United States Government Accountability Office

Report to Congressional Committees

November 2020

DEFENSE ACQUISITIONS

Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance

GAO-21-68

GAO Highlights

Highlights of GAO-21-68, a report to congressional committees

November 2020

DEFENSE ACQUISITIONS

Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance

Why GAO Did This Study

Cyberspace is a growing, human-made environment that touches many parts of life, including education, economic development, health, and other public services. For DOD, cyberspace is as important as the traditional land, sea, air, and space warfighting domains. To integrate these disparate cyber systems into a more cohesive capability, U.S. Cyber Command introduced an overarching vision for cyber capabilities known as the Joint Cyber Warfighting Architecture.

The Senate Armed Services Committee included a provision for GAO to review the status of the JCWA. This report (1) describes the JCWA concept, systems, and planned capabilities; and (2) assesses the extent to which DOD has defined interoperability goals and a governance structure to guide JCWA cyber system acquisitions.

To do this work, GAO reviewed acquisition program documents and joint cyber warfighting requirements information. GAO conducted interviews with DOD officials from key cyber warfighting organizations, including Cyber Command, as well as JCWA program offices and stakeholders.

What GAO Recommends

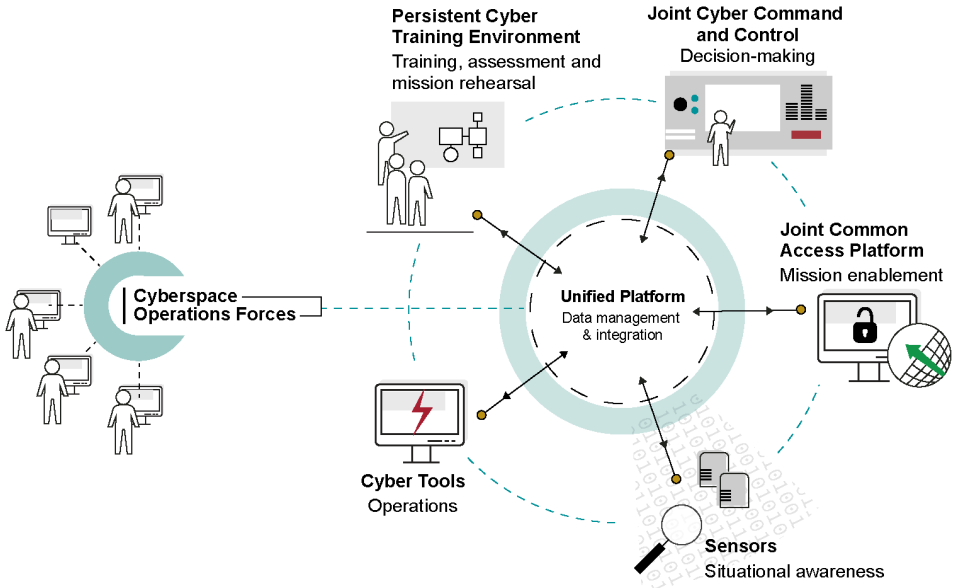
GAO is making two recommendations for Cyber Command to define and document JCWA interoperability goals as well as the JCWA governance structure roles and responsibilities of key offices. DOD concurred with the first and partially concurred with the second recommendation. DOD's plans are consistent with the intent of GAO's recommendations.

View GAO-21-68. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov.

What GAO Found

U.S. Cyber Command created the Joint Cyber Warfighting Architecture (JCWA) as a concept to integrate cyber warfighting systems. Department of Defense (DOD) officials told GAO that the JCWA is to serve as a guiding concept for cyber warfighting acquisitions and investment decisions, rather than a traditional architecture that DOD's systems engineering guidance states would address functions, relationships, and dependencies of constituent systems. As of August 2020, the JCWA consisted of a diagram of systems, including four acquisition programs and the cyber tools and sensors that support cyber warfighting (see figure). Three of these programs were in development before Cyber Command began efforts to link them together to create a more integrated set of systems.

Joint Cyber Warfighting Architecture Conceptual Diagram



Source: GAO representation of Department of Defense documentation. | GAO-21-68

Although the primary element of the JCWA concept, according to Cyber Command officials, is the interoperability and information sharing among these systems, Cyber Command has not defined JCWA interoperability goals for constituent systems. The lack of defined goals is due in part to most programs now included in the JCWA being in development prior to the concept being initiated. However, goals are essential to ensuring that operators have system capabilities as anticipated. Cyber Command recently established two new offices that would be responsible for prioritizing JCWA program acquisition requirements but as of August 2020, had not yet assigned roles and responsibilities for these key offices. Until Cyber Command develops a governance structure for the new offices with defined roles and responsibilities, it risks delays in providing needed joint cyber warfare capabilities.

Contents

Abbreviations

DevSecOps	Development, Security, and Operations
DOD	Department of Defense
DODIN	DOD Information Network
JCWA	Joint Cyber Warfighting Architecture

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 19, 2020

Congressional Committees

Cyberspace is a growing, human-made environment that reaches into many parts of life, including education, economic development, health, and other public services. It has also evolved into an arena of conflict for nation-states and independent groups or actors. From a military perspective, cyberspace is as important as the traditional land, sea, air, and space warfighting arenas or domains. Military actions in cyberspace cover a spectrum of actions: from defensive activities that protect vulnerable networks to offensive operations that damage enemy capabilities.

Since 2016, the Department of Defense (DOD) has invested in a range of joint cyber warfighting systems and capabilities to support the full spectrum of military cyber operations carried out by DOD's Cyberspace Operations Forces—units of cyber operators that support the armed services and combatant commands across all warfighting domains. In 2019, to integrate these disparate systems into a more cohesive capability, U.S. Cyber Command introduced an overarching vision for all cyber warfighting known as the Joint Cyber Warfighting Architecture (JCWA).

Senate Report 116-48, accompanying the National Defense Authorization Act for Fiscal Year 2020, includes a provision for us to review the status of the JCWA. This report (1) describes the JCWA concept, systems, and planned capabilities; and (2) assesses the extent to which DOD has defined interoperability goals and a governance structure to guide cyber system acquisitions associated with the JCWA.

To address our first objective, we reviewed program briefs, budget information, plans, and requirements documents from 2017-2020 to identify the capabilities U.S. Cyber Command procures as part of the JCWA. We obtained and reviewed individual acquisition program documentation from each of the ongoing JCWA acquisitions (Unified Platform, Joint Cyber Command and Control, the Persistent Cyber Training Environment, and the Joint Common Access Platform). We used these acquisition documents to identify program acquisition strategies and interviewed cognizant program officials to discuss program progress and confirm details.

To address our second objective, we met with Cyber Command officials to discuss the origins of the JCWA and how it changed over time. We obtained available documentation of the JCWA, including early iterations of the Unified Platform program and cyber warfighting Initial Capabilities Documents. To identify the extent to which Cyber Command developed key goals for the JCWA and its governance structure, we reviewed these documents and interviewed JCWA stakeholders to assess these steps against our prior work on the Government Performance and Results Act and federal internal control standards related to achieving management objectives.[1] We obtained cyber warfighters' perspectives on the JCWA by interviewing officials from each service's cyber component: Army Cyber Command, Marine Corps Forces Cyberspace Command, Navy's Fleet Cyber Command/Tenth Fleet, and Sixteenth Air Force (Air Forces Cyber). We also interviewed officials from U.S. Cyber Command, the Office of the Director, Operational Test and Evaluation; Office of Cost Assessment and Program Evaluation; Office of the Under Secretary of Defense for Acquisition and Sustainment; Office of the DOD Principal Cyber Advisor; and the Office of the Under Secretary of Defense for Policy.

We limited our analysis to unclassified information sources due to COVID-19-related restrictions that limited travel and access to systems we use to process sensitive or classified information. We plan to include these sources in future work.

We conducted this performance audit from October 2019 to November 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1]GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996) and *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

Background

DOD conducts cyber operations through its Cyberspace Operations Forces, which include the Cyber Mission Force. U.S. Cyber Command is responsible for commanding DOD's cyberspace operations forces, as well as identifying acquisition requirements to support cyber operations.

DOD Cyber Operations

Cyber operations entail cyber warfare, both offensive and defensive actions in cyberspace. To defend against and engage cyber adversaries, DOD relies on three primary types of cyber operations:

DOD Information Network (DODIN) Operations. The DODIN is a set of information technology capabilities and processes for collecting, processing, storing, disseminating, and managing information needed by DOD personnel. According to DOD documentation, the DODIN comprises all of DOD cyberspace, including classified and unclassified global networks and many other components and weapon systems such as aircraft and ships that rely on connected devices, networks, and software.[2] DODIN operations entail actions to secure, configure, operate, extend, maintain, and sustain DOD cyberspace.

Defensive Cyber Operations. DOD executes defensive cyber operations to defend the DODIN or, when ordered, non-DOD networks. Defensive missions defeat specific threats that have bypassed, breached, or are threatening to breach security measures. Cyber forces conduct defensive missions in response to specific threats of attack, exploitation, or other effects of malicious cyberspace activity. Their actions can include outmaneuvering or interdicting adversaries or returning a compromised network to a secure and functional state.[3]

Offensive Cyber Operations. According to DOD, offensive cyber missions extend military operations in and through foreign cyberspace in support of national security objectives. All actions cyber forces conduct outside of DOD-protected cyberspace are considered offensive missions.

Examples of Cyber Command's cyber operations include supporting forces in Iraq and Afghanistan, defending the 2018 midterm elections, and fighting terror groups in cyberspace.

[2]Chairman of the Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (June 8, 2018).

[3]*Joint Publication 3-12*.

Cyberspace Operations Forces and the Cyber Mission Force

DOD relies on a variety of military and civilian personnel to conduct cyber operations through its Cyberspace Operations Forces, which include Cyber Command subordinate Command elements, DOD Component Network Operations Centers, and Cybersecurity Service Providers, special capability providers, and specially designated units. As we noted above, part of the Cyberspace Operations Forces is the Cyber Mission Force, consisting of over 6,000 military, civilian, and contractor personnel from across the military services. We previously reported that the Cyber Mission Force primarily includes the following kinds of units:

- Combat Mission Teams and their associated Combat Support Teams support combatant commands by providing offensive cyberspace capabilities in support of operational plans and contingency operations.
- National Mission Teams and their associated Mission Support Teams defend the United States and its interests against cyberattacks of significant consequence.[4]
- Cyber Protection Teams augment traditional defensive measures and defend priority DOD networks and systems against priority threats.

U.S. Cyber Command began creating the Cyber Mission Force in 2013 and declared full operational capability in 2018.[5] DOD currently has 133 teams from across the military services, including Air National Guard and Air Force Reserve personnel. Cyber Command plans for a second wave of 21 additional Cyber Protection Teams with Army Reserve and Army National Guard personnel to reach full operational capability by fiscal year 2024.[6]

U.S. Cyber Command History

As DOD's reliance on computers, networks, and software-intensive systems has grown, the department's approach to managing its use of cyberspace has also evolved. DOD initially developed a series of joint task forces to address computer network defense in the 1990s. In October 2000, U.S. Space Command formally took control of DOD's

[4]The National Mission Teams and Combat Mission Teams have support teams that typically include linguists, analysts, and other specialists.

[5]According to DOD officials, full operational capability for Cyber Mission Force teams is an evaluation that the team can perform its mission as designed.

[6]GAO, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, D.C.: Mar. 6, 2019).

computer network activities.[7] Then, in 2002, the computer network defense mission moved to U.S. Strategic Command. Offensive cyber operations also fell under Strategic Command but under the oversight of the National Security Agency.

In the 2004 *National Military Strategy*, the Joint Chiefs of Staff declared cyberspace a domain or warfighting arena, alongside air, land, sea, and space. Strategic Command reorganized cyber operations, though offensive operations remained under dual oversight with the National Security Agency. In 2008, DOD completed several reviews of the organization of its cyber functions, roles, and missions, leading department leadership to consider merging offensive and defensive cyber operations. In November 2008, the Secretary of Defense directed the creation of a new subunified command to Strategic Command: U.S. Cyber Command. As part of this effort, DOD merged offensive and defensive cyber operations under a new "dual-hat" structure that made the Commander of Cyber Command also the Director of the National Security Agency. DOD formally created Cyber Command in June 2009.

In recognition of the growing centrality of cyberspace to U.S. national security, the Secretary of Defense recommended elevating U.S. Cyber Command to a unified combatant command in August 2017. At presidential direction, Cyber Command became a unified combatant command in May 2018. Cyber Command relies on forces drawn from the military service cyber components and their cyber component commands, which the services began developing in 2009. Between 2013 and 2018, Cyber Command began organizing and developing the Cyber Mission Force with the service cyber components.

Cyber Command Acquisitions

In the National Defense Authorization Act for Fiscal Year 2016, Congress granted acquisition authority up to $75 million to U.S. Cyber Command to support cyber operations—most other combatant commands do not have

[7]DOD originally established U.S. Space Command in 1985 but deactivated the command in 2002 and transferred its responsibilities to U.S. Strategic Command. DOD re-established Space Command in August 2019.

such an authority.[8] However, Cyber Command currently relies on Executive Agents, such as the Air Force, and other agreements through the military services for acquisition of the four main components of the JCWA.[9] Table 1 identifies the primary stakeholders in JCWA acquisitions.

Table 1: Key Department of Defense (DOD) Stakeholders in Joint Cyber Warfighting Architecture (JCWA) Acquisitions

Stakeholder	Role
U.S. Cyber Command	Combatant command responsible for cyber operations and overseeing Cyberspace Operations Forces
Service Cyber Components: • Army Cyber Command • Marine Corps Forces Cyberspace Command • Fleet Cyber Command/Tenth Fleet (Navy) • Sixteenth Air Force (Air Forces Cyber)	Each component is the service's cyber warfighting element that provides personnel to Cyberspace Operations Forces as well as to support other kinds of cyber operations. They also provide subject matter experts to cyber acquisition programs to support development.
Service Component Acquisition Executives: • Assistant Secretary of the Army for Acquisition, Logistics, and Technology • Assistant Secretary of the Air Force for Acquisition, Technology and Logistics	Officials within the DOD components with Decision Authority for program execution for current and planned programs within the JCWA concept
Acquisition Program Executive Officers (PEOs): • Army PEO Intelligence, Electronic Warfare, and Sensors • Army PEO Simulation, Training, and Instrumentation • Air Force PEO Command, Control, Communications, Intelligence and Networks	Responsible for leading acquisition program offices, which develop and acquire the relevant technological solution. The PEOs identified are responsible for current and planned acquisition programs within the JCWA concept.
Principal Cyber Advisor	Office of the Under Secretary of Defense for Policy staff advisor to the Secretary of Defense on military and civilian cyber forces and activities
Under Secretary of Defense for Acquisition and Sustainment	Defense Acquisition Executive
Under Secretary of Defense for Research and Engineering	DOD authority for development and oversight of technology

[8]Pub. L. No. 114-92, § 807 (2015). The Senate Report to the National Defense Authorization Act for Fiscal Year 2021 included a provision to remove the $75 million cap on cyber acquisitions obligations and expenditures. However, the report cautioned Cyber Command against attempting expansive acquisition efforts itself, including major defense acquisition programs, as the command lacks the capacity and expertise to manage large acquisition programs. S. Rep. No. 116-236, 116th Cong, 2d Sess. 338 (2020), (accompanying S. 4049, National Defense Authorization Act for Fiscal Year 2021).

[9]According to DOD Directive 5101.1, *DOD Executive Agent*, a DOD Executive Agent is the head of a DOD component to whom the Secretary of Defense or Deputy Secretary assigned specific responsibilities, functions, and authorities to provide defined levels of support for operational missions or administrative or other designated activities that involve two or more of the DOD components. For example, the Director of the Defense Information Systems Agency is the Executive Agent for Information Technology Standards, developing and maintaining information technology standards.

Stakeholder	Role
Director of Cost Assessment and Program Evaluation	DOD Principal Staff Assistant for independent cost assessment, program evaluation, and analysis
Chief Information Officer	Senior Advisor for information technology, including national security systems and defense business systems
Director, Operational Test and Evaluation	DOD's operational test authority
Combatant Commands and Services	These components rely on the cyber warfighting systems and Cyberspace Operations Forces to support operations among the land, sea, air, space, and cyber domains.

Source: GAO summary of DOD documents. | GAO-21-68

JCWA Is DOD's Concept for Harmonizing Cyber Warfighting Acquisition Programs

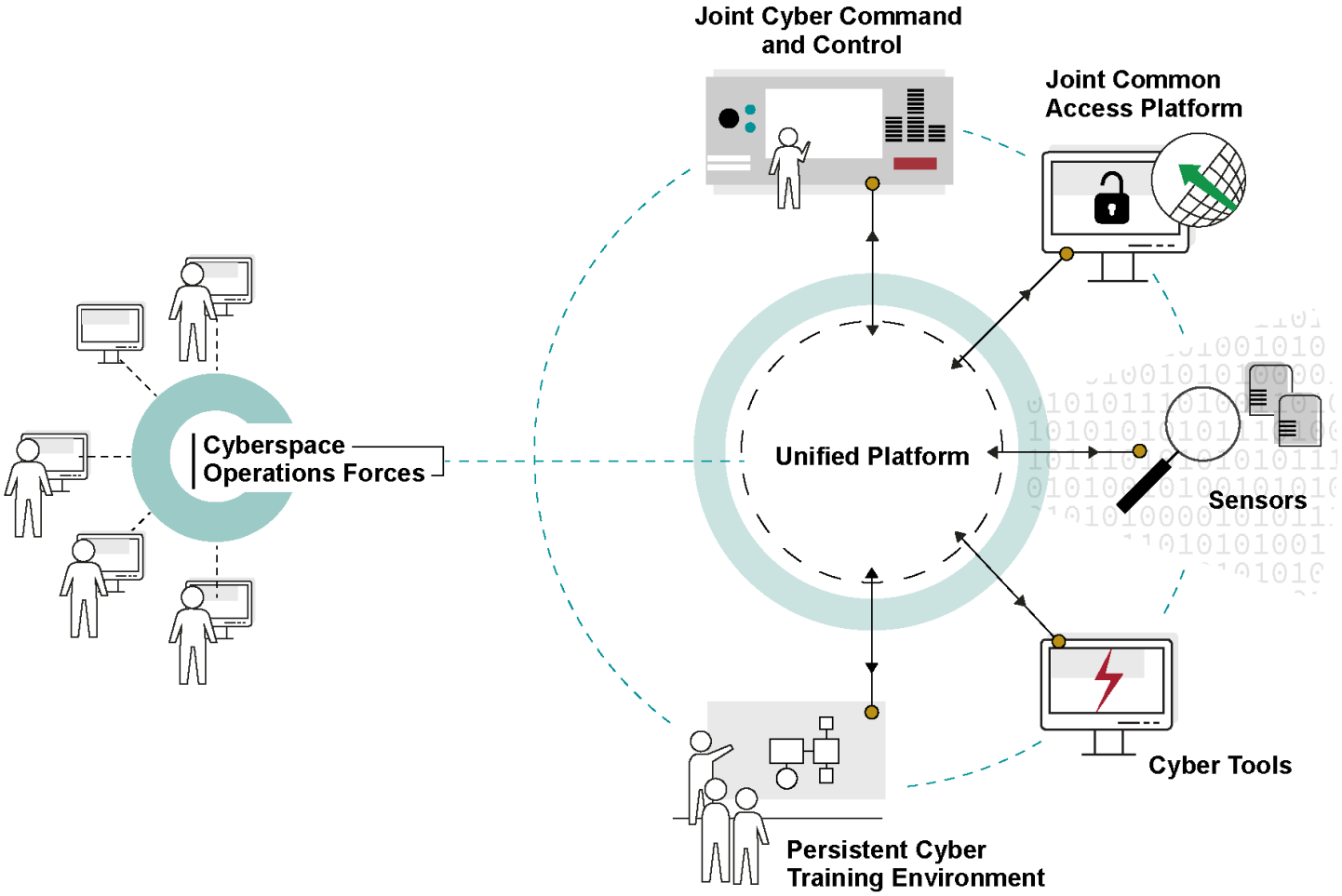
DOD created the JCWA as a concept to harmonize cyber capabilities and their enabling acquisition programs to meet the needs of the Cyberspace Operations Forces. Cyber Command officials told us that the defining goal of the JCWA concept is to develop interoperability among systems to provide a comprehensive, integrated, cyberspace architecture. The Cyberspace Operations Forces primarily rely on independent military services' systems to conduct cyber operations, but common systems that are more interoperable could help unify information sharing and decision-making to support joint operations. However, Cyber Command officials also told us that the JCWA is only loosely an architecture—an idea to bring acquisitions together. In contrast, DOD guidance defines an architecture as part of a system of systems that addresses overall system objectives and encompasses the functions, relationships, and dependencies of constituent systems.[10] According to Cyber Command officials, the JCWA is to serve as a guiding concept for the acquisition of cyber warfighting capability, helping steer requirements and investment decisions.

As of August 2020, the JCWA is defined by a diagram of its programs and systems as outlined below. Cyber Command currently identifies four acquisition programs and two other types of cyber warfighting support as part of the JCWA. Three of these four programs were at least in development before Cyber Command began linking them together to create a more capable set of systems. The programs that already had defined, approved requirements could change depending on how Cyber Command develops the JCWA concept. In November 2020, Cyber Command officials stated that they are making progress in further

[10]Office of the Deputy Undersecretary of Defense for Acquisition and Technology, Systems and Software Engineering, *Systems Engineering Guide for Systems of Systems, Version 1.0*. (Washington, D.C.: Aug. 2008), 19.

defining a JCWA systems architecture. Figure 1 depicts the programs within the JCWA concept and the Cyberspace Operations Forces.

Figure 1: Joint Cyber Warfighting Architecture Conceptual Diagram



Source: GAO representation of Department of Defense documentation. | GAO-21-68

Unified Platform–data management and integration. The purpose of Unified Platform is to function as a data synchronization and access system for cyber warfighters and supporting personnel. According to program officials, Cyberspace Operations Forces will be able to obtain data across the military services to conduct advanced analytics as well as access other JCWA capabilities such as Joint Cyber Command and Control. The program office plans to deliver its next increment by October 2020.

Joint Cyber Command and Control–decision making. The goal of this program is to integrate situational awareness data from multiple sources to support commanders' warfighting decisions. This system relies in part on information from Unified Platform. The majority of the Joint Cyber Command and Control system development efforts are planned to begin during fiscal year 2021.

Persistent Cyber Training Environment–training, assessment, and mission rehearsal. This system provides a platform for training, assessment, and mission rehearsal. The purpose of such a framework is to create an environment for cyber warfighters to configure networks, devices, software, and tools to evaluate and practice operations—for example, simulating the cyberspace disruption of an enemy system to develop new methods and tactics. The system recently supported a large-scale cyber exercise, Cyber Flag 20-2, by successfully connecting users across five countries with a high volume of data traffic.

Joint Common Access Platform–mission enablement. The purpose of the Joint Common Access Platform is to provide a common cyber firing platform for cyber operators to project combat power, using a comprehensive suite of tools. It is the newest JCWA program, initiated in May 2020.

Cyber Tools and Sensors–operations and situational awareness. Cyber tools and sensors do not represent a single program or family of programs, but are multiple ongoing and planned efforts within each service and U.S. Cyber Command. These efforts acquire and deploy cyber tools to defend friendly networks and systems as well as affect the operations of enemy systems. Sensors help deliver intelligence, surveillance, and reconnaissance data to inform cyber warfighters. Examples include tools, such as forensic kits to evaluate enemy actions and sensors such as firewalls to detect adversary activity.

Appendix I includes additional details on these programs.

DOD Has Not Defined Key Goals and Governance Details for the JCWA

DOD created the JCWA as a concept to harmonize cyber capabilities. However, as of August 2020, Cyber Command had not yet progressed beyond diagramming the JCWA concept and beginning efforts to establish supporting offices. Specifically, Cyber Command has not established the goals or objectives that would define interoperability requirements across JCWA systems or a governance structure to prioritize requirements among the programs. According to Cyber Command and acquisition program officials, without clearly defined

interoperability requirements, JCWA programs may face challenges in providing needed capabilities to Cyberspace Operations Forces.

Cyber Command Has Not Established JCWA Interoperability Requirement Goals

Cyber Command has not defined goals for the JCWA that would describe how current and future joint cyber warfighting systems DOD procures would interoperate. The absence of goals is contrary to leading practices we identified in our prior work, which call for program goals to clearly define desired program outcomes.[11] Clearly defined goals explain the purposes of a program and the results an organization intends to achieve. Goals also provide the basis for developing performance measures that help organizations demonstrate progress. By defining JCWA goals, DOD can describe overall system objectives, relationships, and dependencies of its JCWA programs and then develop performance measures to track progress of the JCWA systems as whole.

In the absence of interoperability goals, JCWA programs lack objectives that would implement consistent practices among the programs, such as data tagging standards. Program officials told us they discuss such standards informally, in a "coalition of the willing." This group represents acquisition personnel within the various JCWA programs that coordinate informally to share information, but these efforts are not synchronized through JCWA goals—meaning each program is working independently to become interoperable. According to program officials we interviewed, information sharing, user feedback, and collaboration across Unified Platform, Joint Cyber Command and Control, and the Persistent Cyber Training Environment occur regularly, but this effort between programs is largely ad hoc and does not systematically address broader data sharing or interoperability questions.

According to Cyber Command officials, operational challenges and strategic changes delayed Cyber Command in developing JCWA goals. Cyber Command officials told us that cyber warfighting techniques can evolve rapidly and systems need to support new tactics. However, determining program requirements to support these techniques that can change in hours or days is a challenge. Cyber Command developed the systems to support the pace of cyber warfare before developing broader goals to make the systems interoperate. Further, Cyber Command previously focused on establishing the Cyber Mission Force and since

[11]GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June, 1996).

2018 has reoriented to identify and procure the systems to support cyber warfighting.

According to Cyber Command and acquisition program officials, without clearly defined goals, JCWA programs may fail to interoperate as anticipated, despite early informal successes in information sharing. For example, Cyber Command plans for Unified Platform to provide data analysis to support cyber operations. However, it relies on different systems and Big Data Platforms that collect data in different formats.[12] DOD officials stated that, to make these disparate data readily available for search and analysis within Unified Platform, each system must tag data as they are collected, according to common, pre-determined standards, which Cyber Command has not defined for the JCWA. As a result, Unified Platform may not be able to fully interoperate with other systems' data. If Unified Platform or other JCWA systems are not interoperable, Cyberspace Operations Forces may not have anticipated system capabilities to conduct operations.

Cyber Command Has Not Defined JCWA Governance Structure Roles and Responsibilities

We also found that Cyber Command has not defined roles and responsibilities to manage the JCWA, despite recent efforts to establish new offices. Federal internal control standards state that managers should establish an organizational structure with assigned responsibilities to achieve the organization's objectives.[13] Cyber Command identifies requirements or needs for a cyber warfighting system but relies on the military services to procure these systems. Therefore, developing a governance structure for the JCWA involves organizations outside of Cyber Command.

Officials we interviewed from the DOD organizations involved in cyber warfighting acquisitions, including users, identified a lack of command-level coordination of the JCWA concept that is causing operational confusion and uncoordinated acquisitions. Further, our review of Cyber Command documents shows early efforts underway to develop a governance structure and define command-level coordination, but they are not yet complete or approved. In early 2020, Cyber Command

[12]The Defense Information Systems Agency developed its Big Data Platform to provide a computing solution that is capable of ingesting, storing, processing, sharing, and visualizing multiple petabytes of data from DODIN sources. Three of the service cyber components—Army, Marine Corps, and Air Force—each has its own Big Data Platform and ingest data from its respective cyberspace missions.

[13]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

established its JCWA Integration Office to help address some of the challenges associated with defining and implementing the JCWA concept. According to Cyber Command officials, this office will help develop guidance to integrate the individual JCWA programs into a more holistic, interoperable construct. In addition, Cyber Command officials stated that a new JCWA Capabilities Management Office will work with the JCWA Integration Office to identify and align requirements across JCWA systems based on Cyberspace Operations Forces' needs. Although DOD introduced the JCWA concept in early 2019, Cyber Command officials were still drafting a charter for the JCWA Integration Office and working with other DOD stakeholders on the JCWA concept to establish roles and responsibilities to oversee and implement the JCWA as of August 2020.[14] In November 2020, Cyber Command officials stated they are making progress to define these offices' roles and responsibilities within Cyber Command.

Improved governance would help with prioritizing and coordinating acquisition program requirements and broader JCWA goals. Defined roles and responsibilities for the JCWA Integration Office and JCWA Capabilities Management Office would allow Cyber Command to assess requirements collectively to prioritize cyber warfighting needs across programs. Further, Cyber Command officials stated that these offices will also help ensure program interoperability in support of the JCWA's primary goal. However, until Cyber Command defines these roles and responsibilities, DOD is at risk of delaying needed joint cyber warfighting capabilities.

Conclusions

To defend and fight in cyberspace, DOD is procuring new systems to harmonize cyber functions and promote information sharing. However, DOD and Cyber Command have just begun their work to support these systems as a unified whole. U.S. Cyber Command established program requirements and initiated several of the cyber acquisition programs now identified as part of the JCWA prior to developing the concept itself.

[14]The Senate Armed Services Committee also noted concern that oversight and coordination of the JCWA acquisition programs is inadequate and stated that DOD must exercise deliberate oversight to ensure that acquisition priorities and objectives are aligned to Cyber Command's mission needs. In the Senate Report accompanying the National Defense Authorization Act for Fiscal Year 2021, the committee directed DOD to develop a plan by December 1, 2020 to include (1) a structure and process to enable the proper integration of JCWA components as a functional system of systems that can readily adapt to cyber mission needs; and (2) a mechanism to ensure that the JCWA component program offices are responsive to the needs of the Joint Force as represented by Cyber Command. S. Rep. No. 116-236, 116th Cong, 2d Sess. 357 (2020), (accompanying S. 4049, National Defense Authorization Act for Fiscal Year 2021).

Rapidly evolving cyber warfighting techniques coupled with a lack of goals to define interoperability has hampered JCWA efforts. The JCWA concept also lacks command-level coordination needed for a portfolio of interoperable systems. Cyber Command has begun to grapple with these challenges by taking initial steps at identifying governance roles and responsibilities within and elsewhere in DOD. Until Cyber Command establishes goals for interoperability requirements as well as addresses governance shortfalls, the JCWA portfolio of programs remains at risk of failing to provide needed joint cyber warfighting capability.

Recommendations for Executive Action

We are making two recommendations to the Department of Defense.

- The Secretary of Defense should direct the Commander, U.S. Cyber Command, to define and document Joint Cyber Warfighting Architecture goals for interoperability requirements to help synchronize acquisition efforts. (Recommendation 1)
- The Secretary of Defense should direct the Commander, U.S. Cyber Command, to further develop the Joint Cyber Warfighting Architecture governance structure by defining and documenting the roles and responsibilities of the Joint Cyber Warfighting Architecture Integration Office and Joint Cyber Warfighting Architecture Capabilities Management Office. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this product to the Department of Defense for comment. In its comments, reproduced in appendix II, DOD concurred with our first recommendation and partially concurred with the second. Specifically, DOD concurred with our first recommendation and noted that JCWA interoperability goals are required and plans to ensure that JCWA material solution integration and architecture goals are also addressed. DOD partially concurred with our second recommendation and stated that Cyber Command plans to further develop the JCWA governance structure with DOD stakeholders. These actions align with the intent of our recommendations and we will continue to monitor DOD efforts in our future work. DOD also provided technical comments that, among other things, provided updates on JCWA implementation activities and clarified JCWA program funding, which we incorporated as appropriate and where documentation was provided.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and the Commander, U.S. Cyber Command. In addition, the report will be available at no charge on GAO's website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or russellw@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

W. William Russell
Director, Contracting and National
Security Acquisitions

List of Committees

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard C. Shelby
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Peter J. Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Joint Cyber Warfighting Architecture (JCWA) Acquisition Program Information and Status

The following acquisition programs and supporting systems were part of the JCWA concept as of August 2020.

Unified Platform–data management and integration. The Air Force, as Executive Agent, initiated Unified Platform as a middle tier acquisition rapid prototyping program but realigned the program to DOD's new Software Acquisition Pathway.[1] The Air Force is managing system integration efforts for Unified Platform and using a Development, Security, and Operations (DevSecOps) approach to software development with the intent of continuously delivering capability to the user.[2] The DevSecOps approach emphasizes delivery of new system capabilities to users in iterations—every 3 months in the case of Unified Platform. According to program officials, the Air Force established the LevelUP software factory to more rapidly develop, test, and field these new capabilities for Unified Platform and other JCWA programs.[3] U.S. Cyber Command accepted six increments of Unified Platform capability between April 2019 and July 2020.

[1]The Under Secretary of Defense for Acquisition and Sustainment released the Software Acquisition Pathway in January 2020, entitled Software Acquisition Pathway Interim Policy and Procedures. In its recent guidance restructuring the defense acquisition system, DOD designed the Software Acquisition Pathway to facilitate rapid and iterative deployment of software capability. Operation of the Adaptive Acquisition Framework, DOD Instruction 5000.02, January 23, 2020. The rapid prototyping pathway is to use innovative technologies to rapidly develop fieldable prototypes to demonstrate new capabilities and meet emerging needs. The objective of a rapid prototyping program is to field a prototype in an operational environment and provide for a residual operational capability within 5 years of the development of an approved requirement.

[2]The DevSecOps concept of software development emphasizes rapid prototyping, security, and continuous integration and delivery of software products.

[3]LevelUP software factory is the Air Force's centralized team for developing cyber capability using a DevSecOps method. The Defense Science Board defines software factories as a set of software tools programmers use to write their code, confirm it meets requirements, collaborate with members of the programming team, and automatically build, test, and document their progress. This type of software production is intended to result in more rapid and continuous iteration, enabling greater flexibility as requirements change.

Table 2: Unified Platform Acquisition Status

Procuring service	Air Force
Vendor	Unified Platform relies on a variety of government and contractor personnel leveraging the Air Force's cyber software factory to develop the system.[a]
Contracting strategy	Unified Platform uses multiple contracts and multiple contract types to acquire required expertise, labor, and tools to accomplish government-lead development efforts, rather than relying on a contractor for systems development.
Next event	Program increment 7 is planned to formally conclude in October 2020.

Source: Department of Defense (DOD) officials and GAO review of DOD documentation. | GAO-21-68

[a]The Defense Science Board defines software factories as a set of software tools programmers use to write their code, confirm it meets requirements, collaborate with members of the programming team, and automatically build, test, and document their progress.

Joint Cyber Command and Control–decision making. The Air Force, as Executive Agent, initiated this program in 2017, but it has not yet formally entered the acquisition lifecycle. Program officials expect the program to follow the Software Acquisition Pathway. According to program officials, the program has sustained and delivered multiple systems while the majority of the Joint Cyber Command and Control system development efforts will begin during fiscal year 2021 when the program's available funding increases. Air Force officials stated that the program is currently leveraging existing technology development efforts, such as the DOD Strategic Capabilities Office's Project IKE—a prototype for cyber situational awareness.

Joint Cyber Command and Control is using the same DevSecOps approach to development as Unified Platform and is also relying on the LevelUP software factory. Officials stated that they are using this approach to help synchronize development between Joint Cyber Command and Control and Unified Platform.

Table 3: Joint Cyber Command and Control Acquisition Status

Procuring service	Air Force
Vendor	Joint Cyber Command and Control uses a variety of government and contractor personnel leveraging the same software factory as Unified Platform to develop the system.
Contracting strategy	Joint Cyber Command and Control uses multiple contracts and multiple contract types to acquire required expertise, labor, and tools to accomplish government-lead development efforts, rather than relying on a contractor for systems development.
Next event	According to DOD officials, the program plans to enter the software acquisition pathway in the fourth quarter of fiscal year 2020.

Source: Department of Defense (DOD) officials and GAO review of DOD documentation. | GAO-21-68

Persistent Cyber Training Environment–training, assessment, and mission rehearsal. The Army initiated this program in 2016 pursuant to a prior iteration of *DOD Instruction 5000.02*. The program achieved Milestone B to enter system development in December 2019. The program is using an Agile approach to software development that releases incremental software upgrades based on user feedback from across the services. Additionally, different contractor or government teams can develop individual training modules and content that they share with other system users.

Table 4: Persistent Cyber Training Environment Acquisition Status

Procuring service	Army
Vendor	Persistent Cyber Training Environment uses multiple vendors while the government acts as the system integrator to coordinate the integration of different vendor capabilities.
Contracting strategy	Persistent Cyber Training Environment uses diverse contract vehicles to acquire required expertise and tools. For example, the program has used Other Transactions and other contracts, but will add an indefinite delivery/indefinite quantity contract with its Cyber TRIDENT contract award.
Next event	Cyber TRIDENT contract award planned for the second quarter of fiscal year 2021.

Source: Department of Defense (DOD) officials and GAO review of DOD documentation. | GAO-21-68

Joint Common Access Platform–mission enablement. The Army is the lead for this program, which DOD formally initiated in May 2020. DOD officials stated that, when the system enters the acquisition lifecycle they expect to follow the major capabilities pathway, but are also considering the Software Acquisition Pathway. The program is likely to leverage and enhance existing programs, with the intent of incorporating “best of breed” components.

Cyber Tools and Sensors–operations and situational awareness. Cyber Tools and Sensors is a category describing multiple acquisition efforts ranging from technology development efforts to application of existing technologies. The services and Cyber Command are responsible for procuring tools and sensors to meet their mission needs.

Appendix II: Comments from the Department of Defense

THE ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

ACQUISITION

Mr. William Russell
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Russell,

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-21-68, "DEFENSE ACQUISITIONS: JOINT CYBER WARFIGHTING ARCHITECTURE WOULD BENEFIT FROM DEFINED GOALS AND GOVERNANCE," dated 18 September 2020 (GAO Code 103881).

Attached is the DoD's response to the subject report. My point of contact is Ms. Katherine Arrington, (703) 695-9332, katherine.e.arrington.civ@mail.mil.

FAHEY.KEVIN.M.1228589795
Digitally signed by FAHEY.KEVIN.M.1228589795
Date: 2020.11.05 17:17:30 -05'00'

Kevin Fahey

GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT DATED SEPTEMBER 18, 2020
GAO-21-68 (GAO CODE 103881)

"DEFENSE ACQUISITION: JOINT CYBER WARFIGHTING ARCHITECTURE (JCWA) WOULD BENEFIT FROM DEFINED GOALS AND GOVERNANCE"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends the Secretary of Defense should direct the Commander, United States Cyber Command, to define and document JCWA goals for interoperability requirements to help synchronize acquisition efforts.

DoD RESPONSE: DoD concurs with Recommendation 1. DoD agrees that JCWA interoperability goals are required; however, to ensure success we need to also address JCWA material solution integration and architecture goals. Per U.S.C. Section 167b, USCYBERCOM is the requirements owner for cyber operations activities and is responsible for ensuring the interoperability of cyber operations equipment and forces (includes JCWA).

Commander, United States Cyber Command, will use the Cyber Capabilities Integration and Development System (CCIDS) process, as needed, to develop and validate JCWA requirements. USCYBERCOM has drafted a JCWA Concept of Operations (CONOPS), which will inform stakeholders on how JWCA must be employed operationally and execute information / knowledge / data exchanges across components, program managers, and operators as needed to support operations.

RECOMMENDATION 2: The GAO recommends the Secretary of Defense direct the Commander, United States Cyber Command, to further develop the JCWA governance structure by defining and documenting the roles and responsibilities of the JCWA Integration Office and the JCWA Capabilities Management Office.

DoD RESPONSE: DoD partially concurs with Recommendation 2. Commander, United States Cyber Command, to further develop the JCWA governance structure by defining and documenting the roles and responsibilities of the JCWA Integration Office and the JCWA Capabilities Management Office with Department stakeholders.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

W. William Russell at (202) 512-4841 or russellw@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Raj Chitikila, Assistant Director; Brandon Booth; Virginia Chanley; Burns C. Eckert (Analyst-in-Charge); Brian Fersch; Lori Fields; Laura Greifner; Jordan Kudrna; Christine Pecora; and Jessica Waselkow made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548