Recommendation 44: Exempt DoD from Clinger–Cohen Act Provisions in Title 40.

Problem

Two decades after its implementation, the Clinger–Cohen Act of 1996 (CCA) has made significant progress in instilling an enterprise view of IT acquisition among federal agencies, but other goals have proven harder to achieve. Many agencies continue to lag in prioritizing commercial technology and best practices over government-unique processes, a key mandate of CCA. Additionally, newer laws such as FITARA strengthen CCA provisions, including the use of modular contracting and the agency CIO role created—but not sufficiently empowered—by CCA.

Within DoD, the CCA compliance process is not only outdated but also a time-consuming burden for programs that are layered on top of DoD's robust resources, requirements, and acquisition system. This multilayered process renders many CCA requirements redundant with other laws, regulations, and policies. DoD's checklist-oriented compliance process occurs at major milestones rather than throughout the development process. DoD's current compliance with CCA provides limited strategic value for CIOs and programs, and it has become more of a hurdle than an enabler in efforts to streamline and modernize IT acquisition.

Background

CCA is a group of legal provisions intended to provide enterprisewide oversight and discipline for IT acquisition across all federal agencies. CCA is mainly codified under Subtitle III of Title 40, Information Technology Management.[1] DoDI 5000.02, which lays out the process for defense acquisition, contains a list of 11 specific requirements program offices must meet to be considered compliant with CCA.[2] This list has been incorporated into other tailored guidance for the acquisition of services and defense business systems, DoDI 5000.74 and DoDI 5000.75, respectively.

CCA History

CCA was enacted as part of the FY 1996 NDAA.[3] It comprised two bills that were added to the NDAA—the Federal Acquisition Reform Act and the Information Technology Management Reform Act (ITMRA). Together they are known collectively as CCA, although most provisions relating to IT come from the ITMRA portion, and DoD's implementation of CCA explicitly identifies compliance only with ITMRA.[4] In 2002, the IT provisions of CCA were codified under Title 40 of U.S. Code.[5]

CCA repealed the Automatic Data Processing Act of 1965, informally known as the Brooks Act, and instituted updated guidance for management and acquisition of federal IT. In 1994, then-Senator William S. Cohen released his investigative report *Computer Chaos: Billions Wasted Buying Federal Computer Systems*.[6] The report's analysis of existing federal information systems found that many

[1] As of mid-2018, 40 U.S.C. § 11101 through 40 U.S.C. § 11704.
[2] Operation of the Defense Acquisition System, DoDI 5000.02, Enclosure 1, Table 10, 76 (2017).
[3] FY 1996, Pub. L. No. 104-106 (1996). Codified in law as Information Technology Management, 40 U.S.C. Subtitle III.
[4] Implementation of Subdivision E of the Clinger–Cohen Act of 1996 (Public Law 104-106), DOD Memorandum (1997).
[5] Codifying Title 40, United States Code—Public Buildings, Property, and Works, Pub. L. No. 107-217 (2002).
[6] William S. Cohen, *Computer Chaos: Billions Wasted Buying Federal Computer Systems,* U.S. Government Printing Office, 1994.

agencies were undertaking IT initiatives that were not related to their mission or sufficiently integrated with existing IT, much of which was archaic and difficult to maintain or modernize. Additionally, GSA offices charged with overseeing and preapproving all federal IT procurement were overworked and understaffed, leading to delays. Cohen's report provided support for and directly led to the reforms of CCA.

CCA revisited the acquisition of federal IT in a systemic way, and it set out new best practices from the private sector meant to create efficiencies. CCA was intended to improve slow and uncoordinated acquisition of computers and software on the federal level, shift oversight from GSA to federal agencies and OMB, and shift IT purchases to being viewed as strategic investments rather than isolated expenses. For the first time in law, CCA established CIOs in government agencies, detailing their roles and responsibilities. CIOs were meant to oversee all major IT investments in coordination with their agency heads, linking capital planning, budget formulation, and execution. CCA also encouraged incremental acquisition and modular contracting, and it required agencies to use commercial solutions rather than develop unique software or business processes.[7]

CCA in DoD

As implemented in DoD, CCA created three strategic planning steps for IT: make sure the IT investment directly supports the agency's mission; procure commercial technology if available; and if DoD-specific IT must be developed, conduct BPR first to ensure processes are modernized alongside technology.[8]

CCA was originally created to solve problems with both civilian agencies and DoD. Civilian agencies continue to have less sophisticated acquisition processes than DoD, and some of them struggle with effective oversight of IT acquisition.[9] DoD's acquisition structure provides substantial oversight for all acquisitions at an enterprise level, as detailed in DoDD 5000.01, The Defense Acquisition System, and DoDI 5000.02, Operation of the Defense Acquisition System. DoD has an additional acquisition process for IT, originally detailed in the DoDI 5000.02 as Enclosure 11, Requirements Applicable to All Programs Containing Information Technology and Enclosure 12, Defense Business Systems. Guidance for CCA compliance is also found in DoDI 5000.74, which contains the same 11-item compliance list as DoDI 5000.02 and DoDI 5000.75. This list integrates CCA compliance with other processes rather than as a separate checklist.[10]

---

[7] These requirements can also be found in 10 U.S.C. § 2222.

[8] Secretary of Defense, DoD Memorandum, *Implementation of Subdivision E of the Clinger–Cohen Act of 1996 (Public Law 104-106),* 1997, accessed October 22, 2018, https://www.acq.osd.mil/dpap/Docs/clinger.pdf.

[9] The IRS, for instance, was cited by the Treasury Inspector General for lacking a cloud migration strategy despite a 2010 cloud-first mandate from the federal CIO. In 2015, the IRS developed Form 990 using cloud services without crafting an agreement that adheres to FedRAMP-approved best practices. DoD, by contrast, has created its own cloud provider, the Defense Information Systems Agency (DISA). Treasury Inspector General for Tax Administration, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service,* August 7, 2017, accessed June 15, 2018, https://www.treasury.gov/tigta/auditreports/2017reports/201720032fr.pdf.

[10] Defense Acquisition of Services, DoDI 5000.74, Enclosure 7, Table 2: CCA Compliance, 31 (2017).

DoDI 5000.02's Enclosure 11 clarifies the additional steps to demonstrate CCA compliance, which apply to all IT programs of any size, including National Security Systems (NSSs). The Milestone Decision Authority (MDA) may not issue a milestone approval until the following transpires:

> *(1) The sponsoring DoD Component or program manager has satisfied the applicable acquisition phase-specific requirements of the CCA as shown in Table 9 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.*[11]

Below is the 11-item CCA checklist from DoDI 5000.02 and DoDI 5000.74:

- Make a determination that the acquisition supports core, priority functions of the DoD.
- Establish outcome-based performance measures linked to strategic goals.
- Redesign the processes that the system supports to reduce costs, improve effectiveness, and maximize use of commercial off-the-shelf (COTS) technology.
- Determine that no private-sector or government source can better support the function.
- Conduct an analysis of alternatives.
- Conduct an economic analysis that includes a calculation of the return on investment; or for non-automated-information-systems programs, conduct a lifecycle cost estimate.
- Develop clearly established measures and accountability for program progress.
- Ensure that the acquisition is consistent with the DoD Information Enterprise policies and architecture, to include relevant standards.
- Ensure that the program has a cybersecurity strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.
- Ensure, to the maximum extent practicable, (a) modular contracting has been used, and (b) 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 increment.
- Register mission-critical and mission-essential systems with the DoD CIO (Implemented as the DoD Information Technology Portfolio Repository (DITPR)).

These eleven items correspond to the original language in CCA as codified in Titles 10, 40, and 41. Table C-1 (in Appendix C) details this crosswalk between DoD policy and statute. DoD policy implements this statutory requirement as a documentation checklist, described in more detail below.

[11] Operation of the Defense Acquisition System, DoDI 5000.02, Enclosure 11, 140–141 (2017).

CCA Compliance Process

As executed, DoD's process of CCA compliance has four main steps, the first three involving multiple layers of review before approval is granted:

- The PM compiles documentation to demonstrate CCA compliance with the 11 criteria at key milestones.
- This documentation is reviewed by the program executive officer (PEO).
- Following this review, the documentation goes to the Component CIO. (The Air Force has modified this process to reverse steps 2 and 3, so PEO review occurs after CIO approval.)
- PMs or Component CIOs enter information in DITPR, which is used to satisfy required reporting of enterprisewide compliance and coordination to the Secretary of Defense and Congress. CIOs also write a memorandum demonstrating program compliance.

This process is completed using documents that are also reviewed and approved within the traditional acquisition review chain, going up to the component acquisition executive and defense acquisition executive, based on the program's acquisition category level. The same documents are repurposed for the CCA compliance process, which brings them to the CIO's attention with the goal of having a single point of oversight for all DoD IT acquisitions. DoDI 5000.02, Enclosure 1, Table 10: CCA Compliance, lists the acquisition documents that can provide evidence of CCA compliance. Element 3, for instance, can be satisfied by information found in the initial capabilities document (ICD), information systems ICD, concept of operations, analysis of alternatives, or BPR.[12]

In February 2017, DoDI 5000.75, Business Systems Requirements and Acquisition, created new guidance that replaced Enclosure 12 of DoDI 5000.02. This guidance was intended to streamline the acquisition process for defense business systems (DBSs) and make it more compatible with flexible and iterative development approaches. This new instruction explicitly states that CCA compliance should not require separate documentation and can be satisfied by existing documentation and reviews, a streamlined practice that was already common in the Air Force. It replaces milestones with authority to proceed decision points, encouraging oversight of DBSs on an ongoing basis instead of only at predetermined points in the lifecycle.

DBSs guidance states that "decision authorities will prevent tailored procedures from including separate reviews and approvals by other organizations when confirmation through direct collaboration is sufficient."[13] This revision to the DBS acquisition process reflects the need for fewer formal review processes and more teamwork; it also shows the extent to which CCA compliance has become embedded in DoD practices, particularly those governing DBSs. As more IT programs begin using Agile development and acquisition processes, DoD process requirements will need to evolve from checklists to ongoing collaboration.

[12] Ibid, Enclosure 1, Table 10, 76.
[13] Business Systems Requirements and Acquisition, DoDI 5000.75 (2017).

Discussion

CIOs Lack Authority to Fully Implement CCA-Directed Oversight

The positive intent of CCA has not consistently translated into action. CCA was meant to empower agency CIOs, yet multiple evaluations of federal agencies show that CIOs did not receive enough authority over strategic and budget decision making, were dividing their attention among multiple leadership roles in their organization, or did not report directly to the head of their agency—necessary conditions for effectiveness.[14] In 2015, the FITARA gave new legal mandate and authority for empowering CIOs.

FITARA was passed as part of the FY 2015 NDAA and was arguably the most significant legislative initiative on federal IT acquisition since CCA.[15] FITARA attempted to address some of the CIO issues by bolstering OMB's oversight role, establishing in law the Federal IT Dashboard, and reinforcing the authority of agency CIOs.[16] FITARA was also meant to reinforce the mandate to engage in modular contracting and adopt more commercial technology, requiring CIOs to "certify that information technology investments are adequately implementing incremental development."[17] In FY 2016, federal agencies reported that 64 percent of active software development projects were slated to deliver usable functionality every 6 months.[18] Within DoD, only 8 percent of projects—4 out of 51 projects—were planning delivery of releases every 6 months.[19] The cultural preference for big programs has not been alleviated by statutory requirements for modular contracting and incremental development.

The role of agency CIOs is outlined in 40 U.S.C. § 11315, which states that a CIO has the following responsibilities and duties:

- Providing advice and assistance on IT acquisition to the agency head.
- Ensuring a sound, secure, and integrated IT architecture.
- Promoting effective and efficient design and operation of IT management processes.

---

[14] See for instance "Information Technology: Opportunities for Improving Acquisitions and Operations," U.S. Government Accountability Office, April 2017, https://www.gao.gov/assets/690/684047.pdf. Also see *Information Technology: Improved Implementation of Reform Law Is Critical to Better Manage Acquisitions and Operations, GAO-17-263T,* December 6, 2016, 13, accessed October 23, 2018, https://www.gao.gov/assets/690/681420.pdf.

[15] FY 2015 NDAA, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (2014). Other IT legislation includes Title III of the E-Government Act (Pub. L. No. 107-347) and the Federal Information Security Management Act of 2002 (FISMA, updated in 2014 as the Federal Information Security Modernization Act under Pub. L. No. 113-283). FISMA requires agencies to demonstrate security of information and information systems, but does not take such a systemic approach to the management and acquisition of IT.

[16] "How the Clinger–Cohen Act Continues to Ripple Through Federal IT Today," Wylie Wong, FedTech Magazine, February 10, 2016, accessed October 23, 2018, http://www.fedtechmagazine.com/article/2016/02/how-clinger-cohen-act-continues-ripple-through-federal-it-today

[17] Resources, Planning, and Portfolio Management, 40 U.S.C. § 11319(b)(1)(B)(ii).

[18] GAO, *Information Technology: Improved Implementation of Reform Law Is Critical to Better Manage Acquisitions and Operations, GAO-17-263T,* December 6, 2016, 13, accessed October 23, 2018, https://www.gao.gov/assets/690/681420.pdf.

[19] Ibid, 15-16. GAO notes a disparity between agencies' reporting of projects on the IT Dashboard and to GAO. For DoD, the numbers reported to GAO demonstrated that 8% of projects planned delivery every 6 months. The data on the IT Dashboard showed 63% of projects planned delivery every 6 months.

- Monitoring and evaluating IT program performance and providing advice on whether to end programs.
- Annually engaging in strategic planning and performance evaluation processes.

Missing from this list is budget authority for IT investments. Several IT experts said that because CIOs do not have access to substantial amounts of funding, they need to have a role in the acquisition process to ensure strategic spending within funded entities.[20] That role is ensured with the CCA compliance process, for which CIOs conduct cost analysis on a program-by-program basis. Some component CIOs have more opportunities for influence over Military Service priorities and spending decisions, as the Air Force CIO does on the AF Corporate Board. On an enterprise level, one expert shared that the DoD CIO had seen some success in promoting collective pricing arrangements across DoD components, lowering overall vendor costs.[21] He conceded, however, that CCA should be "revamped a little."[22] Current means for enabling CIOs have led to modest success, but CIO authority falls short of the original intent of CCA.

CIO turnover at agencies has been high. As a 2004 GAO report pointed out, in the 8 years following CCA enactment, the average tenure of federal CIOs was 2 years. This trend has continued and intensified. Agency CIOs and IT executives generally agree that they need 3 to 5 years to become effective.[23] DoD has had 14 different CIOs between 1996 and 2018, nine of whom were in an acting capacity for all or part of their tenure. During this period, the average tenure for the DoD CIO was 24 months. With the change in presidential administrations in 2017, seven federal agency CIOs handed over their responsibilities within the span of a few months, renewing concerns about consistency in federal IT leadership.[24]

The CIO Council, established in 2002, provides support and guidance for agency CIOs. In 2008 and 2012, the CIO Council issued versions of the CCA Core Competencies, a training document based on CCA to educate CIOs on IT acquisition and management strategies. This document notes that no one individual can accomplish all the goals, emphasizing the importance of training the entire IT acquisition workforce. The 2012 version added nine competencies, including guidance on cloud computing and social media, two fundamental pieces of modern computing that did not exist in 1996. The guidance on acquisition acknowledges, "Acquisition needs to move from what [has] been a singular focus on process to one that considers both process and objectives."[25]

OMB has issued similar guidance, such as OMB Circular A–130, Management of Federal Information Resources, the primary policy document for federal IT management. Circular A–130 establishes policy

---

[20] DoD CIO officials and Deputy Assistant Secretary of Defense, Command, Control, Communications, Cyber, and Business Systems (DASD (C3CB)), discussions with Section 809 Panel, February–March 2018.
[21] DoD CIO official, discussion with Section 809 Panel, March 2018.
[22] Ibid.
[23] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges, GAO-04-823,* July 2004, 4 and 47, accessed October 23, 2018, https://www.gao.gov/new.items/d04823.pdf.
[24] "GAO Chief: CIO Departures Are 'An Area of Concern,'" Carten Cordell, Scoop News Group, August 23, 2017, accessed October 23, 2018, https://www.fedscoop.com/gaos-dodaro-says-cio-departures-area-concern/.
[25] CIO Council, *2012 Clinger–Cohen Core Competencies and Learning Objectives*, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/2012-Learning-Objectives-Final.pdf.

implementing CCA and other IT laws, both predating and postdating CCA. The most recent revision was published in July 2016 and reflects changes from FITARA.

DoD CIO and CMO Offices are Reorganizing More Effectively

Recent DoD leadership changes created new processes intended to achieve goals similar to those envisioned by CCA and changed the nature of the CIO to refocus more strategically on IT issues rather than business management. The FY 2017 NDAA established the office of chief management officer (CMO) and elevated the position to third-highest ranking official in DoD.[26] The FY 2018 NDAA expanded the CMO role, shifting existing authorities over business systems from CIO to CMO.[27] These changes reflected a congressional perception of the CMO as better suited to oversee certain IT investments, encompassing not only the acquisition process but also BPR.[28]

Ultimately, a DoD CMO with broader authority, including budget allocation and reprogramming authority, may be more successful at overseeing business processes and enforcing incremental development. DoD's report to Congress on the CMO reorganization clarified that both team leaders and reform leaders will complete initial BPR assessments across eight lines of business operations including human resources, health care, financial management, and other functional areas.[29] The CCA requirement for BPR will be fulfilled by this process, making the legal provision redundant. Additionally, the FY 2018 NDAA gives the CMO the duty of "serving as the principal advisor to the Secretary and the Deputy Secretary on establishing policies for, and directing, all enterprise business operations of the Department, including planning and processes, business transformation, performance measurement and management, and business information technology management and improvement activities and programs, including the allocation of resources for enterprise business operations and unifying business management efforts across the Department."[30] Maintaining and reinforcing this budget authority is necessary for empowering the CMO and ensuring effective IT management and BPR.

Other recent changes underline that the CIO role is in transition. The Navy announced in March 2018 that it would consolidate the functions of CIO and CMO under a single office. A Navy memo stated that the consolidation would "contribute to a leaner, more focused approach to business transformation and will help facilitate greater cross-enterprise collaboration on critical issues that

---

[26] Section 901 of FY 2017 NDAA, Pub. L. No. 114-328 (2016).
[27] Section 910 of FY 2018 NDAA, Pub. L. No. 115-91 (2017).
[28] As the SASC Report on the FY 2018 NDAA explains, "Decisions related to business systems could be more effectively handed [sic] by the entity coordinating business management and reform across the Department. Therefore, the committee recommends the shifting of several major Chief Information Officer functions to the Chief Management Officer organization, and consolidation of the rest in a Chief Information Warfare Officer." (page 210) The report also notes, "The committee's intent is not for the addition of large internal bureaucracy to manage these new responsibilities, and expects the Chief Management Officer to instead gather those personnel currently fulfilling these roles within the Office of the Secretary of Defense and the Chief Information Officer organization."
See *Senate Armed Services Committee Report to Accompany S.1519 – National Defense Authorization Act for Fiscal Year 2018,* July 10, 2017, accessed June 18, 2018, https://www.congress.gov/115/crpt/srpt125/CRPT-115srpt125.pdf.
[29] Office of the Secretary of Defense, *Report to Congress Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization* ("Section 901 Report"), August 2017, accessed June 18, 2018, https://www.defense.gov/Portals/1/Documents/pubs/Section-901-FY-2017-NDAA-Report.pdf.
[30] Section 910 of FY 2018 NDAA, Pub. L. No. 115-91 (2017). Codified at 10 U.S.C. § 132a.

require an enterprise approach."[31] Then-HASC Chairman Mac Thornberry's initial version of the FY 2019 NDAA would have eliminated all but five of the CIOs in DoD.[32] The final, amended version of the bill did not contain this language.[33]

The CIO role is evolving as technology evolves, with additional demands creating new responsibilities, positions, and structures that do not fit neatly into CCA's concept of a single CIO. Many people familiar with CCA compliance believe planning for cybersecurity to be among the most important elements of CCA. Responsibility for DoD's cybersecurity strategy rests with the Deputy CIO for Cyber Security, and component CIO offices similarly have individuals in the role of chief information security officer (CISO). In July 2018, DoD hired its first chief data officer (CDO), a position already created in the Air Force and Army. The rise of the CISO, CMO, and now CDO reveals the complexity of the CIO office along with a need for flexibility and collaborative accountability.

Document-based Compliance Is Slow and Adds Little Value

CCA compliance is completed using a series of standardized document approvals that take months to complete and rarely improve acquisition outcomes.[34] Instead of having an ongoing relationship with programs, CIO offices are often only asked to provide feedback to programs when they are facing urgent demands and impending milestone deadlines. Feedback at these points is typically administrative rather than substantive in nature. Numerous respondents shared this view of CCA compliance, voiced in conversations with the Military Services and Defense Agencies and from both the program and CIO perspective.

A representative from the Army's PEO enterprise information system office confirmed that he had never seen a CCA documentation package rejected for not being compliant.[35] The Army representative stated that the tool used to verify CCA documentation "is basically checking the box that the program is compliant."[36] A Military Service's CIO office CCA administrator stated that he would welcome the opportunity to be more involved with programs as they are developing their program strategy (specifically by working with integrated product teams), but described this approach as a luxury he did not have.[37]

---

[31] Under Secretary of the Navy Thomas B. Modly, "Restructure of Secretariat Functions," March 16, 2018, accessed June 18, 2018, http://www.navy.mil/undersec/docs/Secy_reorg_memo.pdf.
[32] See Section 917 of HASC Chairman's Mark of H.R. 5515, "FY19 National Defense Authorization Bill," accessed June 18, 2018, https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/wysiwyg_uploaded/FY19%20NDAA%20Chairman%27s%20Mark%20Final.pdf.
[33] H.R. 5515 ("National Defense Authorization Act for Fiscal Year 2019"), accessed June 18, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[34] Program managers; DoD component CIOs; Deputy Assistant Secretary of Defense, Command, Control, Communications, Cyber, and Business Systems (DASD (C3CB)); and Navy Program Executive Officer of Enterprise Information Systems (PEO EIS), interviews with Section 809 panel, 2017 and 2018.
[35] Representative from Army's PEO EIS office, email with Section 809 Panel, August 16, 2017.
[36] Ibid.
[37] Military Service's CIO's office CCA administrator, interview with Section 809 Panel, September 2017.

CCA compliance is confirmed at major milestones, after full requirements have been developed.[38] It does not guarantee systems are initially designed for interoperability, information assurance, or risk management framework compliance, contrary to evidence-based practices. One official stated,

> *Doing the checklist, submitting it for review, and signing off on the checklist became a separate activity, almost an end unto itself. The engagement between program and CIO oversight started to be all about the checklist: when will the complete package be submitted, how long will it take to review, what more information do you need. The actual exchange flow waited for the run-up to the milestone, while other program efforts continued moving forward.*[39]

The revised process in DoDI 5000.75 is intended to address some of this situation, so that "program and oversight…interact more frequently as the program progresses, through either direct engagement upfront or preplanned technical and management assessments." DoDI 5000.75 governs only DBSs, however, which represent a fraction of DoD IT investments.

In a 2015 GAO survey of documentation requirements for 24 major weapon system programs, respondents consistently ranked CCA compliance as a low-value process and added commentary that CCA is out of date with current acquisition practices. This study also showed that it took on average 10 months to process CCA documentation, about 6 months to complete and another 4 months for review.[40]

Guidance in DoD components confirms this slow turnaround. The Air Force's compliance guide, for instance, stipulates, "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."[41] In December 2016, the Air Force conducted a Rapid Improvement Event to streamline the CCA process. People involved in that study explained that CCA compliance was seen as a *chokepoint* in the acquisition process. One program took 525 days to produce and coordinate CCA documents. Legacy programs and new starts commonly take 13 months to coordinate approvals, delays added on top of the time required to create documents.[42] One Air Force enterprise architect reported that CCA compliance has nothing to do with the program's execution, adding that the Air Force Research Laboratories have an office just for compliance. As a result of this study, the Air Force delegated approval authority to the PM for eight of the 11 elements. The Air Force CIO retains approval for elements 8, 9, and 11.

---

[38]According to 2008 DoD guidance, the CIO is required to "certify, prior to each milestone A, B, or full rate production approval (or their equivalent), that a Major Automated Information System (MAIS) is being developed in accordance with the Clinger–Cohen Act (CCA) of 1996. It also requires the DoD CIO to submit timely notification of such certifications to the congressional defense committees." (DoD Deputy Chief Information Officer Memorandum: *Clinger–Cohen Act (CCA) Compliance Certification of Major Automated Systems (MAIS) for Fiscal Year (FY) 2008,* March 13, 2008).

[39] DoD office of Deputy Assistant Secretary of Defense for Command, Control, and Communication, Cyber, and Business Systems (DASD C3CB), email to Section 809 Panel, August 7, 2017.

[40] GAO, *DOD Should Streamline Its Decision-Making Process for Weapon Systems to Reduce Inefficiencies*, *GAO-15-192,* February 2015, accessed July 2, 2018, http://www.gao.gov/assets/670/668629.pdf.

[41] Clinger–Cohen Act (CCA) Compliance, AFMAN 17-1402, 7-8 (2018).

[42] Interview with Section 809 Panel, February 2, 2018.

DISA Defense Information Technology Contracting Organization reported that it takes 6 to 8 weeks to process CCA compliance documentation. The people processing the approvals often lack the background to provide guidance, so it becomes a paperwork exercise instead of strategic planning.[43] The Army CIO office reported that CCA packages spend additional time going through legal review with the Army Office of General Counsel.[44] Some of this time comes from mapping existing program documents to the CCA compliance checklist tool. One individual involved in this compliance exercise suggested that documents are simply too long to be useful, giving the example of mining a 150-page acquisition strategy for evidence of compliance. He observed that briefings can produce better feedback for programs than documents, and can do so more efficiently. The same CIO office said that the CIO review of these documents does not affect other enterprise decisions or strategies.

The 2016 revision of OMB Circular A–130 acknowledges the checklist mentality problem in federal IT acquisition. The circular emphasizes three strategic priorities: real-time knowledge of the environment, proactive risk management, and shared responsibility for privacy and security of information. The authors of the circular explain that "we must move away from periodic, compliance-driven assessment exercises [….] Throughout the circular, we make clear the shift away from check-list exercises and toward the ongoing monitoring, assessment, and evaluation of Federal information resources."[45] The need for continuous monitoring of federal and DoD IT suggests the processes put in place by CCA, despite good intentions, are no longer relevant.

CCA Overlaps with Other IT Legislation, Regulations, and Policy

Overlap exists between CCA compliance and other laws, regulations, and policy. These other requirements arguably meet the same needs that CCA was intended to fulfill. Table C-2 (in Appendix C) details these many redundancies, which include overlap with the planning, programming, budgeting, and execution process; statutes such as 10 U.S.C. § 2222, Information Technology: Additional Responsibilities of Chief Information Officers, and 10 U.S.C. § 2223a, Information Technology Acquisition Planning and Oversight Requirements, as well as other DoD policies. As discussed above, CCA compliance is additive to traditional acquisition processes, which require programs to demonstrate similar strategic planning in such documents as the Acquisition Strategy and Economic Analysis.

Newer federal laws governing IT acquisition better reflect the current acquisition and technology environment. The Federal Information Security Management Act (FISMA) of 2002 was enacted as part of the 2002 E-Government Act and was amended in 2014 by the Federal Information Security Modernization Act to address evolving security concerns.[46] FISMA added several new cybersecurity provisions to Title 44 of U.S. Code and amended CCA provisions to clarify requirements for

[43] DISA Defense Information Technology Contracting Organization (DITCO), interview with Section 809 Panel, February 14, 2018.
[44] Army CIO office, interview with Section 809 Panel, February 2018.
[45] "Managing Federal Information as a Strategic Resource," Office of Management and Budget, July 27, 2016, accessed October 23, 2018, https://obamawhitehouse.archives.gov/blog/2016/07/26/managing-federal-information-strategic-resource
[46] See Title III of E-Government Act of 2002, Pub. L. No. 107-347 (2002). Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014).

information security.[47] Other changes included less overall reporting and more use of continuous monitoring in systems.[48]

In many ways, FITARA has created a more modern process for achieving transparency and oversight. As mentioned above, FITARA bolstered much of CCA that had not been fully implemented and codified much of the guidance that OMB had issued in the preceding decade. FITARA led to the IT Dashboard, a publicly available tool showing agencies' spending on IT and their performance on the biannual FITARA scorecard, which originally assessed agencies on five metrics.[49] These scorecard metrics have been updated to reflect changes in technology and federal IT laws, with 2018 bringing two new metrics for cybersecurity and agency implementation of the Modernizing Government Technology (MGT) Act.[50] Because the scorecard is a living document, there is speculation that older metrics will drop off the scorecard once desired progress has been achieved, and more relevant metrics will be added.[51]

DoD remains only partially compliant with FITARA, despite FITARA's successes in improving CIO authority and other features of federal IT management. Originally, the only aspect of FITARA that created new mandates for DoD was the requirement for annual reporting about data center consolidation.[52] The scorecard now assesses DoD, fully or partially, on all metrics except for cybersecurity, and the agency has consistently earned Ds and Fs. DoD has been called to testify about its persistent poor performance on the scorecard, with lawmakers seeing opportunity to use this tool to improve DoD's IT management and reporting.[53]

As IT acquisition continues to rapidly evolve, effective legislation and guidance will look more like FITARA, FISMA, or the MGT Act, all of which provide increased flexibility and more effective oversight. Much of this legislation owes it effectiveness to the precedent set by CCA, but future innovation will not come from processes defined by an existing law that is more than 2 decades old. DoD, in particular, has an acquisition system already robust enough to ensure strategic planning, but, also bureaucratic enough to need help evolving its IT acquisition practices, so it can more readily innovate.

---

[47] See 44 U.S.C. §§ 3551–3559.
[48] "Risk Management: FISMA Background," National Institute of Standards and Technology, Computer Security Resource Center, accessed October 23, 2018, https://csrc.nist.gov/Projects/Risk-Management/Detailed-Overview.
[49] The original metrics were Agency CIO authority enhancements, Transparency and risk management, Portfolio review, Data center optimization initiative, whether CIO's boss is Secretary or Deputy Secretary, and CIO Status. In 2017, the Scorecard changed to include metrics on software licenses and whether CIOs were acting or permanent. See www.itdashboard.gov and "A Look Back: How the FITARA Scorecards Have Evolved," MeriTalk, accessed September 6, 2018, https://www.meritalk.com/articles/a-look-back-how-the-fitara-scorecards-have-evolved/.
[50] Oversight and Government Reform, *OGR Biannual Scorecard – May 2018* (May 2018 FITARA Scorecard), accessed September 6, 2018, https://oversight.house.gov/wp-content/uploads/2018/05/OGR-Scorecard-6.0-v2.pdf.
[51] "Agencies Could Be Graded on More than FITARA under New Scorecard," Aaron Boyd, NextGov.com, accessed September 6, 2018, https://www.nextgov.com/cio-briefing/2018/03/agencies-could-be-graded-more-fitara-under-new-scorecard/146694/.
[52] DoD, "Plan for Implementing the Federal Information Technology Acquisition Reform Act (FITARA)," October 15, 2015, Enclosure 1, accessed June 18, 2018, https://www.defense.gov/Portals/1/Documents/DoD_FITARA_Implementation_Plan_Oct15.pdf.
[53] "Hearing: The Federal Information Technology Acquisition Reform Act (FITARA) Scorecard 6.0," Oversight and Government Reform, accessed September 6, 2018, https://oversight.house.gov/hearing/the-federal-information-technology-acquisition-reform-act-fitara-scorecard-6-0/.

Conclusions

In 1996, CCA instilled discipline in federal IT acquisition, but it has outlived its usefulness. The real-world effect of CCA compliance has been to add complexity and checklist-based documentation requirements atop DoD's existing acquisition bureaucracy, creating a slow and frustrating process for programs that provides limited value to CIOs.

DoD's IT acquisition can be made more efficient by reducing redundancies and checklist requirements. CCA requires many of these redundant and low value-added provisions from which DoD should be exempted. Several initiatives recognize the burden of CCA compliance and propose solutions to mitigate it, including the revised guidance for business systems in DoDI 5000.75 and the Air Force's streamlined process for CCA compliance.

Exempting DoD from CCA is one step in streamlining IT acquisition, but not the final step. DoD must continue to shift toward more strategic, collaborative processes that restore accountability to the appropriate individuals. It is imperative that DoD continue to follow many of the best practices mandated by CCA and enforced by newer laws, including continuous assurance of cybersecurity, BPR, and the adoption of commercial technology and processes. Congress should not repeal CCA provisions altogether, because they may remain useful for civilian agencies.

Congress should exempt DoD from the CCA provisions in Title 40 and instruct DoD to replace the 11 CCA checklist requirements in the DoDI 5000.02 and other acquisition policy documents with a truly strategic, outcome-oriented IT acquisition process that empowers the lower-level workforce, shortens delivery schedules, and avoids paperwork for its own sake. Once Congress has approved the exemption of DoD from CCA provisions, DoD and OMB should modify existing policy and guidance documents to reflect these changes.

Implementation

Legislative Branch

- Exempt DoD from 40 U.S.C. Subtitle III (Clinger–Cohen Act).
- Delete 10 U.S.C. § 2224 note (Strategy on Computer Software Assurance), which has become obsolete.[54]
- Direct DoD, in the legislative history of this exemption, to eliminate all 11 of its CCA-related CIO document approval requirements. These include the document approval requirements with language derived from 40 U.S.C. Subtitle III, 41 U.S.C. § 2308, which requires that the FAR support modular contracting, and 10 U.S.C. § 2224 note.
- Direct DoD leadership to acquire IT strategically by empowering the lower-level workforce, shortening delivery schedules, and avoiding paperwork for its own sake.

[54] This note section of Title 10 required DoD to develop by the end of FY 2011 a "strategy for assuring the security of software and software-based applications." As the deadline expired years ago, the section is no longer relevant. See Section 932 of FY 2011 NDAA, Pub. L. No. 111-383 (2011).

Executive Branch

- Revise DoDI 5000.02 to eliminate the checklist requirement under Table 10 of Enclosure 1, CCA Compliance. The checklist should be replaced with guidance established by the CMO and other officials as empowered by the Secretary of Defense.[55]

- Revise DoDI 5000.02 to eliminate the CCA requirements under Section 3 of Enclosure II, Requirements Applicable to all Programs Containing Information Technology.

- Revise DoDI 5000.74 to eliminate Section 2 and Table 2 of Enclosure 7, Acquisition Considerations for IT within Services.[56]

- Revise DoDI 5000.75 to delete references to CCA, including in Table 4: Statutory Requirements of Appendix 4A: Supporting Information.[57]

- Revise Section 9 of Circular A-130, Managing Information as a Strategic Resource to exempt DoD from the CCA provisions in Title 40.[58]

Implications for Other Agencies

- Other federal agencies may not have the sophisticated IT acquisition oversight processes that exist in DoD. For this reason, repealing Subtitle III of Title 40 entirely might disrupt civilian agencies' IT acquisitions. Exempting DoD, however, would not have implications for other agencies.

[55] Operation of the Defense Acquisition System, DoDI 5000.02 (2017).
[56] Defense Acquisition Services, DoDI 5000.74 (2017), Enclosure 7: Acquisition Considerations for IT within Services.
[57] Business Systems Requirements and Acquisition, DoDI 5000.75 (2017), Appendix 4A: Supporting Information.
[58] OMB Circular No. A-130, *Managing Information as a Strategic Resource,* updated July 28, 2016, Section 9, 26, accessed June 20, 2018, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

RECOMMENDED REPORT LANGUAGE

SEC. ___. EXEMPTION OF DEPARTMENT OF DEFENSE FROM CLINGER-COHEN ACT.

The section would exempt the Department of Defense from the Clinger-Cohen Act. The committee notes that at the time of its enactment in 1996, the Clinger-Cohen Act instilled discipline in information technology acquisitions within the federal agencies, including the Defense Department. In recent years, however, the real-world effect of Clinger-Cohen Act compliance has been to add complexity and checklist-based documentation requirements atop the existing acquisition bureaucracy. This has created a slow and frustrating process that provides limited value to the Department or its Chief Information Officers in executing a disciplined method for IT acquisition.

In the committee's view, exempting the Department of Defense from the Clinger-Cohen Act is a necessary condition for streamlining information technology acquisition. The committee notes that such streamlining should also include a continuing shift by the Department away from checklists and toward a more strategic, collaborative process that places both authority and accountability in the hands of appropriate individuals. This collaborative process should empower the workforce at all levels, shorten delivery schedules, and avoid paperwork for its own sake.

The committee emphasizes that the Department should continue to follow the best practices laid out under the Clinger-Cohen Act and subsequent laws. These best practices include continuous assurance of cybersecurity, business process reengineering, and the adoption of commercial technology and processes.

The committee does not recommend repealing the Clinger-Cohen Act since it may remain a useful tool for civilian agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

SEC. ___. EXEMPTION OF DEPARTMENT OF DEFENSE FROM CLINGER-COHEN ACT.

(a) EXEMPTION.—Paragraph (2) of section 11101 of title 40, United States Code, is amended by inserting before the period at the end the following: ", but does not include the Department of Defense or a military department".

(b) REPEAL OF OBSOLETE PROVISION.—Section 932 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383; 10 U.S.C. 2224 note), relating to a strategy on computer software assurance, is repealed.

Title 40—PUBLIC BUILDINGS, PROPERTY, AND WORKS

SUBTITLE III—INFORMATION TECHNOLOGY MANAGEMENT

[NOTE: Subtitle III is popularly known as the Clinger-Cohen Act]

CHAPTER 111—GENERAL

Sec.
11101. Definitions.
11102. Sense of Congress.
11103. Applicability to national security systems.

§11101. Definitions

In this subtitle, the following definitions apply:

(1) COMMERCIAL ITEM.—The term "commercial item" has the meaning given that term in section 103 of title 41.

(2) EXECUTIVE AGENCY.—The term "executive agency" has the meaning given that term in section 133 of title 41***, but does not include the Department of Defense or a military department***.

(3) INFORMATION RESOURCES.—The term "information resources" has the meaning given that term in section 3502 of title 44.

(4) INFORMATION RESOURCES MANAGEMENT.—The term "information resources management" has the meaning given that term in section 3502 of title 44.

(5) INFORMATION SYSTEM.—The term "information system" has the meaning given that term in section 3502 of title 44.

(6) INFORMATION TECHNOLOGY.—The term "information technology"—

(A) with respect to an executive agency means 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 by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) 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; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

*****

Section 932 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011

(Public Law 111-383; 10 U.S.C. 2224 note)

~~**SEC. 932. STRATEGY ON COMPUTER SOFTWARE ASSURANCE.**~~

~~(a) STRATEGY REQUIRED.—The Secretary of Defense shall develop and implement, by not later than October 1, 2011, a strategy for assuring the security of software and software-based applications for all covered systems.~~

~~(b) COVERED SYSTEMS.—For purposes of this section, a covered system is any critical information system or weapon system of the Department of Defense, including the following:~~

~~(1) A major system, as that term is defined in section 2302(5) of title 10, United States Code.~~

~~(2) A national security system, as that term is defined in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].~~

~~(3) Any Department of Defense information system categorized as Mission Assurance Category I.~~

~~(4) Any Department of Defense information system categorized as Mission Assurance Category II in accordance with Department of Defense Directive 8500.01E.~~

~~(c) ELEMENTS.—The strategy required by subsection (a) shall include the following:~~

~~(1) Policy and regulations on the following:~~

~~(A) Software assurance generally.~~

~~(B) Contract requirements for software assurance for covered systems in development and production.~~

~~(C) Inclusion of software assurance in milestone reviews and milestone approvals.~~

(D) Rigorous test and evaluation of software assurance in development, acceptance, and operational tests.

(E) Certification and accreditation requirements for software assurance for new systems and for updates for legacy systems, including mechanisms to monitor and enforce reciprocity of certification and accreditation processes among the military departments and Defense Agencies.

(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

(2) Allocation of adequate facilities and other resources for test and evaluation and certification and accreditation of software to meet applicable requirements for research and development, systems acquisition, and operations.

(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber attack by acquiring and improving automated tools for—

(A) assuring the security of software and software applications during software development;

(B) detecting vulnerabilities during testing of software; and

(C) detecting intrusions during real-time monitoring of software applications.

(4) Mechanisms providing the Department of Defense with the capabilities—

(A) to monitor systems and applications in order to detect and defeat attempts to penetrate or disable such systems and applications; and

(B) to ensure that such monitoring capabilities are integrated into the Department of Defense system of cyber defense-in-depth capabilities.

(5) An update to Committee for National Security Systems Instruction No. 4009, entitled 'National Information Assurance Glossary', to include a standard definition for software security assurance.

(6) Either—

(A) mechanisms to ensure that vulnerable Mission Assurance Category III information systems, if penetrated, cannot be used as a foundation for penetration of protected covered systems, and means for assessing the effectiveness of such mechanisms; or

(B) plans to address critical vulnerabilities in Mission Assurance Category III information systems to prevent their use for intrusions of Mission Assurance Category I systems and Mission Assurance Category II systems.

(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems.

(d) REPORT.—Not later than October 1, 2011, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the strategy required by subsection (a). The report shall include the following:

(1) A description of the current status of the strategy required by subsection (a) and of the

~~implementation of the strategy, including a description of the role of the strategy in the risk management by the Department regarding the supply chain and in operational planning for cyber security.~~

~~(2) A description of the risks, if any, that the Department will accept in the strategy due to limitations on funds or other applicable constraints.~~