United States Government Accountability Office

Report to Congressional Committees

March 2022

DEFENSE ACQUISITIONS

Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities

Accessible Version

GAO-22-104695

GAO Highlights

Highlights of GAO-22-104695, a report to congressional committees

March 2022

DEFENSE ACQUISITIONS

Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities

Why GAO Did This Study

The U.S. faces increasingly sophisticated cyber threats, such as the 2019 SolarWinds security breach. To mitigate these threats, DOD is continually developing new software-based capabilities. Cyber Command created the JCWA in 2019 to address these needs and synchronize cyber warfighting programs across DOD. The JCWA includes a range of software-enabled systems, sensors, and tools that the Army and Air Force are procuring for Cyber Command.

In November 2020, GAO reported shortfalls in the JCWA governance structure and interoperability goals and recommended that Cyber Command define roles and responsibilities for overseeing the JCWA programs and develop such goals.

A Senate report included a provision for GAO to review the status of the JCWA. This is GAO's second report. This report examines Cyber Command's progress in defining JCWA roles, responsibilities, and interoperability goals; and efforts to assess the JCWA acquisitions using outcome-based metrics. To conduct this work, GAO obtained and reviewed relevant documents and met with DOD officials.

What GAO Recommends

GAO is recommending that Cyber Command develop outcome-based metrics to inform future Value Assessments. DOD concurred with the recommendation and identified steps it is taking to develop metrics for future Value Assessments.

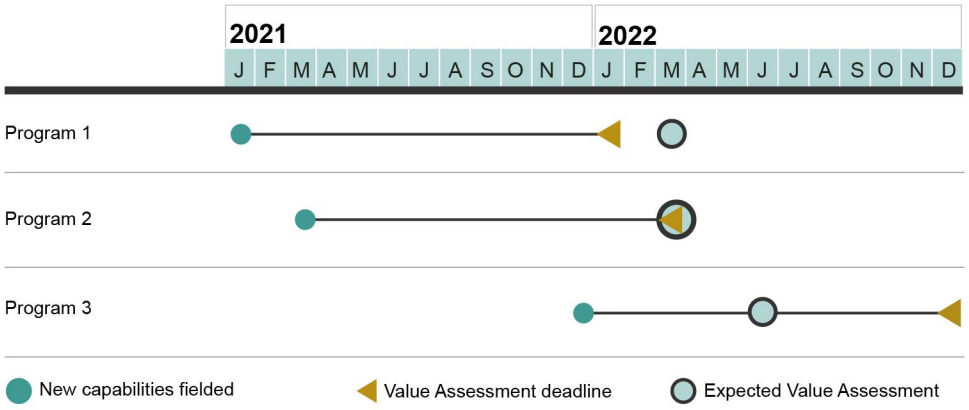
View GAO-22-104695. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov.

What GAO Found

In response to previous GAO recommendations, Cyber Command—the Department of Defense (DOD) command responsible for cyberspace operations—is maturing its Joint Cyber Warfighting Architecture (JCWA) to integrate systems that enable the cyber warfighting mission. In December 2020, the command identified JCWA roles and responsibilities, and, in September 2021, it approved a JCWA Concept of Operations to define interoperability goals and intended outcomes of the programs.

Cyber Command has initiated efforts to assess JCWA acquisitions. DOD policy requires outcome-based evaluations, called Value Assessments, for programs within 1 year of fielding capabilities to determine whether they result in mission outcomes that are worth the investment. DOD clarified its Value Assessment guidance after GAO raised Cyber Command's confusion regarding its role in scheduling these assessments. The command subsequently initiated the JCWA program Value Assessments, once it understood it was responsible for doing so, and these assessments were underway as of March 2022 (see figure).

Joint Cyber Warfighting Architecture Acquisition Program Value Assessment Timelines



Source: GAO review of program documents and interviews with program officials. | GAO-22-104695

Cyber Command has not yet developed required outcome-based metrics to support the Value Assessments. DOD policy and guidance call for such metrics to help programs understand mission improvements. For example, measuring improvements in the speed of operations could help Cyber Command determine whether programs are delivering intended outcomes. The command has been slow to determine metrics, in part because of inexperience conducting Value Assessments and the challenge of accounting for other factors—like new cyber operations tactics—on mission outcomes. Though this process is new, DOD guidance encourages experimentation and learning, so that metrics can continue to be refined over time. While the command is unlikely to have outcome-based metrics for the first three assessments that are underway, there is sufficient time for it to do so for those it has not yet initiated. If Cyber Command does not develop outcome-based metrics to inform future Value Assessments, it risks not being able to understand whether and how new capabilities benefit the cyber warfighting mission.

Contents

Abbreviations

DevSecOps	Development, Security, and Operations
DOD	Department of Defense
JCWA	Joint Cyber Warfighting Architecture
OUSD(A&S)	Office of the Under Secretary of Defense for Acquisition and Sustainment

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

March 30, 2022

Congressional Committees

The increasing sophistication of cyber threats requires that Department of Defense (DOD) cyberspace capabilities continue to evolve to support all forms of combat operations, as well as defend critical U.S. infrastructure from foreign actors. DOD's efforts, with other federal agencies, to respond to cyber events, like the 2019 SolarWinds security breach, reinforce the gravity of these threats. According to Cyber Command—DOD's combatant command responsible for cyber operations—DOD must provide the necessary cyber warfighting capabilities to defeat its adversaries. To unify these capabilities, Cyber Command created the Joint Cyber Warfighting Architecture (JCWA) in 2019. The architecture is to synchronize DOD's multiple programs and functions, such as cyber operations training or battle management, across the military departments to more effectively support cyberspace operations and amplify military combat power. According to the Commander of Cyber Command, the JCWA is not to be a fixed future state, but a set of evolving capabilities that address technological change, operational outcomes, and shifting threats.

In November 2020, we issued our first report on the JCWA, which reviewed the relevant acquisition programs and DOD's governance of the JCWA.[1] We found shortfalls in the JCWA governance structure and recommended that Cyber Command define roles and responsibilities for overseeing the JCWA programs. We also found Cyber Command had not defined interoperability goals to help integrate JCWA program functions and recommended that the command develop such goals. Cyber Command officials partially agreed with our recommendations.

Senate Report 116-48 accompanying the National Defense Authorization Act for Fiscal Year 2020 included a provision for us to review the status of the JCWA. This second report describes (1) actions Cyber Command has taken to define JCWA roles and responsibilities as well as interoperability

[1]GAO, *Defense Acquisitions: Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance,* GAO-21-68 (Washington, D.C.: Nov. 19, 2020).

goals, and (2) the extent of Cyber Command's efforts to assess the value of JCWA acquisitions.

To identify actions Cyber Command took to define roles and responsibilities, we obtained and reviewed relevant documents, as well as the JCWA Concept of Operations, which command officials planned to use to address interoperability goals for the JCWA systems. To assess Cyber Command's efforts to coordinate and assess the value of JCWA acquisitions using the Software Acquisition Pathway, we used DOD policy, and Cyber Command and program documents to identify the command's responsibilities and plans to conduct Value Assessments. We conducted meetings with officials from relevant organizations, including Cyber Command and the four JCWA program offices, to clarify details and confirm the information we reviewed. For more information about our scope and methodology, see appendix I.

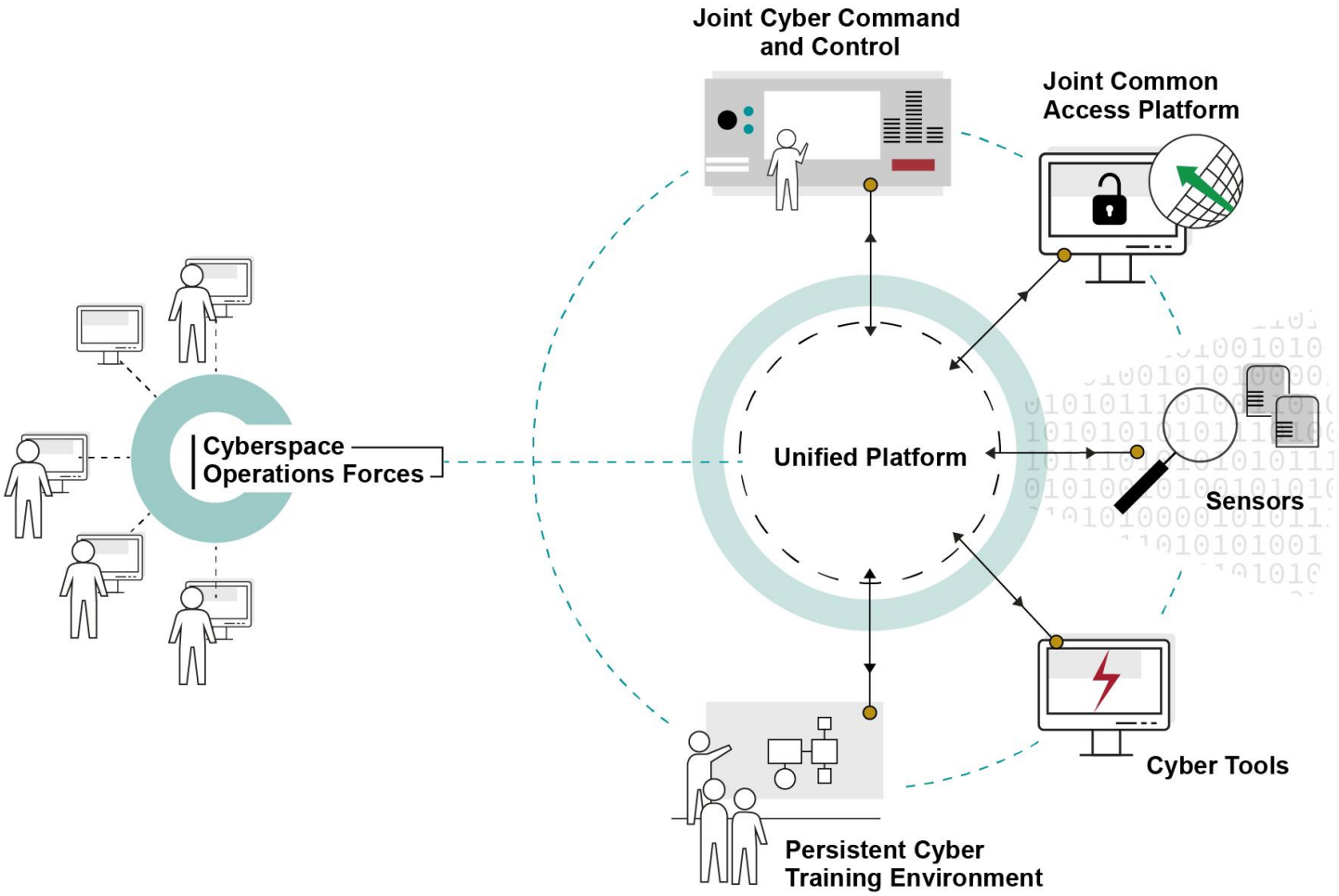
We conducted this performance audit from December 2020 to March 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions 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.

Background

Joint Cyber Warfighting Architecture Programs and Relevant Organizations

DOD created the JCWA to harmonize cyber capabilities across the military departments to meet the needs of Cyberspace Operations Forces—DOD's cyber warfighters and supporting personnel. Cyber Command officials told us the defining goal of the JCWA is to develop interoperability among systems to provide a comprehensive, integrated cyberspace architecture. Figure 1 shows the initial construct of the JCWA with its six components and cyber forces accessing the architecture.

Figure 1: Joint Cyber Warfighting Architecture Diagram



Source: GAO representation of Department of Defense documentation. | GAO-22-104695

The JCWA components comprise computer-based capabilities that support defensive, offensive, and DOD network operations—the full spectrum of cyberspace operations.[2] Of these six components, four entail acquisition programs that are currently underway:

Persistent Cyber Training Environment. The Army initiated this program in 2016 to provide a platform for training, assessment, and mission rehearsal. The purpose is to create an environment for cyber warfighters to configure networks, devices, software, and

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

tools to evaluate and practice cyber operations. The Persistent Cyber Training Environment is in widespread use for major cyber training exercises, such as Cyber Flag training events that include hundreds of users across DOD and allied partners, as well as cyber unit-specific training.

Unified Platform. The Air Force initiated this program in 2018 to function as a data synchronization, storage, and access system for cyber warfighters and supporting personnel. For example, it enables users to access cyber data across multiple military department systems at various classification levels.

Joint Cyber Command and Control. The Air Force initiated this program in 2017 to provide integrated situational awareness. This includes tracking the flow of cyber actors and information on networks, as well as battle management functions to support commanders' warfighting decisions. The program is expanding upon existing DOD systems.

Joint Common Access Platform. The Army initiated this program in 2020 to provide a common access platform for cyber warfighters to project combat power using a comprehensive suite of tools.

See appendix II for additional details on the four JCWA programs.

The JCWA also includes Cyber Tools and Sensors, which are not a single acquisition program or family of programs, but multiple ongoing and planned efforts led by each military department and Cyber Command. These efforts acquire and deploy cyber tools to defend friendly networks as well as attack enemy systems. Sensors help deliver intelligence, surveillance, and reconnaissance data to inform cyber operations.

Cyber Command's budget control responsibilities for cyber warfighting capabilities are evolving and expanding. The National Defense Authorization Act for Fiscal Year 2022 directed that Cyber Command's budget control responsibilities be expanded in fiscal year 2024 to enable the command to control Cyber Mission Force resources, subject to the

authority, direction, and control of the DOD Principal Cyber Advisor.[3] This new budgeting responsibility will enable Cyber Command to use DOD's Planning, Programming, Budgeting, and Execution Process rather than rely on the military departments for budgeting and planning the JCWA programs. The act also directed DOD to submit an implementation plan for how the command will use its expanded budgeting responsibility to Congress in January 2022.[4] That plan is to include workforce estimates to enact these new authorities and time frames for when that workforce will be in place.[5]

DOD Software Acquisition Pathway and the JCWA

In October 2020, DOD released DOD Instruction 5000.87 – *Operation of the Software Acquisition Pathway*. This pathway is for the timely acquisition of custom software capabilities developed for DOD, such as those associated with the JCWA.[6] All of the major JCWA programs are using the Software Acquisition Pathway, except for the Persistent Cyber Training Environment, and officials from that program stated they are considering a move to this pathway in the future. The Software Acquisition Pathway emphasizes frequent, ongoing collaboration between the program office, software developers, and the software user community. To ensure collaboration among these communities, the Software Acquisition Pathway integrates modern software development practices—such as Agile—that rely on continuous feedback between these communities as well as regular assessments of new capabilities.

The Software Acquisition Pathway feedback relationship for a single acquisition program is straightforward, but for the integrated JCWA programs it is more complicated. For a single program, there is a single feedback loop: the program office, which is part of the acquisition community, works with users and developers to continuously assess new capabilities and provide feedback. For the JCWA, these feedback

[3]National Defense Authorization Act for Fiscal Year 2022. Pub. L. No. 117-81, § 1507 (a)(2)(A)-(B) (2021). The Principal Cyber Advisor is the Office of the Under Secretary of Defense for Policy staff advisor to the Secretary of Defense on military and civilian cyber forces and activities.

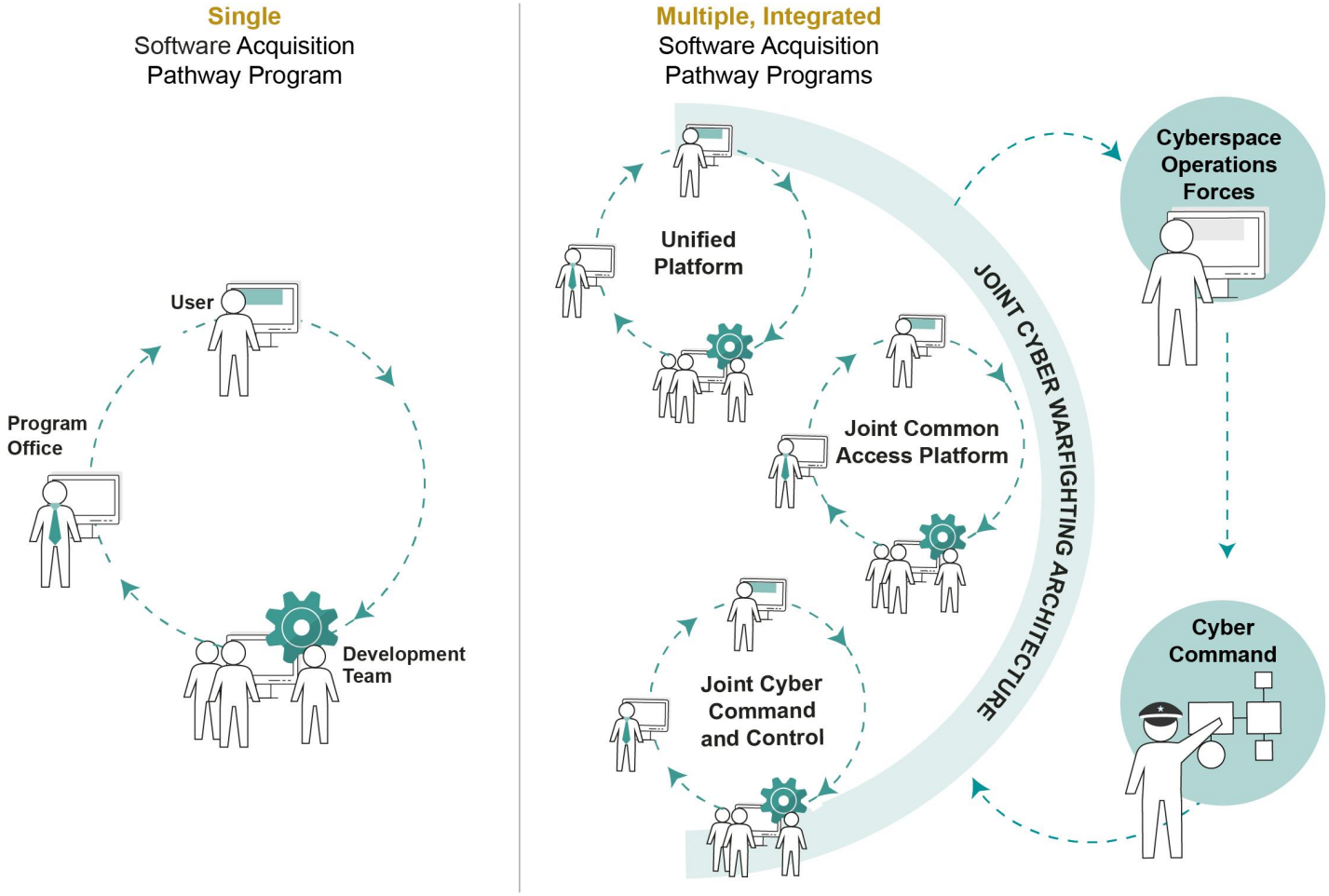
[4]Pub. L. No. 117-81, § 1507 (c)(1).

[5]Pub. L. No. 117-81, § 1507 (c)(2)(A)-(B).

[6]Department of Defense, *DOD Instruction 5000.87*, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020). DOD also publishes and updates guidance for implementing the Software Acquisition Pathway at https://aaf.dau.edu/aaf/software/.

relationships are more complex because Cyber Command is responsible for identifying the programs' requirements but does not yet execute the programs itself, due to its evolving authority, and must rely on the military departments. Therefore, each JCWA program would have an internal feedback relationship between the acquisition and user communities, focused on specific, day-to-day development of new capabilities. Each program would also be part of a broader feedback relationship with Cyber Command, users in the Cyberspace Operations Forces, and other JCWA programs focused on the results of these new capabilities. Figure 2 describes these two levels of feedback relationships.

Figure 2: Software Acquisition Pathway and Joint Cyber Warfighting Architecture Feedback Relationships



Source: GAO review of Department of Defense documentation. | GAO-22-104695

The Software Acquisition Pathway defines several key roles in the acquisition process that the military departments, Cyber Command, and JCWA program offices fill. As a combatant command, Cyber Command has numbered staff offices or directorates, such as the J3 (Operations Directorate) that has both JCWA roles and additional responsibilities unrelated to the JCWA. Table 1 defines the Software Acquisition Pathway roles and the relevant Cyber Command directorate or military organization filling the role for the JCWA.

Table 1: Selected Software Acquisition Pathway Roles and Responsibilities for Joint Cyber Warfighting Architecture (JCWA) Organizations

Software Acquisition Pathway role	Responsibilities	Relevant organization for the JCWA
Decision authority	The official responsible for oversight and key decisions of programs that use the pathway. The official designates a program manager and supports this person in tailoring and streamlining processes, reviews, and decisions to enable speed of capability delivery. The official may be the Defense Acquisition Executive, Component Acquisition Executive, Program Executive Officer, or other official designated by the Component Acquisition Executive.	Joint Common Access Platform – Program Executive Officer Intelligence, Electronic Warfare, and Sensors Unified Platform and Joint Cyber Command and Control – Secretary of the Air Force
End user/user community	Those who will ultimately use the software solution. Users convey operational concepts, requirements, and needs; participate in continuous testing activities; and provide feedback on developed capabilities.	For requirements, the Cyber Command Operations Directorate (J3), and the Capability and Resource Integration Directorate (J8). For continuous testing activities and feedback, both Cyber Command and the Service Cyber Components, such as the Air Force's 16th Air Force, provide end users.
Sponsor	The individual or organization that identifies and advocates for needed end user capabilities and associated resource commitments. The sponsor is responsible for identifying the needed capabilities to justify initiating a software acquisition.	Cyber Command Capability and Resource Integration Directorate (J8).

Source: Department of Defense Instruction 5000.87 and JCWA program documents. | GAO-22-104695

The Software Acquisition Pathway also requires key documents, including:

Capability Needs Statement. A high-level description of mission deficiencies that the development effort is to address and other attributes that provide information to define software solutions as they relate to the overall threat environment. The program office and end users or user community are responsible for drafting this statement, which the sponsor—Cyber Command for the JCWA programs—approves. Programs should review the statement at least annually to determine if updates are warranted.

Product Roadmap. A high-level visual summary that maps out the vision and direction of software solutions over time. It describes the goals and features of each software delivery. The program office and sponsor develop and maintain the roadmap.

User Agreement. A commitment between the sponsor and program manager for continuous user involvement and assigned decision-making authority in the development and delivery of software capability releases. The program office is responsible for developing this document in coordination with the sponsor; the program and sponsor co-sign the agreement.

Value Assessment. An outcome-based assessment of mission improvements and efficiencies realized from the delivered software capabilities, and a determination of whether the outcomes have been worth the investment. The sponsor, program office, and user community are to perform Value Assessments at least annually to inform program decisions. The Value Assessment is the formal, recurring feedback mechanism for each JCWA program acquired through the Software Acquisition Pathway. The sponsor and program office should negotiate the timing and frequency of the Value Assessment and document that schedule in the User Agreement.

These elements of the Software Acquisition Pathway, especially the emphasis on frequent, collaborative software delivery and feedback relationships are, according to DOD policy and guidance, grounded in Agile and other modern practices for software development. According to Software Acquisition Pathway guidance, implementing these practices helps DOD use technological innovation to sustain the U.S. military advantage. In September 2020, we issued our *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*.[7] We said that transitioning to Agile software development methods, as the JCWA programs report doing, requires that practitioners do more than implement new or modify existing tools, practices, and processes. Shifting to Agile methods requires organizations to embrace rapid, iterative development in place of a sequential approach to defining requirements, developing a solution, and then testing. The guide describes our leading practices for adopting Agile principles, including elements that address

[7]GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590G (Washington, D.C.: Sept. 28, 2020).

organizational environment, program operations, and engaging users early to limit the risk of investing in a failing program or outdated technology.

Cyber Command Is Making Progress Maturing JCWA Governance and Interoperability Goals

Cyber Command Defined JCWA Roles and Responsibilities and Is Assessing Workforce Shortfalls

Cyber Command identified initial JCWA roles and responsibilities in December 2020, in response to our prior recommendation, and plans to continue to refine these definitions as it matures the JCWA.[8] Cyber Command established new offices and roles to manage and coordinate the JCWA with the military departments, separate from the Software Acquisition Pathway roles we identified above. The Cyber Command document that outlines these roles and responsibilities focuses on offices within the command that support the JCWA, as described in table 2.

[8]GAO-21-68.

Table 2: Cyber Command Roles and Responsibilities for Joint Cyber Warfighting Architecture (JCWA) Programs

Office or organization	GAO summary of responsibilities
JCWA Capabilities Management Office	• Develops the JCWA concept to synchronize actions across multiple cyberspace-based platforms; develops JCWA strategic roadmap • Establishes Cyber Command guidance and operational concepts, including mitigation plans for any gaps in existing policy • Works with warfighters and partner organizations to identify operational gaps and risks across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy to inform and develop requirements
JCWA Integration Office	• Coordinates integration activities across the four JCWA programs to enable an integrated solution for Cyber Command by developing and maintaining the JCWA integrated master schedule as well as assessing cost, schedule, and performance of the JCWA programs • Coordinates with and among JCWA and other acquisition program offices to develop capabilities aligned with Cyber Command priorities • Coordinates training, delivery, and updates to JCWA components with the JCWA Capabilities Management Office

Capability and Resource Integration Directorate (J8)	• Serves as Cyber Command's lead office for managing requirements, resources, and assessments to facilitate capabilities integration through existing enterprise processes and systems, including
	  • Requirements: Manages requirements development, validation, and prioritization
	  • Resources: Plans, programs, budgets, executes, and prioritizes resources for Cyber Mission Force activities, to include the JCWA, in coordination with the military departments and Service Cyber Components
	  • Assessments: Directs and manages cyber capability-based assessments to inform cyber requirements and conducts Software Acquisition Pathway Value Assessments

Command Acquisition Executive	• Supervises the acquisition of cyber capabilities to address urgent warfighter needs • Interacts with JCWA acquisition Program Executive Officers or lead program developers on specific acquisition strategies, processes, and milestone decision reviews • Serves as Cyber Command's representative in acquisition meetings and negotiates Memoranda of Agreement with the military departments to advance JCWA materiel development

Source: GAO representation of Cyber Command documents. | GAO-22-104695

Cyber Command plans to continue revising internal JCWA roles and responsibilities and expand these duties to external stakeholders, according to officials. In our November 2020 report on the JCWA, we recommended that Cyber Command define and document the roles and responsibilities of the JCWA Capabilities Management Office and JCWA Integration Office to help develop the architecture's governance structure.[9] The command's actions to date address the intent of our recommendation by documenting roles and responsibilities within Cyber Command. Officials from Cyber Command said they are now in the

[9]GAO-21-68.

process of defining the roles and responsibilities for JCWA stakeholders outside the command, such as the DOD Principal Cyber Advisor and others.[10] As of December 2021, Cyber Command officials anticipate completing a first revision of the roles and responsibilities document by April 2022.

Cyber Command is also assessing its workforce needs as part of its efforts to mature JCWA governance. According to command officials, after identifying initial internal roles and responsibilities, they realized that the offices involved in executing the JCWA and other command responsibilities do not have sufficient personnel. For example, Cyber Command officials stated the JCWA Integration Office has seven staff, but officials estimate that it needs approximately 55 personnel. It will take time to fill additional positions, in part, because Cyber Command officials said they must first justify and validate the command has a need before beginning to bolster the workforce in fiscal year 2025. Cyber Command has a workforce study underway that officials anticipate will be complete later in fiscal year 2022.

According to Cyber Command officials, understaffing is creating an all-hands-on-deck atmosphere, with individuals attempting to address emergent issues regardless of their office's role, rather than a more coordinated approach. JCWA program officials said this atmosphere creates confusion because they are in contact with multiple Cyber Command officials, but unsure which official has the authority to advise or make decisions for their programs. Cyber Command officials stated they are working on this issue in coordination with their revisions of the JCWA roles and responsibilities and workforce study.

[10]Cyber Command is responsible for cyber operations, but also works with other DOD organizations that support the cyber mission: the Principal Cyber Advisor (advises the Secretary of Defense on military and civilian cyber forces); the Chief Information Officer (responsible for information technology, including national security systems); the Office of the Under Secretary of Defense for Acquisition and Sustainment (responsible for acquisition policy); the Director, Operational Test and Evaluation (oversees the military departments' operational test agencies and issues operational test policy); as well as other organizations.

Cyber Command Defined Initial JCWA Interoperability Goals and Expects to Regularly Update These Goals

In September 2021, Cyber Command approved its first JCWA Concept of Operations, in part, to define interoperability goals between the JCWA programs to ensure they interoperate as planned. This action addresses our recommendation from November 2020.[11] We recommended that Cyber Command define interoperability goals, which would help the command describe the overall system objectives, relationships, and dependencies of the JCWA programs. The Concept of Operations is the core reference document for leaders to understand how the JCWA can support operational planning and decision-making. It uses a set of attributes—or key characteristics the systems must enable—to describe the capabilities the JCWA programs are developing. The document explains that these attributes are interdependent characteristics that set goals for interoperability. For example, training data from the Persistent Cyber Training Environment needs to be accessible to other JCWA systems. To share data with other programs, Persistent Cyber Training Environment developers must either use the same data formats as the other programs or work with those programs' developers to translate training data.

The JCWA Concept of Operations also provides high-level summaries and operational scenarios that incorporate interoperability goals and operational outcomes associated with the programs. Officials from two of the JCWA programs who reviewed the Concept of Operations told us that these scenarios help them better understand the role and intended operation of the systems they are developing within the overall JCWA construct. For example, one scenario describes cyberspace operators using a JCWA program collaboration tool to share information with other federal agencies and conducting research through another JCWA program to head off a threat to a U.S. facility. Such details of information sharing and research needs inform the JCWA programs about which other agencies may need access to data or which databases will support research.

Cyber Command officials stated they intend for the Concept of Operations to be a living document that they will update at regular intervals as cyber operations evolve. The document contains projections for a 5-10 year future, identifying technologies Cyber Command officials

[11]GAO-21-68.

expect to play a greater role in the architecture, such as artificial intelligence. Officials anticipate the document will also guide changes to cyber policy, doctrine, and training within Cyber Command and DOD, as JCWA users develop new tactics for cyber operations.

Cyber Command Scheduled JCWA Program Value Assessments but Has Not Defined Outcome-Based Assessment Metrics

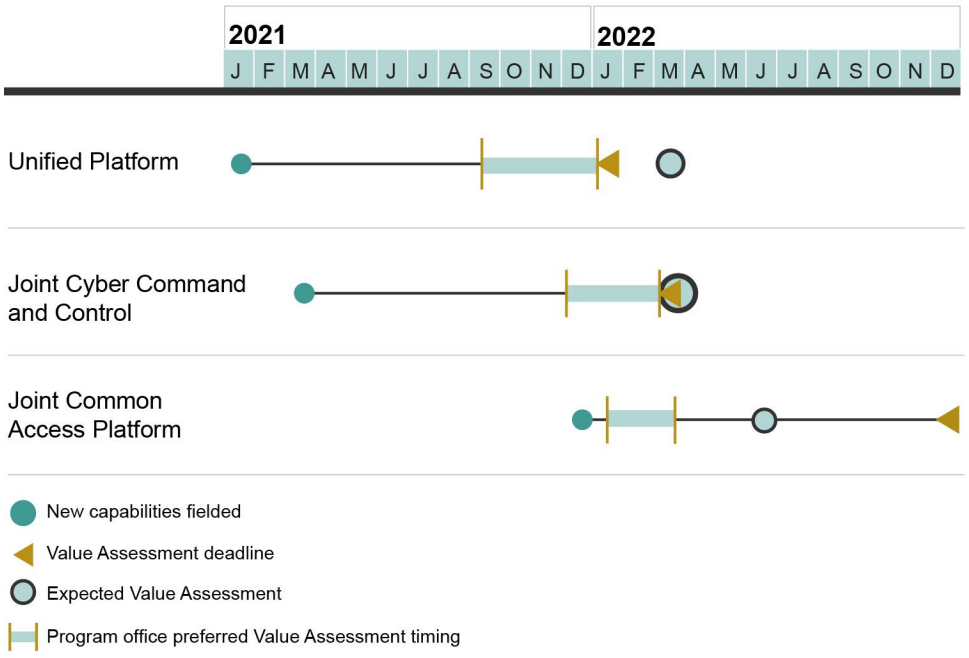
Cyber Command Scheduled Value Assessments with JCWA Programs after Clarifying Its Role in Conducting These Assessments

The Value Assessment is a formal, recurring assessment of an acquisition program's effect on mission outcomes and whether those outcomes are worth the investment. DOD Instruction 5000.87 requires that a program initial warfighting capabilities to enhance mission outcomes within 1 year after the date on which funds are first obligated to acquire or develop a new software capability. After the capabilities are delivered, the program sponsor must conduct a Value Assessment within 1 year, but has the flexibility to conduct them sooner and more frequently. As noted above, as the sponsor for JCWA programs, Cyber Command is responsible for conducting these assessments.

Cyber Command started to schedule these assessments beginning in September 2021 during the course of our review, and after we raised concerns that they had not been scheduled in a timely manner. However, the command will not complete all of them by the required dates. As of March 2022, Cyber Command reported initiating Value Assessments for the three JCWA programs that use the Software Acquisition Pathway. The Joint Cyber Command and Control and Joint Common Access Platform Value Assessments were scheduled to be completed on or ahead of their respective due dates. Cyber Command officials noted that Unified Platform's assessment would be finished by March 2022, which is two months late, based on when the program first fielded capabilities under the Software Acquisition Pathway. According to Unified Platform officials, Cyber Command did not schedule the assessment early enough to complete it by the required date. The Value Assessments for Unified Platform and Joint Cyber Command and Control were still underway during the time of our review. Figure 3 shows the acquisition timelines of

the three JCWA programs on the Software Acquisition Pathway, including their Value Assessment deadlines and anticipated completion dates.

Figure 3: Joint Cyber Warfighting Architecture Acquisition Program Timelines for Value Assessments



Source: GAO review of program documents and interviews with program officials. | GAO-22-104695

Cyber Command officials we met with stated they did not schedule Value Assessments earlier because they misunderstood their role in leading them and did not document schedules in User Agreements. In our discussions, Cyber Command officials told us they thought the programs, not Cyber Command, were responsible for requesting the Value Assessments and were unsure of the deadlines for each program's assessment. Cyber Command officials noted their staff began preparing for assessments in July 2021 but did not ultimately schedule Value Assessments until September 2021. Cyber Command officials further explained that the Software Acquisition Pathway is still new to DOD and the JCWA programs are some of the first to use it, which contributed to their misunderstanding about their role in leading these assessments. While the Software Acquisition Pathway is new, we found that the pathway instruction did identify that the sponsor, in this case Cyber Command, is responsible for conducting Value Assessments. Furthermore, the accompanying guidance clarifies that the sponsor is responsible for negotiating the time frames for conducting these

assessments with program stakeholders. The guidance also states that these time frames should be documented in the User Agreement, but none of these agreements currently identify Value Assessment schedules. Cyber Command officials said they would work with the JCWA programs to include Value Assessment timelines in future User Agreements.

We discussed Cyber Command's uncertainty with officials from the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))—the authors of DOD Instruction 5000.87 and the accompanying guidance—in September 2021. As a result of that conversation, OUSD(A&S) revised the guidance in October 2021 to make the sponsor's role more clear. For example, we observed that, while the prior guidance stated that sponsors and programs should negotiate and document Value Assessment timing within the User Agreement, the passage noting this requirement was not highlighted and was only mentioned briefly near the end of the guidance. The October 2021 revised guidance more clearly highlights these elements. OUSD(A&S) officials explained that they would continue to refine the guidance to improve operation of the Software Acquisition Pathway based on lessons learned and stakeholder input. They also conducted outreach sessions to educate DOD personnel using the pathway, such as the session they provided for Cyber Command in October 2021.

JCWA program officials stated that Cyber Command is now engaging with them to align future Value Assessments to key program events and better inform program decisions. For example, officials from Unified Platform said they wanted Cyber Command to complete that program's Value Assessments in the fall time frame to inform funding requests and priorities for the next budget cycle. Joint Cyber Command and Control program officials stated their preference is for future Value Assessments to occur before their annual review of the Capability Needs Statement. According to officials, this timing would help the program better align upcoming work with feedback from the Value Assessment. Joint Common Access Platform program officials stated their preference for that program's Value Assessment to occur a few months after the program's initial capability delivery in December 2021 because that delivery comprises a foundational set of capabilities for the program. Cyber Command officials stated that, while current Value Assessments are underway, they would work with the programs to ensure the timing of future assessments meets command and program needs.

Now that Cyber Command is working with the JCWA programs to schedule and conduct Value Assessments, it is better positioned to provide timely, regular feedback on programs' contributions to the cyber warfighting mission, per DOD guidance. The programs can anticipate information from Cyber Command on whether their current efforts are meeting warfighter needs and warrant ongoing investment. Further, as Cyber Command conducts more of these assessments, it will have additional opportunities to coordinate timing that benefits the command and JCWA programs.

Cyber Command Has Not Developed Metrics to Support Value Assessments

As of December 2021, Cyber Command had not developed outcome-based metrics to assess whether JCWA programs are achieving intended operational outcomes, such as those defined in its Concept of Operations. While the programs have metrics they use to assess their own software development processes and performance, Cyber Command officials stated they have yet to develop broader outcome-based metrics that would describe whether the JCWA programs are achieving the intended operational outcomes for cyber operations. For example, the Joint Common Access Platform program office tracks software failure rates to identify the root cause of the failures and identify software fixes. This metric, while useful to program managers, does not align with overarching JCWA operational outcomes such as those defined in the Concept of Operations, which describe broader results like improved infrastructure security.

DOD Instruction 5000.87 states that Value Assessments are to be outcome-based. In our March 2021 report on key terms in program evaluation, we defined outcomes as the desired results of a program; therefore, outcome-based metrics would measure those desired results.[12] Supporting guidance for the Software Acquisition Pathway also describes the importance of outcome-based metrics for programs to understand the mission improvements or efficiencies that newly developed capabilities provide and directs that programs use those results as the basis for the Value Assessment.

[12]GAO, *Program Evaluation: Key Terms and Concepts*, GAO-21-404SP (Washington, D.C.: March 2021).

In the case of the JCWA, the integration of multiple programs means that Cyber Command needs these metrics to identify and assess operational outcomes to understand how the programs are working together. For example, if Cyber Command wants to conduct certain kinds of cyber operations faster, measuring changes in operational efficiency resulting from the JCWA programs would be an outcome-based metric. DOD's Software Acquisition Pathway guidance provides examples of metrics that DOD organizations may use but also states that those organizations should develop outcome-based metrics from their own experimentation and learning. According to OUSD(A&S) officials, identifying outcome-based metrics for Value Assessments is an ongoing process because such metrics will likely be unique to each program and capability. Our Agile Guide echoes this statement in that such metrics should be tailored to a program's needs and should evolve over time.[13]

Cyber Command officials stated that in the spring of 2021, the command established a team to develop metrics, but these officials could not provide a time frame for identifying outcome-based metrics. Command officials stated that they are working on these metrics but cited multiple reasons for slow progress, including:

- their inexperience with the Software Acquisition Pathway and not having relevant examples of such metrics in completed Value Assessments;
- the cyber mission continually changing; and
- the challenge of measuring external factors such as new tactics or training on mission outcomes.

Cyber command has more opportunity to develop outcome-based metrics now that it has an approved Concept of Operations that defines the JCWA's operational outcomes. According to OUSD(A&S) officials, developing outcome-based metrics should not paralyze programs and sponsors. While Cyber Command is unlikely to have outcome-based metrics in place before it completes its first Value Assessments that are already underway, the command will have more time to develop metrics before the JCWA programs' next set of assessments are due. OUSD(A&S) officials told us that, as more programs conduct Value Assessments, they expect metrics will evolve as needed to track progress toward long-term goals. If Cyber Command does not develop outcome-based metrics to inform the second round of Value Assessments, it will be

[13]GAO-20-590G.

at greater risk of not understanding whether and how new capabilities benefit the cyber warfighting mission.

Conclusions

Cyber Command's recent actions to better understand its role and to schedule Value Assessments with the JCWA programs are positive first steps to continue developing DOD's cyber operations capacity. It will be important for Cyber Command to continue engaging with the programs on when to schedule this feedback in the future. The JCWA programs depend on timely and regular feedback to understand whether new capabilities benefit cyber warfighters, or whether resources would be better used for other efforts. Cyber Command's feedback will be hindered, however, until it develops outcome-based metrics to inform the Value Assessment. Developing such metrics for software-intensive programs is a recognized challenge within DOD, but this challenge should not stop Cyber Command from putting metrics in place for upcoming Value Assessments. The inherent flexibility of the Software Acquisition Pathway encourages experimentation and learning; if the first set of metrics is not effective, try again. While Cyber Command is unlikely to have outcome-based metrics to inform its initial Value Assessments, the command should have sufficient time to develop metrics for future assessments. Cyber Command can use the first Value Assessments as an opportunity to gain experience with this new process while also providing valuable feedback to the programs. However, until Cyber Command defines outcome-based metrics to inform future assessments, it risks investing in capabilities that do not fully meet the command's needs for cyber warfighting.

Recommendation for Executive Action

The Secretary of Defense should direct the Commander, Cyber Command, to develop outcome-based metrics for the JCWA programs that are on the Software Acquisition Pathway to support future Value Assessments. (Recommendation 1)

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 III, DOD concurred

with our recommendation to develop outcome-based metrics to support future Value Assessments for JCWA programs. DOD reported that it requested additional resources from within DOD to assist this effort and described actions the command is taking to support Value Assessments. DOD also requested a revision to our recommendation to make clear it has initiated Value Assessments. Our intent is to ensure Cyber Command uses outcome-based metrics for future Value Assessments, not those currently underway, to provide the command with the time officials stated they need to develop those metrics. As such, we clarified the wording of the recommendation to emphasize future assessments. DOD also provided technical comments that we incorporated as appropriate. For example, DOD provided updates on the JCWA programs' Value Assessment schedules and information on Cyber Command's Value Assessment coordination with the programs.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and Commander, 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 IV.

W. William Russell
Director, Contracting and National Security Acquisitions

List of Committees

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

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

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Betty McCollum
Chair
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report describes (1) actions Cyber Command has taken to define JCWA roles and responsibilities as well as interoperability goals, and (2) the extent of Cyber Command's efforts to assess the value of JCWA acquisitions.

To identify actions Cyber Command took to define Joint Cyber Warfighting Architecture (JCWA) roles and responsibilities, we obtained and reviewed relevant documents that describe the roles and responsibilities, as well as the Concept of Operations in which command officials planned to address interoperability goals for the JCWA programs. We reviewed these documents to determine whether they addressed those recommendations. We also reviewed legislative changes to Cyber Command's authority that are relevant to the JCWA and how these changes could affect JCWA acquisitions in the future.[1] We conducted follow-up meetings with officials from the Office of the Principal Cyber Advisor and the Service Principal Cyber Advisors to understand their interactions with Cyber Command and its governance of the JCWA. We also met with officials from the four JCWA program offices to learn how these organizations are working with Cyber Command's JCWA governance structure. We obtained their perspectives on the command's coordination with the JCWA programs and corroborated this information with Cyber Command to understand and describe its workforce shortages and Cyber Command's planned actions. We reviewed the JCWA Concept of Operations to identify how that document outlines interoperability of the JCWA systems and plans for the future of the architecture.

To assess Cyber Command's efforts to coordinate and assess the value of JCWA acquisitions using the Software Acquisition Pathway, we used Department of Defense (DOD) policy as well as Cyber Command and program documents to identify the command's responsibilities and plans to conduct Value Assessments. We used Department of Defense Instruction 5000.87 – *Operation of the Software Acquisition Pathway* and additional Software Acquisition Pathway guidance to identify Cyber Command and the JCWA programs' responsibilities under this acquisition pathway. Further, we used our Agile Guide to identify leading practices,

[1]Pub. L. No. 117-81, § 1507 (c)(1).

particularly in developing metrics for programs using Agile methods, such as ensuring metrics are tailored to program needs. We compared these practices with DOD policy and guidance. We obtained and reviewed JCWA acquisition program documents, including Capability Needs Statements and User Agreements to identify program plans for engaging users, and program metrics. We also identified key dates in each programs' acquisition cycle for fiscal years 2021 and 2022. In addition, these acquisition program documents provided information we used to develop our program status update in appendix II. We collected information from the JCWA program offices on their efforts to coordinate Value Assessments with Cyber Command and used meetings with program officials to clarify details and confirm the information we reviewed. We also met with Cyber Command officials to obtain their perspectives on conducting program Value Assessments and efforts to develop outcome-based metrics. We then compared this information to *Department of Defense Instruction 5000.87 – Operation of the Software Acquisition Pathway* and additional Software Acquisition Pathway guidance to assess the timing of the programs' required Value Assessments and their use of outcome-based metrics. We met with officials from the Office of the Under Secretary of Defense for Acquisition and Sustainment, who are responsible for the Software Acquisition Pathway and its supporting guidance, to confirm policy implementation steps and any changes to the pathway instruction or guidance during the period of our review.

We conducted this performance audit from December 2020 to March 2022 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.

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

All of the JCWA programs have delivered software-based capabilities that cyber warfighters are using. Based on our review of program documents and discussion with program officials, programs provide numerous capabilities to expand access to Department of Defense (DOD)-wide data, use collaboration tools to leverage data among cyber warfighters, and facilitate training and mission rehearsal for cyber mission forces. The JCWA programs still have considerable work planned before meeting all of Cyber Command's needs—enhanced use of artificial intelligence and machine learning remain in the JCWA programs' future. All four of the programs reported using Agile software development methodologies, regardless of acquisition pathway, and all programs plan to continue iterative development and delivery of new capabilities. The information below is an update of each program's status since our first report on the JCWA in November 2020.[1]

Persistent Cyber Training Environment-training, assessment, and mission rehearsal.

- Procuring service: Army
- Vendor: The 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: The Persistent Cyber Training Environment uses diverse contract vehicles to acquire required expertise and tools. For

[1]GAO-21-68.

example, the program is using other transactions, indefinite delivery/indefinite quantity, and other contracts.[2]

- Next event: The Persistent Cyber Training Environment program office plans to deliver Versions 5.0 in 2022.

The Army, as Lead Acquisition Component, initiated this program in 2016 pursuant to a prior iteration of *DOD Instruction 5000.02 Operation of the Adaptive Acquisition Framework*. The program follows the Major Capability Acquisition Pathway—DOD's legacy acquisition pathway—but tailored its approach into 5-year development periods for planning and budgeting purposes, according to officials. The Persistent Cyber Training Environment began development in December 2019. Program officials stated that the Army is evaluating whether to transition to the Software Acquisition Pathway for the next development period, starting in 2024. The program reported using an Agile approach to software development that releases incremental software upgrades based on user feedback from across the military departments. The Persistent Cyber Training Environment delivers new versions with new capabilities every 6 months, but developers share training content such as scenarios and simulated systems continuously with users. According to Cyber Command officials, the program delivered Version 4.0 in January 2022.

Cyber warfighters regularly use the Persistent Cyber Training Environment to complete various kinds of training and mission rehearsal. The program reported having almost 9,000 users across all military departments and hosting multiple large exercises for cyber warfighters. Additionally, program officials stated that the Persistent Cyber Training Environment is able to replicate real world events, such as the SolarWinds hack, to develop new training and capabilities. These officials stated that cyber warfighters, through feedback sessions and events, identified numerous capabilities for future program versions, including improvements to individual and collective operator training, certifications, and the ability to share training information within the JCWA.

[2]DOD has statutory authority to use agreements known as other transactions, which can be used to attract companies or other entities that have not typically done business with DOD. See e.g. 10 U.S.C. 2371b. Indefinite delivery/indefinite quantity contracts are awarded to one or more contractors to acquire products or services when the government does not know at the time of award the exact times or exact quantities of future deliveries. The government then places orders through the indefinite delivery contract when it knows the timing and quantity of its needs. FAR 16.504.

Unified Platform-data management and integration.

- Procuring service: Air Force
- Vendor: Unified Platform relies on a variety of government and contractor personnel leveraging the Air Force's LevelUP software factory to develop the system.[3]
- Contracting strategy: Unified Platform uses multiple contracts and contract types to acquire required expertise, labor, and tools to accomplish government-led development efforts, rather than relying on a prime contractor for systems development.
- Next event: The program manager confirmed that Program Increment 13 is scheduled for delivery by May 2022.

The Air Force, as Executive Agent, initiated Unified Platform on the Middle Tier Acquisition Pathway and transitioned the program to the Software Acquisition Pathway in July 2020—the first DOD program to do so according to officials.[4] Unified Platform continues to use a Development, Security, and Operations (DevSecOps) approach to software development. This approach emphasizes continual development, integration, and delivery of new system capabilities to users in regular iterations with emphasis on cybersecurity. Unified Platform is delivering new capabilities in 3-month program increments. The program also relies on the LevelUP software factory. 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. Unified Platform delivered its first set of

[3]The 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 that 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.

[4]Department of Defense Instruction 5000.80 defines the Middle Tier of Acquisition as a pathway to fill a gap in the Defense Acquisition System for those capabilities that have a level of maturity to allow them to be rapidly prototyped within an acquisition program or fielded within 5 years of the program start. 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 involved 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.

capabilities under the Software Acquisition Pathway, known as Program Increment 8, in January 2021.

The Unified Platform program reported delivering multiple capabilities to cyber operators. This includes making over 37 petabytes of information, across all classification levels, available to over 9,000 users. The Principal Cyber Advisors from the Army, Navy, and Air Force—staff advisors to their respective military department secretaries on cyber forces and activities—confirmed that, combined with the Joint Cyber Command and Control program, these new capabilities supported past and continue to support ongoing cyber operations. Now that the program has made DOD network data from across the military departments available to cyber warfighters, future plans include adding more data sources, expanding interoperability with allied and coalition partner systems, and enhancing artificial intelligence and machine learning driven capabilities.

Joint Cyber Command and Control-decision-making.

- Procuring service: Air Force
- Vendor: Joint Cyber Command and Control uses a variety of government and contractor personnel leveraging the LevelUP software factory with Unified Platform to develop the system.
- Contracting strategy: Joint Cyber Command and Control uses multiple contracts and contract types to acquire required expertise, labor, and tools to accomplish government-led development efforts, rather than relying on a prime contractor for systems development.
- Next event: Minimum viable capability release for situational awareness—tracking the flow of users and information on networks—is planned for May 2022.

The Air Force, as Executive Agent, established the program management office in 2017 and the program entered the Software Acquisition Pathway in October 2020. Joint Cyber Command and Control is using the same DevSecOps approach and LevelUP software factory as Unified Platform. In April 2021, the Air Force transitioned Project Ike, a prototype situational awareness capability, from the DOD Strategic Capabilities Office to the Joint Cyber Command and Control program. The program has delivered software in quarterly program increments, but also has defined two sets of deployable capabilities that the program refers to as minimum viable capability releases. The program defines one set of capabilities as the situational awareness minimum viable capability release and the second

set is battle management. The program plans to deliver the situational awareness release in May 2022 and the battle management release 6 months later.

The Joint Cyber Command and Control program reported delivering multiple command and control tools to cyber operators in addition to harnessing data from Unified Platform and other sources. Military department cyber representatives and program officials stated that Joint Cyber Command and Control was important in the government response to a widespread hacking campaign as well as helping secure key U.S. events and systems. For future efforts, beyond completion of its minimum viable capability releases, the program office anticipates increasing integration with other JCWA capabilities, such as the Persistent Cyber Training Environment, and increasing program use of artificial intelligence and machine learning.

Joint Common Access Platform-mission enablement.

- Procuring service: Army
- Vendor: ManTech is the prime contractor and system integrator, currently supported by nine subcontractors, according to officials.
- Contracting strategy: Joint Common Access Platform officials stated they are currently using a single prime contractor and system integrator for development, but expect to transition to a competitive indefinite delivery/indefinite quantity contract with a system integrator for future work.
- Next event: The Joint Common Access Platform program office plans to deliver minimum viable capability release 2 in April 2022.

The Army is the lead for this program, which the service formally initiated in May 2020. The program entered the Software Acquisition Pathway in November 2020. Program officials told us that they anticipate longer delivery timelines for initial program increments, but they expect to reach a 3-month delivery cadence once the program fields baseline capabilities. The Joint Common Access Platform builds upon earlier systems, with the intent of incorporating the best components of those systems. The program manager said it delivered minimum viable capability release 1 in December 2021, although these capabilities will not be operational until additional testing is complete.

Appendix III: Department of Defense Comments

OFFICE OF 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-22-104695, 'DEFENSE ACQUISITIONS: Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities,' dated January 24, 2022 (GAO Code 104695).

Enclosed is DoD's response to the subject report. My point of contact is Mr. Mark Godino who may be reached at mark.godino.civ@mail.mil and phone 571-309-4934.

Sincerely,

Tanya M. Skeen
Acting Assistant Secretary of Defense
for Acquisition

Enclosure:
As stated

GAO DRAFT REPORT DATED JANUARY 24, 2022
GAO-22-104695 (GAO CODE 104695)

"DEFENSE ACQUISITIONS: CYBER COMMAND NEEDS TO DEVELOP METRICS TO ASSESS WARFIGHTING CAPABILITIES"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should direct the Commander, Cyber Command, to develop outcome-based metrics for the JCWA programs that are on the Software Acquisition Pathway to support Value Assessments the command has not yet initiated.

DoD RESPONSE: Concur. For clarification DoD recommends changing "to support Value Assessments the command has not yet initiated" to "to support command initiated Value Assessments."

Cyber Command (CYBERCOM) agrees that continued emphasis on, and improvement of, outcome-based metrics is necessary to support Department objectives and would be served by Departmental directive.

To provide a more complete picture of the external dependencies affecting CYBERCOM efforts to build an outcome-based metrics program, it should be noted that CYBERCOM has submitted a request to DoD for additional resources to enhanced the command's ability to develop in this area, which has a decision pending at OMB.

The following specific CYBERCOM Value Assessment (VA) accomplishments further demonstrate CYBERCOM's initiative:

a. Issued TASKORD 21-0097, 21 December 2021, to relevant DoD stakeholders for the collection of survey responses to support the Unified Platform (UP) VA.
b. Implemented an O-6 led JCWA Metrics Working Group with meetings weekly.
c. Coordinated with Office of the Under Secretary for Defense, Acquisition and Sustainment (OUSD(A&S)) to develop value streams along the following metrics categories: (1) Mission effectiveness; (2) Cost efficiencies; (3) Workload reduction; (4) Manpower reduction; (5) Equipment footprint reduction; and (6) User adoption.
d. Published the current VA schedule which has been coordinated with the Service Program Management Offices:
    - UP - Program Increment (PI), March 2022
    - Joint Cyber Command and Control (JCC2) - PI, March 2022
    - Joint Common Access Platform (JCAP) - PI, June 2022

Accessible Text for Appendix III: Department of Defense Comments

March 9, 2022

Mr. William Russell
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
44 I 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-22-104695, 'DEFENSE ACQUISITIONS: Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities,' dated January 24, 2022 (GAO Code 104695).

Enclosed is DoD's response to the subject report. My point of contact is Mr. Mark Godino who may be reached at mark.godino.civ@mail.mil and phone 571-309-4934.

Sincerely,

Tanya M. Skeen
Acting Assistant Secretary of Defense
for Acquisition

Enclosure:
As stated

GAO DRAFT REPORT DATED JANUARY 24, 2022 GAO-22-104695 (GAO CODE 104695)

“DEFENSE ACQUISITIONS: CYBER COMMAND NEEDS TO DEVELOP METRICS TO ASSESS WARFIGHTING CAPABILITIES”

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should direct the Commander, Cyber Command, to develop outcome-based metrics for the JCWA programs that

are on the Software Acquisition Pathway to support Value Assessments the command has not yet initiated.

DoD RESPONSE: Concur. For clarification DoD recommends changing “to support Value Assessments the command has not yet initiated” to “to support command initiated Value Assessments.”

Cyber Command (CYBERCOM) agrees that continued emphasis on, and improvement of, outcome-based metrics is necessary to support Department objectives and would be served by Departmental directive.

To provide a more complete picture of the external dependencies affecting CYBERCOM efforts to build an outcome-based metrics program, it should be noted that CYBERCOM has submitted a request to DoD for additional resources to enhanced the command’s ability to develop in this area, which has a decision pending at OMB.

The following specific CYBERCOM Value Assessment (VA) accomplishments further demonstrate CYBERCOM's initiative:

a. Issued TASKORD 21-0097, 21 December 2021, to relevant DoD stakeholders for the collection of survey responses to support the Unified Platform (UP) VA.

b. Implemented an O-6 led JCWA Metrics Working Group with meetings weekly.

c. Coordinated with Office of the Under Secretary for Defense, Acquisition and Sustainment (OUSD(A&S)) to develop value streams along the following metrics categories: (1) Mission effectiveness; (2) Cost efficiencies; (3) Workload reduction; (4) Manpower reduction; (5) Equipment footprint reduction; and (6) User adoption.

d. Published the current VA schedule which has been coordinated with the Service Program Management Offices:

- UP - Program Increment (PI), March 2022
- Joint Cyber Command and Control (JCC2) - PI, March 2022
- Joint Common Access Platform (JCAP) - PI, June 2022

Appendix IV: 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, Justin Jaynes, Assistant Director; Burns C. Eckert, Analyst-in-Charge; and Brian Fersch made key contributions to this report. Other contributors included Taylor Boeckman; Virginia Chanley; Raj Chitikila; Yvette Gutierrez; Jennifer Leotta; Christine Pecora; Edward J. SanFilippo; Jessica Steele; and Robin Wilson.

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/about/what-gao-does/fraudnet

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548