accordance with statutory and regulatory requirements. The CIO will:

11.1.1 Provide policy and guidance to Agency personnel involved in the acquisition, procurement, governance, and operation of IT.

11.1.2 Develop processes for Agency personnel that will ensure programs, IT services, systems, and contracts are compliant with the CCA prior to the award of contracts and Milestone Decision Reviews.

11.1.3 Provide a signed CCA Confirmation Memorandum to the CCA PM for IT programs that have complied with all CCA statutory requirements.

11.1.4 Appoint a CCA Compliance Officer to implement and manage the daily functions and processes required to obtain and maintain compliance integrity across the Agency.

11.1.5 Provide advice and other assistance to the Director, DISA; the Component Acquisition Executive (CAE); and other Agency senior management personnel to ensure IT is acquired and information resources are managed in a manner that implements the policies and procedures consistent with chapter 35 of title 44, United States Code.

11.1.6 Serve as the final approval authority of CCA Compliance Memorandums and Blanket Waiver Memorandums, as appropriate.

11.2 **Directors, Executives, Milestone Decision Authorities (MDAs), Program Executive Officers (PEOs), Commanders, and Chiefs of Major Organizational Elements.** These individuals will:

11.2.1 Utilize tools and processes to ensure programs, IT services, and contracts are compliant with the CCA prior to the award of contracts and Milestone Decision Reviews.

11.2.2 Support the CIO in ensuring assigned programs, initiatives, IT services, and other IT acquisitions are compliant with the CCA prior to milestone or key decision reviews.

11.2.3 Provide SMEs to assist in reviewing documents, as needed, for the execution of CCA compliance.

11.2.4 Ensure all DISA programs are entered into the Management Information Decision Support (MIDS) tool, or a subsequent Agency-approved tool, for documenting CCA compliance.

11.3 **Component Acquisition Executive (CAE)**. The CAE will:

11.3.1 Provide support to the CIO to ensure programs, initiatives, IT services, and other IT acquisitions are compliant with the CCA prior to milestone or key decision reviews.

11.3.2 Provide an annual listing of acquisition programs to the CIO to assist in the process of determining programs requiring CCA compliance.

11.3.3 Provide policy requiring PMs, PEOs, and AoS Managers to utilize MIDS, or a subsequent Agency-approved tool, for situational awareness and CCA documentation support.

11.4 **Director for Procurement Services Directorate (PSD)/Defense Information Technology Contracting Organization (DITCO).** The Director, PSD, will utilize tools and processes to ensure programs, IT services, and contracts are compliant with the CCA and, when appropriate, validate confirmation with the office of the CIO prior to the award of all IT contracts.

12. **Duties.**

12.1 **Clinger-Cohen Act (CCA) Compliance Officer.** The CCA Compliance Officer will:

12.1.1 Manage the process for review of CCA compliance approval request packages.

12.1.2 Provide guidance and assistance to PMs and their staffs on CCA statutory requirements and the process for CCA compliance approval.

12.1.3 Provide controlled folders in the CCA Library for PMs to load the documents required for assessments of their programs.

12.1.4 Review all documentation submitted by PMs for CCA confirmation of their respective programs.

12.1.5 Work with the appropriate SMEs for timely review of program documentation to determine CCA compliance.

12.1.6 Provide each PM a cover letter of acknowledgement of combined SME assessments to be signed and returned to CCA Compliance Officer.

12.1.7 Prepare completed CCA review packages, including the SME assessments, signed PM CCA Compliance Checklist, signed PM cover letter, and CIO CCA Confirmation Memorandum, for review and signature.

12.1.8 Provide a copy of the signed CIO CCA Confirmation Memorandum to the PM for the PM records.

12.1.9 Delete supporting acquisition documents from the CCA Library after an assessment has been completed.

12.1.10 Provide formal training on the process for compliance with the CCA statutory requirements, including the use of the MIDS tool, or subsequent Agency-approved tool, for CCA compliance.

12.1.11 Conduct random audits, when necessary, of programs that have been confirmed to be CCA compliant and are below the threshold of less than $10 million for the life cycle of the program or $5 million per fiscal year.

12.1.12 Maintain a record of compliant CCA packages. (Package is to include a signed CIO Confirmation Memorandum, combined SME assessment documents, cover letter signed by the PM acknowledging receipt of the combined SME assessments, signed PM Compliance Checklist submitted by the PM, and Blanket Waiver Memorandum, if applicable.)

12.1.13 Obtain a list of Agency programs from the office of the CAE to help facilitate the process of determining CCA compliance.

12.2 **Information Technology (IT) Program Manager (PM).** An IT PM will:

12.2.1 Report CCA compliance through the Program Executive Office (PEO) to the Milestone Decision Authority (MDA) and the CIO prior to Milestone Decision Reviews.

12.2.2 Ensure all IT programs under their purview are CCA compliant, in accordance with Enclosure 1, Table 9, and Enclosure 11 of DoDI 5000.02, and submit CCA confirmation request packages at least 8 weeks prior to a required acquisition action or proof that CCA compliance has been confirmed.

12.2.3 Initiate the CCA assessment request by providing the required information using a CCA Compliance Checklist. (Refer to paragraph 13 as to the location of the checklist.)

12.2.4 Provide all pertinent documents to the CCA Compliance Office on a timely basis for SME assessments.

12.2.5 Sign an Assessment Results cover letter, provided by the CCA Compliance PM, acknowledging receipt and concurrence with the SMEs assessments.

12.2.6 Maintain copies of the signed CCA Confirmation Memorandum and any applicable CCA Blanket Waiver Memorandum for proof of CCA compliance when submitting acquisition packages.

12.2.7 Attend (PMs and designated personnel) the CIO-provided CCA training on an annual basis.

12.2.8 Ensure programs within their organizations use MIDS, or subsequent Agency-approved tool, for documenting CCA compliance.

12.2.9 Utilize the MIDS tool and CCA processes to ensure programs, IT services, and contracts are compliant with CCA prior to the award of contracts and Milestone Decision Reviews.

13. **Guidance and Resources.** Guidance and resources pertaining to CCA compliance for IT acquisition, to include the DISA CCA Compliance Guide and the CCA Compliance Checklist, are located on the CCA Webpage, which is accessed via the Department of Defense Enterprise Portal Service (DEPS) Dateline DISA. The drop down menus are Communities, DISA CIO Community of Practice (CoP), and Clinger-Cohen Act.

BARNHART.BRADLEY.WILLIAM.1140635789
Digitally signed by BARNHART.BRADLEY.WILLIAM.1140635789
Date: 2018.11.01 20:29:51 -04'00'

Enclosure a/s

BRADLEY W. BARNHART
Colonel, USAF
Chief of Staff

SUMMARY OF SIGNIFICANT CHANGES. This revision updates the dollar threshold from 1 million over the fiscal year to 5 million over the fiscal year and 5 million over the life cycle of the program to 10 million over the life cycle of the program. The responsibilities and duties have been updated.

---

*This Instruction replaces DISAI 630-225-9, 22 December 2014.
OPR: OC OCM4 - https://disa.deps.mil/disa/org/cia/CI21/CCA/SitePages/Home.aspx
DISTRIBUTION: Intended for public release.

Enclosure

DEFINITIONS

Acquisition Program. A directed, funded effort designed to provide a new, improved, or continuing materiel, weapon, or information system or service capability in response to a validated operational or business need. Acquisition programs are divided into different categories that are established to facilitate decentralized decision-making, execution, and compliance with statutory requirements. Technology projects are not acquisition programs.

Acquisition Category (ACAT). Categories established to facilitate decentralized decision-making and execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures.

Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR). The authoritative source for data regarding information technology (IT) systems. It is a comprehensive inventory of DoD's mission critical and mission essential IT systems and their interfaces and contains basic overview information regarding all DoD IT systems to include system names, acronyms, descriptions, sponsoring component, approval authority, points of contact, and other basic information required for any analysis of DoD inventory, portfolios, or capabilities.

Information Resources. Personnel, equipment, funds, and technology related to IT.

Information System. Infrastructure by which information resources are used to fulfill the role of IT.

Information Technology (IT). As defined in title 40 of U.S. Code, 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. IT is equipment used by DoD directly or is used by a contractor under a contract with DoD that requires the use of that equipment. IT does not include any equipment acquired by a federal contractor incidental to a federal contract.

Major Automated Information System (MAIS) (ACAT IAM or IAC). A system that is designated by the DoD Chief Information Officer (CIO) as a MAIS or estimated to require program costs in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life-cycle costs in excess of $378 million in FY 2000 constant dollars. MAISs do not include highly sensitive classified programs (as determined by the Secretary of Defense) or tactical communication systems. For the purpose of determining whether AIS is a MAIS, the following will be aggregated and considered a single AIS: the separate AISs that constitute a multi-element program, the separate AISs that make up an evolutionary or incrementally developed program, and the separate AISs that make up a multi-DoD Component AIS program.

Major Defense Acquisition Program (MDAP) (ACAT ID or IC). An acquisition program that is not a highly sensitive classified program (as determined by the Secretary of Defense) and that is designated by the dollar value for all increments of the program; estimated by the Defense Acquisition Executive (DAE) to require an eventual total expenditure for research, development, and test and evaluation (RDT&E) of more than $480 million in fiscal year (FY) 2014 constant dollars or, for procurement, of more than $2.79 million in FY 2014 constant dollars. The estimate will consider all blocks that will make up an evolutionary acquisition program (to the extent that subsequent blocks can be defined).

Milestone Decision Authority (MDA). The designated individual with overall responsibility for a program. The MDA will have authority to approve entry of an acquisition program into the next phase of the acquisition process and will be accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting.

Mission Critical Information System. A system that meets the definition of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of "mission critical" should be made by a Component Head, a Combatant Commander, or their designee.) A "mission critical information technology system" has the same meaning as a "mission critical information system."

Mission Essential Information System. A system that meets the definition of "information system" in the Clinger-Cohen Act that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of "mission essential" should be made by a Component Head, a Combatant Commander, or their designee). A "mission essential information technology system" has the same meaning as a "mission essential information system."

National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications (40 U.S.C. §11 103(a)(l)).

Portfolio Manager. An individual who manages a portfolio of selected groupings of IT investments (e.g., projects) to achieve a mission capability.

Program. A directed effort that provides a new, improved, or continuing material, weapon, or information system or service capability.

Program Manager (PM). The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment (while in the development phase) to meet the end user's operational needs. A PM is accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority (MDA).

Services. Performance-based manpower requirements that are identified with measurable outcomes and are properly planned and administered to achieve the intended results. Services include, but are not limited to, IT services, telecommunications, program and project support services, operational support services, acquisition consulting services, and technical support services.