



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 630-225-9*

DEC 22 2014

INFORMATION SERVICES

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

- 1. Purpose.** This Instruction prescribes policy and assigns responsibilities for confirming Clinger-Cohen Act (CCA) compliance for information technology (IT) acquisitions.
- 2. Applicability.** This Instruction applies to all DISA activities.
- 3. Scope.** This Instruction applies to acquisitions of IT including under DISA programs, projects, initiatives, services, and other acquisition matters.
- 4. Authority.** This Instruction is published in accordance with the authority contained in Subtitle III of Title 40 of the United States Code; DoD Directive (DoDD) 5000.01, The Defense Acquisition System, 12 May 2003; Interim DoD Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, 25 November 2013; DoDD 8000.01, Management of the Department of Defense Information Enterprise, 10 February 2009; DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004; and DoDD 5105.19, Defense Information Systems Agency, 25 July 2006;
- 5. Objective.** This Instruction serves to institutionalize and streamline the Agency's review and oversight process for confirming that IT acquisitions achieve compliance with Subtitle III of Title 40 of the United States Code, 40 U.S.C. 11101 et seq. (hereinafter referred to as the Clinger-Cohen Act [CCA]).
- 6. General.** The CCA mandates that 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 through strategically applying IT. Procedures for verifying compliance with the CCA are provided in the DISA Clinger-Cohen Act Compliance Guide, Version 1.0, December 2011. (The DISA Clinger-Cohen Act Compliance Guide is located at <https://disa.deps.mil/disa/org/cia/CI%20Documents/Clinger-Cohen%20Act/Guidances,%20Policies,%20Instructions/CCA%20Compliance%20Guide/DISA%20CCA%20Guide%20v21.doc>.)
- 7. Definitions.** Definitions are provided in the enclosure.

8. Policy.

8.1 In accordance with Interim DoDI 5000.02 and DoDD 8000.01 (authority documents), CCA compliance is required for all DISA IT acquisitions including acquisition of IT services.

8.1.1 For DISA IT acquisitions when the total cost of all contracts for the acquisition is estimated at \$5 million or more for all years or \$1 million or more for any fiscal year, compliance with CCA will be confirmed by the Principal Director for Enterprise Information Services (EIS)/Chief Information Officer (CIO).

8.1.2 For DISA IT acquisitions when the total cost of all contracts for the acquisition is estimated below \$5 million for all years and below \$1 million each fiscal year, compliance with CCA will be confirmed by the Program Manager (PM), Project Lead (PL), or Service Manager (SM) to the Principal Director, EIS/CIO.

8.1.2.1 A CCA compliance letter will be used by the PM, PL, or SM to capture and present the Agency's CCA compliance to the Principal Director, EIS/CIO. (Guidance on the compliance letter is provided in paragraph 11.)

8.1.2.2 All IT acquisitions that are confirmed by the PM, PL, or SM will be subject to audit at the discretion of the Principal Director, EIS/CIO, to ensure CCA has been addressed appropriately.

8.2 DISA is prohibited from awarding contracts for the acquisition of IT until the Agency CIO confirms CCA compliance has been accomplished, as detailed in Interim DoDI 5000.02. Furthermore, the Milestone Decision Authority (MDA) will not approve program initiation or entry into any phase that requires milestone approval for any IT acquisition program until the Principal Director, EIS/CIO, confirms CCA compliance.

8.3 The DISA CCA compliance checklist, CCA cover letter, and a memorandum from the Principal Director, EIS/CIO, or CCA compliance letter will be used to confirm CCA compliance.

8.4 In accordance with Interim DoDI 5000.02, Program or Functional Managers are required to conduct a Post Implementation Review (PIR) for all fully deployed IT acquisition category (ACAT) or high-interest programs, including national security systems (NSSs).

9. Responsibilities.

9.1 **Principal Directors, Directors, Commanders, and Chiefs of Major Organizational Elements.** These individuals will provide functional area support for the execution of this Instruction.

9.2 **Principal Director for Enterprise Information Services (EIS)/Chief Information Officer (CIO).** The Principal Director, EIS/CIO, is responsible for IT policy development and IT strategic planning and for ensuring internal networks are compliant with DoD policies.

In addition to providing functional area support for the execution of this Instruction, the Principal Director, EIS/CIO, will:

9.2.1 Provide organizational representation to various acquisition and procurement review boards, as appropriate.

9.2.2 Provide subject matter expertise in the functional areas of CCA compliance.

9.2.3 Comply with and implement CCA management processes and procedures, in accordance with law and DoD and DISA regulations and policies.

9.2.4 Provide forms and instructional guidelines that detail the CCA process along with standard operating procedures.

9.2.5 Serve as an authoritative point of contact for management, oversight, review, and approval of DISA CCA matters.

9.2.6 Conduct random audits of programs, projects, or services that have been confirmed to be in compliance with CCA by a PM, PL, and/or SM to ensure there is proper documentation to support CCA compliance.

9.2.7 Maintain records to include a complete trail of assessments of subject matter experts of CCA compliance that is suitable for an audit, in accordance with DISAI 210-15-6, Records Management.

9.3 Component Acquisition Executive (CAE). In addition to providing functional area support for the execution of this Instruction, the CAE, as the Senior Decision Authority (SDA), will ensure programs, projects, initiatives, IT services, and other IT acquisition matters are in compliance with CCA prior to decision reviews.

9.4 Director for Procurement. In addition to providing functional area support for the execution of this Instruction, the Director for Procurement will ensure acquisition packages are reviewed to verify the Principal Director, EIS/CIO, has approved CCA compliance for all IT acquisitions prior to contract award. (The review is to be accomplished through the Procurement Requirements Checklist process, as outlined in the Requirements Package Checklist/Certifications & Section 508 Determination, located at https://www.ditco.disa.mil/contracts/instruct_docs/Encl1_Rqmnts_ChecklistSection_508.pdf.)

10. Duties of Program Manager (PM), Project Lead (PL), and/or Service Manager (SM). The PM, PL, and/or SM takes mission requirements and performance objectives from stakeholders and/or warfighters and translates them to acquisition requirements and strategies based on market understanding, planning, policies, processes, affordability, and schedule. The PM, PL, and/or SM further conducts the following actions to support CCA compliance, when applicable.

10.1 Ensures all proposed DISA IT acquisitions comply with the CCA precepts, as outlined below:

10.1.1 Ensures the functions supported by the proposed DISA IT acquisition are necessary and in alignment to accomplish its mission or business processes.

10.1.2 Determines that no private sector or government source can better support the function.

10.1.3 Redesigns the processes that the system supports to reduce costs, improve effectiveness, and maximize the use of commercial-off-the-shelf (COTS) technology.

10.1.4 Ensures the acquisition is consistent with the Department of Defense information network (DODIN) policies and architecture, in accordance with DISAI 630-225-14, Enterprise Architecture (EA) Governance Framework.

10.1.5 Validates the proposed acquisition will make the maximum use of COTS IT software and service solutions.

10.1.6 Conducts an analysis of alternatives, identifies and briefly discusses the alternatives (to include the option of utilizing existing technology) examined prior to program initiation, and discusses the methodology and criteria used to evaluate alternatives.

10.1.7 Conducts an economic analysis that includes a calculation of the return on investment or, for nonautomated information systems programs, conducts a Life-Cycle Cost Estimate (LCCE).

10.1.8 Ensures the program has an information assurance strategy that is consistent with DoD policies, standards, and architectures, in accordance with DoDI 8580.1 (authority document).

10.1.9 Completes a Privacy Impact Assessment for appropriate IT acquisitions, in accordance with DISAI 210-225-2, Privacy Program.

10.1.10 Provides guidance on formulating effective outcome-based performance measurements that determine success and measure how well the IT will support DISA's programs or processes.

10.1.11 Ensures, to the maximum extent practicable, that modular contracting, in accordance with the General Services Administration (GSA) Guide for Modular Contracting, December 1998, will be used with programs that are being implemented in phased, successive increments, such that each increment meets part of the mission need and delivers measurable benefit, independent of future increments.

10.1.12 Describes the process and metrics for measuring program progress to include cost, schedule, and technical performance.

10.1.13 Identifies and assesses risk in areas such as cost, schedule, technology, unusual security requirements, software complexity, system integration requirements, or technical configuration.

10.1.14 Registers mission-critical and mission-essential systems within the DoD Information Technology Portfolio Repository (DITPR).

10.2 Develops a plan and conducts a Post-Implementation Review (PIR) for fully deployed IT, including NSSs, in accordance with Interim DoDI 5000.02, for ACAT or special-interest programs.

10.2.1 Provides a basis for comparing actual program results with the established performance goals, in accordance with subparagraph (a)(5) of section 1115 of title 31 U.S.C.

10.2.2 Ensures performance measurements are prescribed for IT used by, or to be acquired for, the executive agency and measure how well the IT supports programs of the executive agency, in accordance with paragraph (ab) section 11313 of Title 40 U.S.C.


10.2.3 Provides to Principal Director, EIS/CIO, a PIR plan to complete the PIR.

10.3 Ensures the CCA compliance process is demonstrated appropriately within the program and/or project plan and provides to the Principal Director, EIS/CIO, a timeline schedule as it relates to confirm CCA compliance.

10.4 Provides to the Principal Director, EIS/CIO, confirmation of CCA compliance for program, project, or acquisition of services below the thresholds, as specified in subparagraph 8.1.2.

11. CCA Compliance Letter and Checklist. The formats for the CCA compliance letter and DISA CCA checklist are to be used by the PM, PL, and SM to show CCA compliance. The formats are located at <https://disa.deps.mil/disa/org/cia/CI2%20Documents/Clinger-Cohen%20Act/Templates>. For information regarding the templates, contact the CIO Compliance Branch at disa.meade.eis.mbx.cca-compliance@mail.mil.

Enclosure a/s


ROBERT J. SKINNER
Brigadier General, USAF
Chief of Staff

*This Instruction must be reissued, canceled, or certified current within 5 years of its publication date. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.

OPR: EIS - disa.meade.eis.mbx.cca-compliance@mail.mil

DISTRIBUTION: P

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 decisionmaking, 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). A consolidated inventory of DoD mission critical and mission essential information systems.

Information Technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

The term "equipment" means any equipment used by a Component directly or used by a contractor under a contract with the Component that requires the use of such equipment or the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term "IT" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "IT" also includes national security systems (NSSs). It does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

Information Technology (IT) System. A discrete set of information resources organized for the collections, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology (IT) Services. The performance of any work related to IT and the operation of IT, including national security systems (NSSs). This term includes IT-based business processes, outsourced IT, and outsourced information functions.

Major Automated Information System (MAIS) (ACAT IAM or IAC). An automated information system (AIS) 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 single AIS: the separate AISs that constitute a multielement 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 Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD[AT&L]) as an MDAP or estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test, and evaluation of more than \$365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than \$2.190 billion in FY 2000 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).

Modular Contracting. An acquisition strategy that breaks a large "grand design" program into discrete components that is easier to manage.

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, subject to the following limitation, 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. §11103(a)(1))).

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. The PM will be accountable for credible cost, schedule, and performance reporting to the Milestone Decision Authority (MDA).

Project. A planned undertaking, independent of a program, having a finite beginning and ending that involves definition, development, production, and logistics support of an IT system or systems. A project may be a technology insertion initiative, an internal process improvement, a technology demonstration, or a stand-alone effort.

Project Leader (PL). The individual responsible for managing a project to include accountability for capability execution and meeting the needs of the mission partner in terms of planning and rapidly delivering IT capabilities. A PL will have the acquisition skills and experience consistent with the size, complexity, scope, and risk of the project.

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 not limited to, IT services, telecommunications, program and project support services, operational support services, acquisition consulting services, and technical support services.