DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

AD-RES-AC-008

SAIS-AD (25-1rrrr)

1 December 2023

MEMORANDUM FOR SEE FOR DISTRIBUTION

SUBJECT: U.S. Army Chief Information Officer Standardization of Clinger-Cohen Act Compliance Guidance

1. References. See Enclosure 1.

2. Purpose. This memorandum standardizes and streamlines the Army's Office of the Chief Information Officer (OCIO) Clinger-Cohen Act (CCA) requirements.

3. Background. In accordance with 40 USC Subtitle III, all programs that acquire information technology, including national security systems (NSS), are subject to the requirements of the Clinger Cohen Act. The CCA mandates the Milestone Decision Authority (MDA) will not initiate a program (nor an increment of a program), approve entry into any phase of the acquisition process that requires formal acquisition milestone approval, or authorize execution of a contract for the applicable acquisition until:

a. The sponsoring Component or Program Manager (PM) has satisfied the applicable requirements of the CCA as shown in Enclosure 2.

b. The Chief Information Officer (CIO), or authorized designee, confirms CCA compliance.

4. Applicability. The provisions of this memorandum apply to Headquarters, Department of the Army, Army Commands, Army Service Component Commands, Direct Reporting Units, the Army National Guard, and the Army Reserve.

5. Policy.

a. Army CIO CCA compliance authorities and processes, including the required compliance actions listed in Enclosure 2, will be executed in accordance with the Department of Defense Instruction (DODI) 5000 and 8500 series.

b. This policy supersedes all prior guidance related to CCA compliance provided in AR 25-1 and DA PAM 25-1-1.

6. Army CIO CCA Compliance Guidance.

a. Programs meeting the Acquisition Category (ACAT) I and II and Business Category (BCAT) I and II programs' threshold will submit CCA confirmation packages to Army CIO. Packages should include the following:

(1) A completed CCA confirmation table indicating which documents support CCA compliance.

(2) Electronic copies or access to documents cited in the CCA confirmation table.

b. CCA confirmation authority meeting the ACAT III and IV and BCAT III programs' threshold are delegated to the program's Milestone Decision Authority (MDA), including all 11 elements required for CCA certification. PMs will make CCA confirmation documents available to the OCIO.

c. For Services Acquisitions, the decision authority will not approve the acquisition of IT services and DOD Components will not award a contract for IT services until the Functional Services Manager (FSM) has satisfied the applicable CCA requirements.

d. PMs/FSMs should use and cite documents using the Adaptive Acquisition Framework Document Identification (AAFDID) tool (https://www.dau.edu/aafdid/) to identify CCA compliance requirements in accordance with appropriate acquisition pathways.

e. The OCIO will coordinate with the appropriate Headquarters, Assistant Secretary of the Army (Acquisition, Logistics and Technology) Department of the Army Systems Coordinators and PMs, as necessary, throughout the acquisition lifecycle to provide recommendations, respond to inquiries, and to support and assist in the preparation and submittal of required CCA compliance documents.

f. The OCIO will generate CCA Compliance Memorandums (See Enclosure 3) meeting ACAT I and II programs.

g. BCAT I and II programs' thresholds will forward the CCA Compliance Memorandum to the Army Acquisition Executive (AAE) or the designated MDA when all CCA actions have been confirmed as completed. Programs meeting ACAT III and IV programs, BCAT III programs threshold MDA will generate compliance memorandums.

7. Points of contact.

a. CIO Policy Inbox: usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil.

b. Mr. David Sultan, SAIS-ADA, david.e.sultan.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2023.12.01 12:41:27 -05'00'

LEONEL T. GARCIGA
Chief Information Officer

4 Encls
1–3, as
4. Acting CIO memo, 7 Mar 2023

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Futures Command
- U.S. Army Pacific
- U.S. Army Europe and Africa
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command
- U.S. Army Corrections Command

Superintendent, U.S. Military Academy
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
(CONT)

DISTRIBUTION: (CONT)
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF:
Principal Cyber Advisor
Director of Enterprise Management
Director, Office of Analytics Integration
Commander, Eighth Army

REFERENCES

a. 40 U.S.C., Subtitle III, §11101 et seq. (Clinger-Cohen Act of 1996)

b. Department of Defense Directive 5000.01 (The Defense Acquisition System)

c. Department of Defense Directive 8000.01 (Management of the Department of Defense Information Enterprise (DOD IE))

d. Department of Defense Instruction 5000.02 (Operation of the Adaptive Acquisition Framework

e. Department of Defense Instruction 5000.74 (Defense Acquisition of Services)

f. Department of Defense Instruction 5000.75 (Business Systems Requirements and Acquisition)

g. Department of Defense Instruction 5000.80 (Operation of the Middle Tier of Acquisition (MTA))

h. Department of Defense Instruction 5000.81 (Urgent Capability Acquisition)

i. Department of Defense Instruction 5000.82 (Requirements for the Acquisition of Digital Capabilities)

j. Department of Defense Instruction 5000.85 (Major Capability Acquisition)

k. Department of Defense Instruction 5000.87 (Operation of the Software Acquisition Pathway)

l. Department of Defense Instruction 5000.90 (Cybersecurity for Acquisition Decision Authorities and Program Managers)

m. Department of Defense Instruction 8500.01 (Cybersecurity)

n. Department of Defense Instruction 8510 (Risk Management Framework (RMF) for DOD Information Technology (IT))

o. Army Regulation 25-1 (Army Information Technology)

p. Army Regulation 25-2 (Cybersecurity)

q. Department of the Army Pamphlet 25-1-1 (Army Information Technology Implementation Instructions)

r. Department of the Army Pamphlet 25-2-11 (Cybersecurity Strategy for Programs of Record)

s. Joint Capabilities Integration and Development System Manual (Manual for the Operation of the Joint Capabilities Integration and Development System)

t. Army Portfolio Management System (APMS) Deskside Reference Manual

u. Adaptive Acquisition Framework Document Identification (AAFDID) Tool

CCA Compliance Requirements. This enclosure describes the supporting documents that demonstrate compliance for each of the 11 CCA actions. Considerations for complying with each CCA Action and likely sources of information and documentation for compliance are presented after the supporting documents for each CCA compliance action.

1. CCA Compliance Action 1. Make a determination that the acquisition supports core, priority functions of the DOD.

a. The supporting documentation for this CCA Action is generally found in an approved Initial Capabilities Document (ICD), Information Systems (IS) ICD, Capability Requirements Document (CRD), or Capability Needs Statement (CNS). DOD core/primary functions are documented in national strategies and DOD mission and strategy documents like the Quadrennial Defense Review, Strategic Planning Guidance, Joint Operating Concepts, Joint Functional Concepts, Integrated Architectures, the Business Enterprise Architecture, the Universal Joint Task List, mission area statements, or Service mission statements. *Other potential sources include the Capability Development Document (CDD) and Analysis of Alternatives (AoA).*

b. Documents submitted to comply with this action should validate and explain the rationale supporting the relationship between the Army's mission (i.e., core/priority functions) as found in Army mission and strategy documents, and the IT function supported by the investment or acquisition.

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

a. The supporting documentation for this CCA Action is generally found in an approved ICD or IS ICD, CDD, CNS, CRD, AoA, Acquisition Program Baseline (APB), or Performance Measurement Plan.

b. Documents submitted to comply with this action should describe the desired outcome and how the program would develop and deploy the solution to achieve that outcome. Outcome-based performance measures (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.

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

a. The supporting documentation for this CCA Action is generally found in an approved ICD or IS ICD, Concept of Operations, AoA, CDD, Acquisition Strategy, or Business Process Reengineering documentation.

b. Documents submitted to comply with this action should demonstrate how the investment reduces costs and improves performance. Documents should describe the actions taken to streamline, reengineer, or redesign existing processes to reduce costs, improve effectiveness, and maximize the use of commercial-off-the-shelf (COTS) items or tailored versions of government-off-the-shelf (GOTS) technology that better support the organization's mission.

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

a. The supporting documentation for this CCA Action is generally found in an approved Acquisition Strategy, supported by an approved AoA or equivalent analysis. *Another potential source is the Market Survey (if one has been performed*).

b. Documents submitted to comply with this action should demonstrate that the acquisition is being undertaken by the Army 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. The Program should determine that the proposed function does not duplicate or overlap with an existing function being performed elsewhere by the Federal Government, DOD, or Army agencies.

5. CCA Compliance Action 5. Conduct an analysis of alternatives.

a. The supporting documentation for this CCA Action is an Acquisition Strategy and an approved AoA, or equivalent analysis. Use OMB Circular A-11, Preparation, Submission and Execution of the Budget, to determine the criteria to be used in the AoA and benefit/cost analysis. Another useful document is OMB's Capital Planning Guide, especially Part 7, Section 300, Planning, budgeting, acquisition, and management of capital assets, and the Part 7 Supplement. Other potential sources include the Business Case Analysis, Trade Survey, Cost and Operational Effectiveness Analysis (COEA), Market Surveys, Cost-Benefit Analysis (CBAs), or equivalent documents that demonstrate best value.

b. The AoA or equivalent analysis submitted to comply with this action should address—

(1) Whether the program conducted a thorough analysis and considered enough reasonable alternatives (DODI 5000.02 states that in developing feasible alternatives, the AoA identify a wide range of solutions that have a reasonable likelihood of providing the needed capability);

(2) The alternatives examined (including the pros and cons of each alternative); and

(3) And why the selected alternative was chosen and why the remaining alternatives were not chosen.

6. CCA Compliance Action 6. Conduct an Economic Analysis that includes a calculation of the return on investment; or for non-automated information system (AIS) programs, conduct a life-cycle cost estimate.

a. The supporting documentation for this CCA Action is an approved Component/Program Cost Estimate or Component/Program Cost Position. Depending on the capability, an approved Life-Cycle Cost Estimate (LCCE) may be substituted.

b. Documents submitted to comply with this action should provide a calculated Return on Investment (ROI) or LCCE depending on the type of system being acquired. DODI 5000.75 provides guidance on how to satisfy the ROI requirement for Defense Business Systems acquisition programs. DODI 5000.02 provides guidance on how to satisfy the ROI requirement for all other defense programs. DODI 5000.74 provides CCA guidance for the acquisition of contracted services.

7. CCA Compliance Action 7. Develop clearly established measures and accountability for program progress.

a. The supporting documentation for this CCA Action is generally found in an approved Acquisition Strategy. Other potential sources are an approved APB and an Earned Value Management System (EVMS).

b. Documents submitted to comply with this action 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.

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

a. The supporting documentation for this CCA action is the system architecture and is generally found in an Information Support Plan (ISP), an approved Joint Capabilities and Integration Development System (JCIDS) / Army Capabilities Integration and Development System (ACIDS) capability development document, CNS, or CRD. Depending on the milestone of the program, the source document can be draft. The final ISP is required during the milestone before the final decision to deploy the capability.

b. Documents submitted to comply with this action should describe the system's function, dependencies, and interfaces with other IT and NSS systems using the DOD IEA's activities and concepts. Submissions should provide graphic views that show the major elements/subsystems that make up the system being acquired, and how they fit together.

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

a. The Cybersecurity Strategy (CSS) submitted to comply with this CCA Action should describe how the program's Cybersecurity features comply with applicable DOD and Army policies, standards, and architectures, and describe the program's certification and accreditation approach.

b. For acquisition categories meeting the ID, IC, IA, IAM, IAC, BCAT I program thresholds , the DOD CIO will review and approve the CSS prior to milestone decisions or contract awards.

c. For program meeting ACAT II and BCAT II programs' threshold the Army CIO will review and approve the CSS prior to milestone decisions or contract awards.

d. For programs meeting ACAT III and IV programs, BCAT III programs' thresholds, the Army CIO delegates the approval authority to the responsible MDAs.

10. CCA Compliance Action 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.

a. The supporting documentation for this CCA Action is generally found in an approved Acquisition Strategy.

b. Documents submitted to comply with this action should describe the extent to which modular contracting principles are adhered. 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 should describe the relationship between each increment and the mission need and benefit associated with that increment.

11. CCA Compliance Action 11. Register Mission-Critical and Mission-Essential systems with the DOD CIO. The Program must be registered in the Army Portfolio Management System (APMS) and the Army IT Registry (AITR), which feed the DOD Information Technology Portfolio Repository (DITPR). Program Managers are responsible for: 1) ensuring the program is registered in APMS; 2) system registration contains the appropriate designation for requiring CCA Compliance; and 3) verifying system information is complete, current, and accurate.

OCIO CCA Compliance Memorandum Template. This enclosure includes a template of the compliance memorandum sent from OCIO to the AAE upon completion of the CCA compliance review process.

DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

SAIS-AD

MEMORANDUM FOR The Assistant Secretary of the Army (Acquisition, Logistics and Technology), 103 Army Pentagon, Washington, DC 20310-0103

SUBJECT: Title 40/Clinger-Cohen Act Compliance Confirmation in Support of the _____ Milestone _____ Decision Review

1. In accordance with Department of Defense (DoD) Instruction 5000.82 (Acquisition of Information Technology), I confirm that my office has assessed the _____ program and determined it to be compliant with all DoD and Army Chief Information Officer Clinger-Cohen Act (CCA) assessment requirements for a Milestone _____ Decision Review, per enclosed compliance matrix.

2. My point of contact for this action is Mr. David Sultan, at david.e.sultan.civ@army.mil or (706) 305-8729.

Encls

LEONEL GARCIGA (or designated authority)
Chief Information Officer

Delegation of Authority for Cybersecurity Strategy Approval. This enclosure includes the Delegation of Authority to approval of Army program Cybersecurity Strategy.

DEPARTMENT OF THE ARMY
THE CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

SAIS-CS 7 Mar 2023

MEMORANDUM FOR ARMY CHIEF INFORMATION SECURITY OFFICER

SUBJECT: Delegation of Authority for Army Program Cybersecurity Strategy Approval

1. References:

a. DoDI 5000.82 (Acquisition of Information Technology (IT)).

b. DoDI 5000.90 (Cybersecurity for Acquisition Systems).

c. DoDI 8500.01 (Cybersecurity).

d. DoDI 8580.01 (Information Assurance (IA) in the Defense Acquisition System).

2. Pursuant to reference 1.d., I hereby delegate the authority and responsibility to review and approve Army Programs Cybersecurity Strategies to the Chief Information Security Officer. This authority may not be further delegated.

3. Although not a limitation on your authority to act on my behalf, I trust that you will exercise sound judgment in keeping me informed of any action under this delegation that will have significant White House, congressional, Department of Defense, or public interest or would represent a significant change in Army precedent or policy. If such circumstances arise, coordinate with me to ensure that I may provide appropriate guidance.

4. This delegation is effective immediately. You are responsible for reviewing this delegation with the Office of the Chief Information Officer every 3 years from the date of signature to ensure it remains current.

5. The point of contact for this action is Dr. Christian Charris at christian.b.charris.civ@army.mil.

MARKOWITZ.DAVID.1228551720
Digitally signed by MARKOWITZ.DAVID.1228551720
Date: 2023.03.07 12:47:25 -05'00'

DAVID MARKOWITZ
Acting Chief Information Officer

DISTRIBUTION:
(see next page)