United States Government Accountability Office

Report to Congressional Committees

March 2021

WEAPON SYSTEMS CYBERSECURITY

Guidance Would Help DOD Programs Better Communicate Requirements to Contractors

GAO@100

Highlights

Highlights of GAO-21-179, a report to congressional committees

March 2021

WEAPON SYSTEMS CYBERSECURITY

Guidance Would Help DOD Programs Better Communicate Requirements to Contractors

Why GAO Did This Study

DOD's network of sophisticated, expensive weapon systems must work when needed, without being incapacitated by cyberattacks. However, GAO reported in 2018 that DOD was routinely finding cyber vulnerabilities late in its development process.

A Senate report accompanying the National Defense Authorization Act for Fiscal Year 2020 included a provision for GAO to review DOD's implementation of cybersecurity for weapon systems in development. GAO's report addresses (1) the extent to which DOD has made progress in implementing cybersecurity for weapon systems during development, and (2) the extent to which DOD and the military services have developed guidance for incorporating weapon systems cybersecurity requirements into contracts.

GAO reviewed DOD and service guidance and policies related to cybersecurity for weapon systems in development, interviewed DOD and program officials, and reviewed supporting documentation for five acquisition programs. GAO also interviewed defense contractors about their experiences with weapon systems cybersecurity.

What GAO Recommends

GAO is recommending that the Army, Navy, and Marine Corps provide guidance on how programs should incorporate tailored cybersecurity requirements into contracts. DOD concurred with two recommendations, and stated that the third—to the Marine Corps—should be merged with the one to the Navy. DOD's response aligns with the intent of the recommendation.

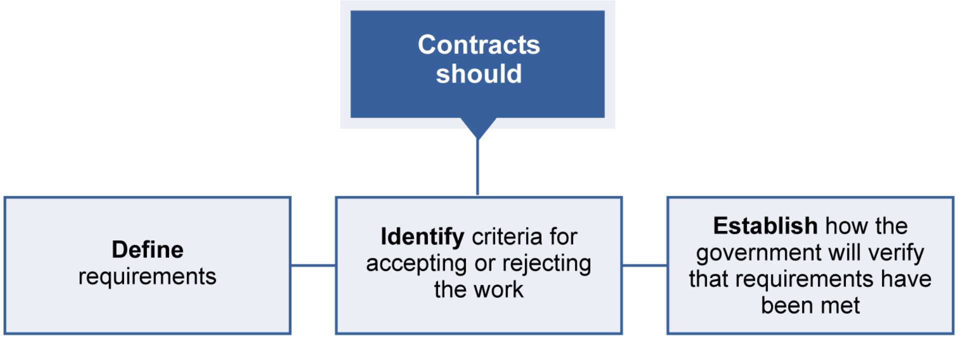
View GAO-21-179. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov.

What GAO Found

Since GAO's 2018 report, the Department of Defense (DOD) has taken action to make its network of high-tech weapon systems less vulnerable to cyberattacks. DOD and military service officials highlighted areas of progress, including increased access to expertise, enhanced cyber testing, and additional guidance. For example, GAO found that selected acquisition programs have conducted, or planned to conduct, more cybersecurity testing during development than past acquisition programs. It is important that DOD sustain its efforts as it works to improve weapon systems cybersecurity.

Contracting for cybersecurity requirements is key. DOD guidance states that these requirements should be treated like other types of system requirements and, more simply, "if it is not in the contract, do not expect to get it." Specifically, cybersecurity requirements should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that requirements have been met. However, GAO found examples of program contracts omitting cybersecurity requirements, acceptance criteria, or verification processes. For example, GAO found that contracts for three of the five programs did not include any cybersecurity requirements when they were awarded. A senior DOD official said standardizing cybersecurity requirements is difficult and the department needs to better communicate cybersecurity requirements and systems engineering to the users that will decide whether or not a cybersecurity risk is acceptable.

Incorporating Cybersecurity in Contracts



Contracts should

Define requirements

Identify criteria for accepting or rejecting the work

Establish how the government will verify that requirements have been met

Source: GAO analysis of DOD information. | GAO-21-179

DOD and the military services have developed a range of policy and guidance documents to improve weapon systems cybersecurity, but the guidance usually does not specifically address how acquisition programs should include cybersecurity requirements, acceptance criteria, and verification processes in contracts. Among the four military services GAO reviewed, only the Air Force has issued service-wide guidance that details how acquisition programs should define cybersecurity requirements and incorporate those requirements in contracts. The other services could benefit from a similar approach in developing their own guidance that helps ensure that DOD appropriately addresses cybersecurity requirements in contracts.

Contents

Tables

Figures

Abbreviations

CIO	chief information officer
CMMC	Cybersecurity Maturity Model Certification
CROWS	Cyber Resiliency Office for Weapons Systems
DOD	Department of Defense
IT	information technology
MCAAP	Marine Corps Assessment and Authorization Process
NAVAIR	Naval Air Systems Command
NIST	National Institute of Standards and Technology
RMF	risk management framework

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

441 G St. N.W.
Washington, DC 20548

March 4, 2021

Congressional Committees

The nation’s network of sophisticated, expensive weapon systems must work when needed, without being incapacitated by cyberattacks. As we reported in 2018, the Department of Defense (DOD) had only recently begun prioritizing weapon systems cybersecurity.[1] Specifically, DOD’s weapon systems acquisition process had struggled to deliver weapons that were cyber resilient, meaning they are still able to fulfill missions in the event of a cyberattack. In its 2019 Annual Report, DOD’s Office of the Director, Operational Test and Evaluation—echoing findings from prior assessments—reported that critical missions remain at high risk of disruption from adversary cyber actions and that DOD continues to field systems without adequate cybersecurity.[2] While DOD is developing and fielding increasingly software-intensive, networked weapon systems as a means of gaining a warfighting advantage, adversaries are making significant investments in offensive cyber capabilities, which they could use against U.S. forces in concert with other types of military attacks.

According to DOD policy, acquisition program officials should plan for and implement cybersecurity protections early and often throughout their program’s lifecycle. Incorporating cybersecurity practices from the earliest stages of an acquisition is typically easier, less costly, and more effective than trying to add, or bolt on, cybersecurity protections late in the development cycle or after a system is fielded. Moreover, because contractors have a key role in designing and building DOD weapon systems, DOD must communicate its cybersecurity requirements in its acquisition program contracts, just as it would with other types of performance requirements. If the government does not include certain specifications in a contract, it runs the risk that modifications will be needed after award that necessitate the negotiation of an equitable adjustment to provide the contractor with additional time and compensation. DOD guidance says simply, “if it is not in the contract, do not expect to get it.”

[1] GAO, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, D.C.: October 9, 2018).

[2] Department of Defense, Director, Operational Test and Evaluation, *FY 2019 Annual Report* (December 20, 2019).

The Senate report accompanying the National Defense Authorization Act for Fiscal Year 2020 included a provision for us to annually review DOD's efforts to improve the cybersecurity of its major defense acquisition programs. Our report addresses (1) the extent to which DOD has made progress in implementing cybersecurity protections for weapon systems during development, and (2) the extent to which DOD and the military services have developed guidance for incorporating weapon systems cybersecurity requirements in contracts.

To address both objectives, we reviewed DOD and military service level policies and guidance related to the implementation of cybersecurity for weapon systems in development.[3] Key DOD policies for information assurance, cybersecurity, acquisition, and requirements include DOD Instruction 5000.02, Operation of the Defense Acquisition Systems; DOD Instruction 5000.82, Acquisition of Information Technology; DOD Instruction 8500.01, Cybersecurity; DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT); and DOD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System. Key DOD guidance documents include the DOD Program Manager's Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Lifecycle; the DOD Cybersecurity Test and Evaluation Guidebook; the Joint Capabilities Integration and Development System Manual; the Cyber Survivability Endorsement Implementation Guide; the Defense Acquisition Guidebook; the Cybersecurity Strategy Outline and Guidance; and DOD handbooks on contracting activities. Service level guidance is discussed in the body of the report.

To inform each objective, we interviewed officials from several Office of the Secretary of Defense organizations, including the Director, Operational Test and Evaluation; Office of the Chief Information Officer (CIO); Office of the Chairman of the Joint Chiefs of Staff; Office of the Under Secretary of Defense (Acquisition and Sustainment); Office of the Under Secretary of Defense (Research and Engineering); and the Defense Digital Service. We interviewed officials with cybersecurity, contracting, and acquisition responsibilities from four military services as well as five selected acquisition program offices. To select the program

[3] The term "services" in this report generally refers to the Army, Navy, Marine Corps, and Air Force. We did not include the Space Force in this audit because the Space Force was established in December 2019, after this audit began, and has not yet established its acquisition organization. In addition, we determined that the Space Force has not yet published independent policies or guidance related to cybersecurity of weapon systems acquisitions. We also did not include the Coast Guard, which is a component within the Department of Homeland Security.

offices, we used a purposeful sample of major defense acquisition programs representing, among other things, different services and types of systems. We also interviewed representatives from 10 defense contractors, 10 legal or consultant organizations, four research organizations with cybersecurity expertise, and two defense industry trade groups. A number of issues discussed in this report have been on GAO's high-risk list for years, including DOD's weapon systems acquisitions as well as the nation's cybersecurity.[4] See appendix I for additional information on our scope and methodology.

The focus of this report is contracting for weapon systems cybersecurity, particularly how DOD acquisition programs establish and define requirements and then communicate those requirements to contractors. Since these activities—establishing, defining, and communicating requirements—primarily occur early in the acquisition process, we did not look in-depth at other important cybersecurity activities, such as testing, that occur later in the acquisition process.[5]

In March 2020, during the course of this engagement, the President declared a national state of emergency as a result of the spread of the Coronavirus Disease 2019. Like other federal agencies, GAO implemented changes to curb the spread of the virus. Accordingly, we reduced the scope of our work so that our analysis did not depend on access to systems we use to store and process classified information sources. We plan to include these sources in future work.

We conducted this performance audit from July 2019 to March 2021 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 conclusion based on our audit objectives.

[4] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: March 6, 2019).

[5] In early 2020, DOD introduced the Cybersecurity Maturity Model Certification (CMMC), which prescribes information network security standards certification that defense contractors will eventually be required to achieve before competing for covered DOD contracts. We did not include CMMC in the scope of this work but have an ongoing review that focuses on CMMC.

Background

Modern DOD weapon systems depend on software and IT to achieve their intended performance.[6] Compared to their predecessors, these systems require a greater number of communications paths for sharing information among various types of subsystems as well as with external systems, enabling a range of warfighting capabilities.[7] As outlined in the 2018 National Defense Strategy, DOD plans to continue modernizing key capabilities through investments in software- and IT-intensive systems and technologies, such as advanced networks, automation, and artificial intelligence, as well as through the integration of cyber capabilities into all types of military operations. For example, the Army plans to replace decades-old vehicles, including the Bradley infantry fighting vehicle and the Abrams main battle tank, with new systems that may incorporate autonomous or semi-autonomous operations requiring robust and secure networking capabilities.[8]

Just as the growth of networked or internet-enabled consumer technologies and devices heightens security risks in the face of increasingly sophisticated cyber threats, as we have reported, DOD's growing dependence on software and IT significantly expands weapons' attack surfaces.[9] Any exchange of information is a potential access point for an adversary.[10] A system designed and built to exchange information with many other systems or subsystems has more potential vulnerabilities to address than a system that has few such connections.

[6] DOD describes its IT as encompassing a variety of forms that "range in size and complexity from individual hardware and software products to stand-alone systems to massive computing environments, enclaves, and networks." The focus of this report is weapon systems that include platform IT, which is "IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to mission performance of special purpose systems." Department of Defense Instruction 8500.01, *Cybersecurity* (October 7, 2019); Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)* (July 28, 2017).

[7] GAO-19-128.

[8] GAO, *Next Generation Combat Vehicle: As Army Prioritizes Rapid Development, More Attention Needed to Provide Insight on Cost Estimates and Systems Engineering Risks*, GAO-20-579 (Washington, D.C.: August 6, 2020).

[9] GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017); and *Internet of Things: Status and Implications of an Increasingly Connected World*, GAO-17-75 (Washington, D.C.: May 15, 2017).

[10] GAO-19-128.

As we reported in 2018, DOD had not prioritized weapon systems cybersecurity until recently, and was still determining how best to address it during the acquisition process. The department had historically focused its cybersecurity efforts on protecting networks and traditional IT systems, but not weapon systems, and key acquisition and requirements policies did not focus on cybersecurity. As a result, DOD likely designed and built many systems without adequate cybersecurity. In operational testing, DOD routinely found mission-critical cybersecurity vulnerabilities in systems under development. Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications. In addition, due to limitations in the extent and sophistication of testing, DOD was likely aware of only a fraction of the total vulnerabilities in its weapon systems.

We also reported that DOD had taken a number of major steps since 2014 to improve weapon systems cybersecurity.[11] Specifically, DOD issued or updated a variety of department-wide policies, guidance documents, and memorandums to better integrate cybersecurity into the acquisition process and to promote more cyber resilient weapon systems. These steps demonstrate DOD's increased emphasis on weapon systems cybersecurity, aligning with DOD's commitment in the 2018 Cyber Strategy to "defend its own networks, systems, and information from malicious cyber activity," and to "ensure the U.S. military's ability to fight and win wars in any domain, including cyberspace." Ultimately, DOD's success in improving weapon systems cybersecurity depends on the extent to which the military services and acquisition community execute these changes to produce better outcomes in their programs.

Weapon Systems Cybersecurity Practices

A cyberattack is an attempt to exploit a vulnerability in a system or network to compromise its confidentiality, integrity, or availability.[12] Even an attack that does not compromise a system or network may delay or disrupt normal operations, undermining the owner's or operator's confidence in their security, according to a senior official from the Office of the Director, Operational Test and Evaluation.

[11] GAO-19-128.

[12] Protecting confidentiality means limiting information and system access to authorized users and purposes. Protecting integrity means ensuring information is not modified or deleted by unauthorized users. Protecting availability means ensuring information and services are available to authorized users. Our prior work discusses in greater detail the general process and terminology of cyberattack and cyber defense. See GAO-19-128.

Cybersecurity practices are intended to protect IT by preventing, detecting, and responding to attacks. They aim to reduce the likelihood that attackers can access DOD systems and limit the damage if they do. Weapon systems confront a variety of cybersecurity challenges throughout the acquisition process. The goal of weapon systems cybersecurity is to help ensure that a system is able to execute its mission in the face of a cyberattack or adverse conditions. A 2015 RAND report identified the following six challenges, summarized below, for managing weapon systems cybersecurity:[13]

- **Complex systems require specialized knowledge**. Modern weapon systems are highly complex, complicating the task of finding and fixing vulnerabilities without compromising functionality. Effective cybersecurity is a technical challenge involving features that might be integral to a system's design, detailed knowledge of which may be confined to only a few experts.
- **Functionality and security can sometimes be at odds**. There are necessary trade-offs between functionality and security. Engineers are willing to accept some level of vulnerability to achieve the functionality that operators need to perform their missions. For weapon systems, an appropriate balance between security and functionality is critical.
- **Threats evolve and adapt**. Cyber threats are rapidly evolving and adapting to countermeasures, such that security solutions implemented at any point in time could be insufficient to deal with future threats.
- **Attackers have advantages**. Cyberattackers have some advantages over cyber defenders. Whereas an attacker only needs to find and exploit one system vulnerability, the defender needs to account for and mitigate risk throughout the system. As a result, cyber defense is both more resource intensive and more difficult.
- **Each new connection is a potential vulnerability**. Systems are interconnected in a variety of ways, such that a vulnerability in one system may be exploited to gain access to another system. An attacker may be able to leverage a vulnerability in a noncritical component or tertiary system to gain access to a system's most critical components.

[13] RAND, *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles* (Santa Monica, CA: 2015).

- **Complete security is unattainable**. Because cyber threats evolve and adapt and cyberattackers have some advantages over cyber defenders, it is impractical to assume that complete security is attainable. Decision makers must determine what level of security is sufficient for their system and mission given finite resources.

Effective Weapon Systems Cybersecurity Practices Depend on Cybersecurity Requirements Development and Contracting Activities

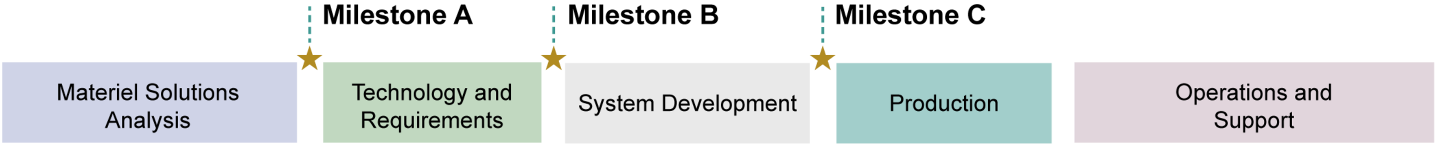
DOD's policies governing major defense acquisition programs outline a series of phases and associated activities to deliver weapon systems that meet a capability gap. While there are important cybersecurity considerations in each acquisition phase, our prior work has shown that establishing firm, feasible requirements is a key early step to reduce risk and set a program up for success.[14] Through solicitations and contracting, the acquisition program then communicates those requirements to the contractor that will develop and produce the system. Contractors may provide important support to the program during requirements development, such as working with the acquisition program office to refine requirements after contract award. Overall, defining needs and then contracting for a solution that meets those needs are as relevant to cybersecurity requirements as they are to other kinds of performance requirements.

Figure 1 shows an overview of DOD's acquisition process for major defense acquisition programs.[15]

[14] GAO, *Weapon System Requirements: Detailed Systems Engineering Prior to Product Development Positions Programs for Success*, GAO-17-77 (Washington, D.C.: November 17, 2016).

[15] In April 2020, DOD reissued its key acquisition instruction to, among other things, establish an adaptive acquisition framework comprised of six acquisition pathways. This review focuses on major defense acquisition programs, which are now covered under the major capability acquisition pathway, and a few of the early, critical steps in that process. Some, but not all, of the activities discussed in this report are relevant to other acquisition pathways. For a more comprehensive discussion of the major defense acquisition program process and the six acquisition pathways, see GAO, *Defense Acquisitions Annual Assessment: Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight*, GAO-20-439 (Washington, D.C.: June 3, 2020).

Figure 1: Department of Defense (DOD) Major Defense Acquisition Program Lifecycle



Source: GAO analysis of DOD information. | GAO-21-179

Developing Cybersecurity Requirements for Weapon Systems Helps Position Acquisition Programs for Success

Developing requirements that address a military need is a key component of successful weapon systems acquisitions. As we reported in 2016, acquisition programs typically use systems engineering to, along with the program contractor, break down validated top-level capability requirements into more specific capability requirements, known as performance specifications, which are then used to create detailed design requirements.[16] In addition to providing requirements traceability to help ensure that the system characteristics and performance address the capability gap, systems engineering also allows acquisition program managers and decision makers to make informed trade-offs between detailed requirements and available resources. As a result, successful acquisition programs do not begin system development until after completing the bulk of their systems engineering activities.[17] The design requirements lead to various system baselines that describe the system's performance requirements, how the subsystems will work together, and the system's final design, among other things.

Cybersecurity requirements are a component of a system's overall requirements. DOD acquisition policy states that cybersecurity is a requirement for all DOD programs and must be implemented in all phases of the acquisition cycle.[18] It also requires acquisition program managers to include cybersecurity in system performance specifications. Similarly, in 2015 guidance on cybersecurity for acquisition program managers,

[16] GAO-17-77.

[17] GAO-17-77.

[18] In 2017, DOD updated its key instruction governing the acquisition process to include a new cybersecurity enclosure. In December 2020, after the scope of our review, DOD issued a new instruction that incorporates and cancels the cybersecurity enclosure. Department of Defense Instruction 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers* (December 31, 2020).

DOD described a key tenet of weapon systems cybersecurity as treating cybersecurity requirements “like other system requirements.”[19] Therefore, cybersecurity requirements should follow a similar pattern as other system requirements, moving from general to more specific and detailed as the acquisition program proceeds.

Since 2015, DOD has required that certain acquisition programs include cyber survivability as part of the mandatory system survivability key performance parameter, which is one type of top-level program requirement, or attribute, that defines a weapon system’s critical performance goals.[20] In addition, DOD’s requirements development policy states that key performance parameters or attributes should establish measures for system survivability that address cyber threats. Cyber survivability, in this context, is meant to ensure that weapon systems are designed to prevent, mitigate, and recover from cyberattacks. However, the details of how cyber survivability is achieved for each system depend on the system’s mission, number and type of internal and external communication paths, and the types of cyber threats it may face, among other things.

Table 1 briefly outlines key requirements documents early in the acquisition cycle and the role of cybersecurity requirements in each.

Table 1: Key Requirements Documents and Cybersecurity Early in the Acquisition Cycle

Document Name	Description
Initial capabilities document	Documents a specific capability gap and the need for a materiel solution, or a combination of materiel and non-materiel solutions, to fill the gap. The initial capabilities document should reflect early, high-level cybersecurity capability requirements along with all other mission capability requirements.
Capability development document	Specifies the requirements and performance attributes, including key performance parameters, for the system that will deliver the capability that meets the criteria in the initial capabilities document. Cybersecurity performance attributes defined in the capability development document must be understandable, testable, measurable, and achievable. The capability development document must be validated before the program releases a request for proposals to industry.

[19] Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *DOD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, Version 1.0 (Washington, D.C.: September 2015).

[20] Key performance parameters are performance attributes that define the capabilities most critical to mission effectiveness. The other two types of performance attributes, key system attributes and additional performance attributes, define other characteristics necessary to achieve satisfactory performance.

Document Name	Description
Program protection plan	Defines the program's critical information and mission-critical functions as well as the systems engineering and security activities the program plans to use to mitigate those risks, including cybersecurity. The program protection plan is included in requests for proposals, and program managers should update the program protection plan after contract award to reflect the selected contractor's proposal.
Cybersecurity strategy	Identifies both the program's long-term approach for, as well as its implementation of, cybersecurity throughout the program lifecycle. The document, an appendix to the program protection plan, is intended to serve as a management tool for program offices to plan for, document, assess, mitigate, and manage cybersecurity risks as the program matures.
Test and evaluation master plan	Describes all program test activities after the start of technology development, including a strategy for testing and evaluating cybersecurity throughout the acquisition lifecycle. Testing cybersecurity as part of developmental testing is intended to identify cyber vulnerabilities and to inform necessary mitigations as well as test critical functions. Testing cybersecurity as part of operational testing is intended to assess the ability of the system to allow personnel to execute critical missions in the expected operational environment.

Source: GAO analysis of DOD policy and guidance documents. | GAO-21-179

Contractor's Solution May Not Align to Military Need Unless Cybersecurity Requirements Are Communicated in Contracts

Defense contractors typically design and build weapon systems. This means that DOD must translate its requirements into contract terms and conditions, which establish an agreement between the government and the contractor. Weapon system contracts generally cover, among other things, the cost or price of the work to be performed, the schedule for delivering goods or services, and performance requirements. DOD policy requires that acquisition program managers confirm that cybersecurity and system security requirements are incorporated into contracts.

Cybersecurity requirements may appear in different portions of the contract. The different contract sections should complement each other and establish a coherent approach to developing a weapon system. For example, the statement of work may identify various activities related to designing a system that meets the performance requirements. In turn, the performance requirements may be outlined in the system specifications in accordance with the schedule identified in the contract data requirements list.

Table 2 lists some of the key sections of the contract for communicating cybersecurity requirements.

Table 2: Key Contract Documents

Contract Document	Description
Statement of work	Describes the work that a contractor is to perform, where the work will be performed, the period of performance, and any applicable conditions, among other things. A statement of work may include a work breakdown structure that reflects different activities the contractor must perform, such as designing and developing the system and conducting and documenting cybersecurity tests. To the extent possible, the statement of work should describe the tasks to be completed as opposed to how the contractor should complete the tasks.
Contract data requirements list	Identifies data, analyses, reports, or other documents the contractor must provide. For example, the government may require the contractor to develop a cybersecurity strategy and implementation plan that describes how the contractor will implement and assess cybersecurity controls. The contract data requirements list identifies the data the contractor must deliver as well as descriptions of the format, content, and how the data will be used.
System specification[a]	Defines a system's quantitative and qualitative design and performance requirements, including detailed cybersecurity requirements. It may identify performance requirements such as achieving a specific speed or range. The system specification defines form, fit, and function characteristics, which could include the size or weight of the system. The system specification should also identify any applicable standards that apply and how the government plans to assess whether each capability is met.
Other	Contracts may include many other provisions or clauses in addition to the statement of work, contract data requirements list, and system specification, some of which are required by acquisition regulations. For example, DOD has a required contract clause that requires contractors to protect certain information about the system they are developing.[b]

Source: GAO analysis of DOD policy and guidance documents. | GAO-21-179

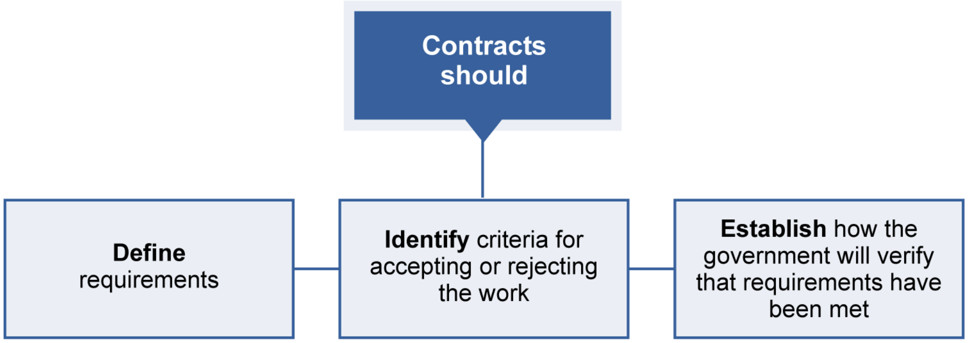
[a] The system specification may be referred to by other names such as a system requirements document or system performance specification.

[b] Defense Federal Acquisition Regulation Supplement, 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*.

The contractor is generally responsible for meeting the terms of the contract, so it is important that the contract reflect the government's requirements. DOD guidance states that the government should include in the contract all applicable terms and conditions necessary for the system to be acceptable. This applies to all aspects of the system including performance requirements such as speed, range, capacity, and cybersecurity. According to DOD guidance, contract requirements should be clear so that the government and contractor have a common understanding of the work to be performed and what is considered acceptable performance. DOD guidance describes characteristics of how requirements should be articulated in contract language, including that contracts define requirements, identify criteria for accepting or rejecting the work, and establish how the government will verify that requirements have been met.[21]

Figure 2 shows characteristics that, according to DOD guidance, contracts should include.

Figure 2: Incorporating Cybersecurity in Contracts


Contracts should
Define requirements
Identify criteria for accepting or rejecting the work
Establish how the government will verify that requirements have been met

Source: GAO analysis of DOD information. | GAO-21-179

DOD Established the Risk Management Framework to Mitigate Cybersecurity Risk to DOD Systems

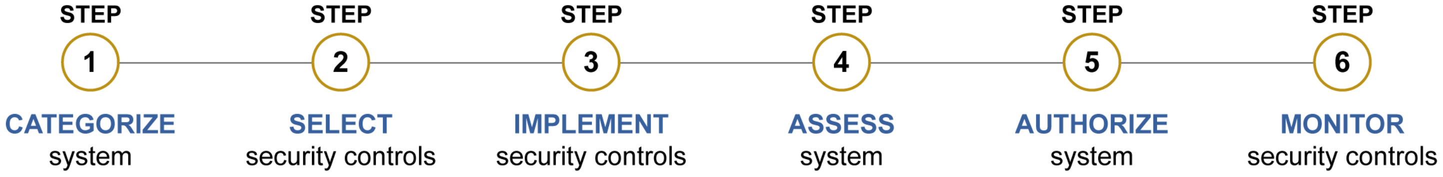
In 2014, DOD established the risk management framework (RMF), a six-step process for managing cybersecurity risk to DOD systems, including weapon systems acquisitions that include IT.[22] In related guidance from 2015, DOD stated that RMF adds a risk-based approach to the implementation of cybersecurity and that early integration of cybersecurity and RMF activities in acquisition processes reduces risk throughout the acquisition lifecycle. DOD's acquisition policy illustrates that RMF informs but does not replace acquisition processes for DOD IT.

The RMF steps and associated activities are shown in figure 3.

[21] Department of Defense MIL-HDBK-245D, *Department of Defense Handbook For Preparation of Statement of Work (SOW)*, (April 3, 1996); Department of Defense MIL-STD-961E, *Department of Defense Standard Practice, Defense and Program-Unique Specifications Format and Content* (April 2, 2008).

[22] DOD designed its RMF instruction, DOD Instruction 8510.01, to include a "companion guide" to National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, which NIST later updated. Specifically, DOD's RMF instruction is intended to provide guidance for implementing NIST Special Publication 800-37 within DOD. DOD updated Instruction 8510.01 in 2017. Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)* (July 28, 2017).

Figure 3: Six Steps of Department of Defense's (DOD) Risk Management Framework



Source: GAO analysis of DOD information. | GAO-21-179

Note: In December 2018, NIST updated its RMF publication to include a 7th step, "Prepare". A DOD official said the department is in the process of updating its RMF instruction and plan to include the new step in the process.

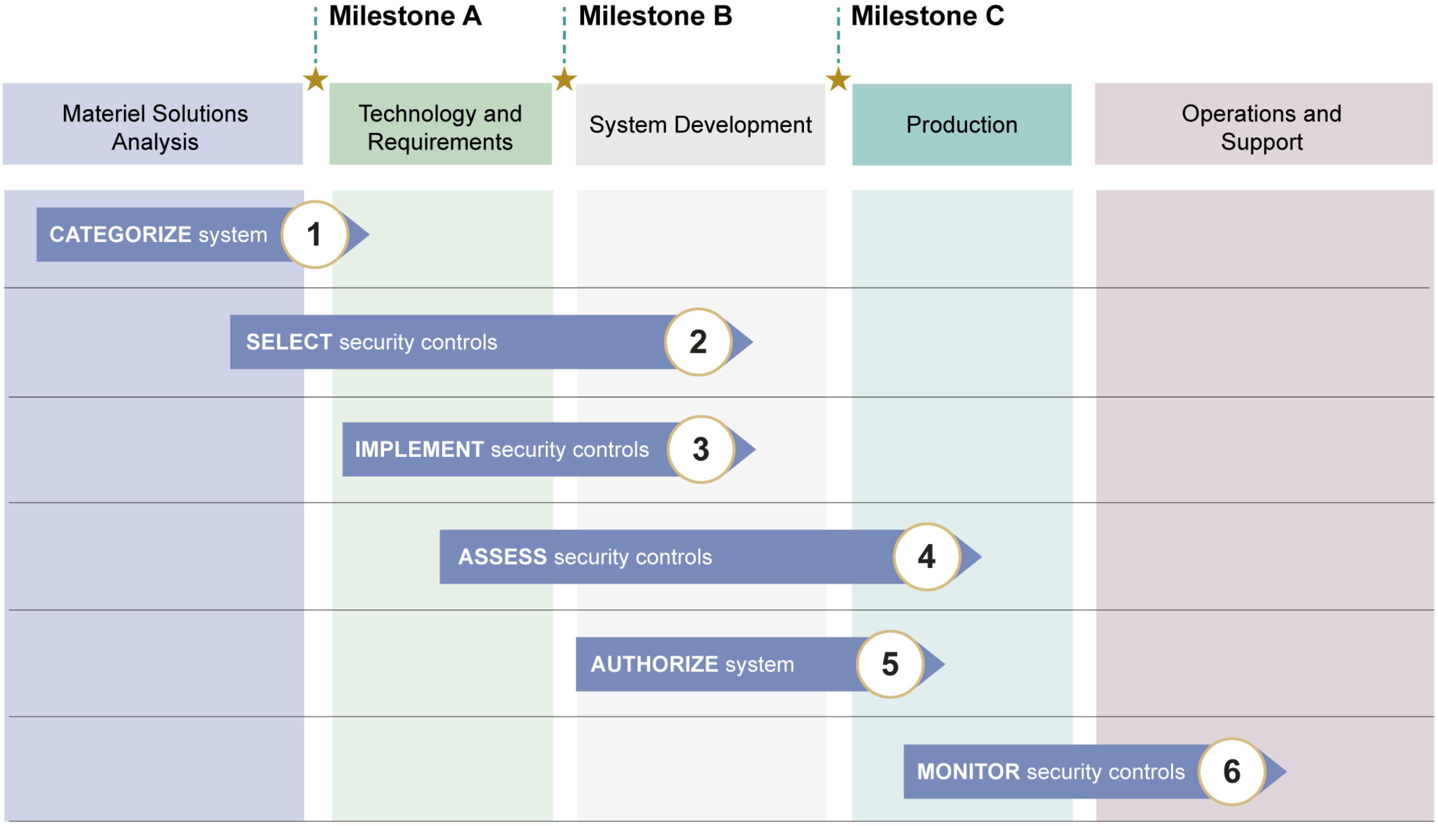
RMF is structured around identifying, implementing, assessing, and managing security controls, which are safeguards or countermeasures applied to a system to protect the confidentiality, integrity, and availability of the system and its information. For example, establishing protections for each type of wireless connection to a system is a safeguard against unauthorized access. According to National Institute of Standards and Technology (NIST) guidance, security controls should be incorporated into systems engineering processes as part of the acquisition program's plans to meet its security requirements. Consistent with NIST policy, DOD guidance states that an acquisition program should implement a tailored set of security controls based on risk assessments of threats and potential impact to mission, among other things. In general, acquisition programs implement RMF as follows:

- Step 1 – **Categorize the system** according to the potential impact (low, moderate, high) resulting from the loss of confidentiality, integrity, and availability if a security breach occurs. For example, a system whose potential impacts to those three security objectives would all be deemed moderate would be classified as a "moderate-moderate-moderate" category system.
- Step 2 – **Select security controls** for the weapon system based on its categorization and other factors. Approximately 300-500 security controls are initially applicable to weapon systems in development, depending on the system's categorization. This list serves as the program's "baseline" controls.
- Step 3 – **Implement controls** through design, production, or deployment. Some controls, such as encryption, are incorporated into a system's hardware or software. Other controls may be inherited from external sources or how a system is operated. For example, systems connected to classified networks may receive some protection from the network's security.

- Step 4 – **Assess controls** to ensure they were properly implemented. Acquisition programs develop, review, and approve a security control assessment plan that aligns with the program's other test and certification activities.
- Step 5 – **Authorize the system** to connect to operational networks or other systems. Each military service selects authorizing officials who review relevant documentation and determine whether a system has met cybersecurity requirements, such as sufficiently addressing known vulnerabilities.
- Step 6 – **Monitor the system** in its operational environment for, among other things, configuration changes that might affect the system's security posture or performance indicators that might suggest a security control is not operating effectively.

The RMF steps are sequential and roughly align to one or more acquisition phases; however, the process, according to NIST guidance, is intended to be flexible and iterative, allowing an acquisition program to respond to new information or circumstances. For example, the results of an assessment in step 4 may require reassessing control implementation in step 3. Figure 4 provides a general overview of how the RMF steps align with DOD's acquisition process for major defense acquisition programs.

Figure 4: Department of Defense's (DOD) Risk Management Framework in the Acquisition Cycle



Milestone A
Milestone B
Milestone C
Materiel Solutions Analysis
Technology and Requirements
System Development
Production
Operations and Support
CATEGORIZE system 1
SELECT security controls 2
IMPLEMENT security controls 3
ASSESS security controls 4
AUTHORIZE system 5
MONITOR security controls 6

Source: GAO analysis of DOD information. | GAO-21-179

DOD and the Military Services Have Taken Action to Improve Weapon Systems Cybersecurity

DOD has made strides in improving weapon systems cybersecurity in recent years. We identified four areas of progress: greater access to cyber expertise, increased use of cyber assessments, better tailoring of security controls, and additional cybersecurity guidance. We reviewed five acquisition programs: a radar, an anti-jammer, a ship, a ground vehicle, and a missile. Officials from these acquisition programs reported having a greater focus on and more resources committed to cybersecurity in several areas, including greater access to cyber expertise and increased use of cyber assessments. Senior DOD and military service officials we spoke with also identified progress with security controls and guidance. While it is too soon to determine whether these efforts will lead to more secure systems, they are further evidence of DOD's commitment to improving weapon systems cybersecurity.

Greater Access to Cyber Expertise

DOD continues to face long-term challenges developing cybersecurity expertise within its acquisition workforce and supporting roles. For example, DOD's Office of the Director, Operational Test and Evaluation's 2019 Annual Report states that there is a widening gap in capabilities between DOD's cyber test teams and nation-state threats. The report further states that closing that gap will require a significant investment of resources. Several DOD officials within Office of the Secretary of Defense-level organizations told us that there are still concerns with whether staff with the appropriate skills are sufficiently involved in key acquisition activities. For example, a senior official involved in developmental testing for cybersecurity said acquisition programs struggle to integrate experts with cybersecurity test engineering skills early in the design process, which would help improve test quality.

Officials from all five weapon system programs we met with said that they had adequate access to cybersecurity expertise despite some challenges hiring and retaining cybersecurity personnel. In 2018, we found that officials identified challenges hiring and retaining people with the necessary cybersecurity skills.[23] Although officials in this review noted some ongoing challenges with hiring and retention, all five programs told us that they were able to fill their cybersecurity positions. Specifically, each program reported having access to an information system security manager and four of the programs reported also having information system security officers. While specific responsibilities may vary across programs, the information system security manager is generally responsible for managing the cybersecurity authorization process for a system and maintaining the cybersecurity program; an information system security officer reports to the information system security manager.

Increased Use of Cyber Assessments

We and DOD have reported in the past on the lack and insufficiency of weapon systems cybersecurity assessments. In particular, we found in October 2018 that the lack of testing meant that programs identified basic cybersecurity problems late in the development process when they were more difficult and costly to fix.[24]

All of the programs we met with reported that they had conducted or planned to conduct some level of cybersecurity assessment throughout the acquisition process, including developmental and operational

[23] GAO-19-128.

[24] GAO-19-128.

testing.[25] Programs reported that their assessments included, or will include, adversarial assessments, where independent testers attempt to find vulnerabilities in the system, as well as cooperative vulnerability and penetration assessments, an examination of the system to identify all significant vulnerabilities and the risk of exploitation of those vulnerabilities. When we met with them in March 2020, officials from one program reported having done two adversarial assessments and two cooperative vulnerability assessments within the last year. Officials from that program reported making a design change due to cyber assessment results. The increased use of cybersecurity assessments is a positive development and may help programs identify vulnerabilities earlier; however, the existence of the assessments alone does not guarantee better outcomes.[26] For example, we previously found that in some systems, the same vulnerabilities were found in multiple rounds of testing, and had gone unaddressed after they were first discovered.[27]

In addition to cyber expertise and cyber assessments, DOD and military service officials representing a range of component organizations described department-wide progress in two areas: improved guidance for cybersecurity and RMF, and better tailoring of security controls to acquisition programs.

Better Tailoring of Security Controls

Service officials reported that the services have made progress tailoring RMF security controls to similar types of systems. Acquisition program officials we spoke to said selecting controls, the second step of RMF, could be a difficult process because of the sometimes large volume of potential controls and complexity of applying them to various systems. The baseline set of controls of about 300 to 500 described above is just a

[25] According to DOD guidance, developmental testing should include ongoing contractor and government cybersecurity assessments to evaluate the system's performance in the presence of cybersecurity threats and to inform decision makers on the system's ability to meet cybersecurity requirements, among other things. Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, Version 2.0, Change 1 (Washington, D.C.: February 10, 2020). DOD guidance states that operational testing must incorporate cybersecurity through formal test events, leading to threat-representative cyberattacks against personnel trained and equipped with a system. Department of Defense, Director, Operational Test & Evaluation Memorandum, *Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs* (April 3, 2018).

[26] In 2020, we found greater variance in the use of cybersecurity assessments among major defense acquisition programs. Specifically, 14 of the 42 programs included in our annual assessment of defense acquisition programs had not completed any cybersecurity assessments. See GAO-20-439.

[27] GAO-19-128.

starting point, so programs may need to add or remove controls depending on their specific needs. In response to that challenge, organizations within DOD have begun developing control “overlays” to help programs tailor controls for their system. Overlays are a specialized set of adjustments to the baseline that can be applied to acquisition programs for similar types of systems. Officials from multiple acquisition programs told us that more tailored overlays would help streamline the process of determining and justifying whether a control is or is not applicable to their system.

We found several instances where overlays are being developed to help programs more easily identify applicable security controls. For example, a DOD CIO official with responsibility for advising acquisition programs on RMF implementation said his office had been working with stakeholders to develop an overlay for tactical radios, which could be applied to future programs developing tactical radios. The official also said that DOD CIO officials supported development of another overlay for nuclear command, control, and communications systems. In another case, officials from one acquisition program told us that the Army was working to develop an overlay for munitions. Like the other efforts described here, the overlays are tools program officials can use to help ensure the appropriate security controls are applied to systems in development, but more time and experience will determine how effectively overlays streamline the control selection process. Further, while overlays may help acquisition program offices select appropriate controls, they do not necessarily help with the challenge of effectively implementing security controls. As we reported in 2018, acquisition programs often had cybersecurity vulnerabilities stemming from poor implementation of security controls.[28]

New and Revised Cybersecurity Guidance

DOD and each of the services has released detailed policies or guidance implementing RMF. While DOD policies broadly define weapon systems acquisition practices and objectives for cybersecurity, the services have a role in developing and issuing complementary guidance, as needed, for implementation within their service acquisition community. For example, a DOD CIO official involved in developing and updating RMF policies and guidance said the department should not prescribe exactly how the services implement RMF or include cybersecurity requirements in contracts; instead, the services should adapt the policies and guidance to their needs and existing processes.

[28] GAO-19-128.

- The Navy issued an RMF process guide in December 2016 with service-specific guidance for acquisition programs on executing RMF.
- The Air Force issued RMF implementing guidance in February 2017, including guidance requiring programs to ensure all security controls are translated into security requirements through systems security engineering.
- The Marine Corps developed guidance on implementing RMF in July 2017 that included an overview of the RMF process.
- Finally, the Army issued guidance implementing RMF in April 2019, which included roles and responsibilities.

The timing of service level guidance is significant because officials from three of the five programs we reviewed reported implementing RMF only after receiving the service level instructions and guidance. For example, the two Army programs began implementing RMF within a couple of months of when the Army issued its RMF guidance. The additional guidance has had an important impact on programs' ability to include cybersecurity requirements in contracts, but much of it was developed years after the start of RMF, and some programs applied the process retroactively. For example, officials for one program said they had already selected all controls for their program before implementing RMF and determining a risk category for the program, the first step of RMF that is meant to inform control selection.

In addition, some DOD components have developed guidance that covers RMF as well as other specific elements of cybersecurity. For example, DOD has guidance that includes example language for contracts to ensure contractors complete adequate cybersecurity testing.[29] The guidance states that if a specific requirement is not in the contract, a program cannot expect the contractor to complete that testing requirement. Further, DOD developed a cybersecurity guidebook for program managers in 2015.[30] This guidance lays out how cybersecurity fits into the overall acquisition process. For example, the guidebook emphasizes the importance of incorporating cybersecurity into the development process early through the statement of work or the request for proposal. The guidance also emphasizes that following RMF alone

[29] Department of Defense, *Cybersecurity Test and Evaluation Guidebook,* Version 2.0, Change 1 (Washington, D.C.: February 10, 2020).

[30] Department of Defense, *DOD Program Manager's Guidebook*.

does not ensure that a system is cyber resilient, as that can only be verified through testing and evaluation.

Selected Programs Struggled to Include Cybersecurity in Contracts, and Most Service Guidance Does Not Address How to Include Cybersecurity Requirements in Contracts

Although it has taken promising steps, DOD still has challenges to overcome in order to improve weapon systems cybersecurity. In particular, DOD is still learning how to contract for cybersecurity in weapon systems, and selected programs we reviewed have struggled to incorporate systems' cybersecurity requirements into contracts. In addition, DOD and contractor officials told us that contracting for cybersecurity requirements is a general challenge. While DOD and the services have since made progress developing guidance related to RMF and weapon systems cybersecurity, there is limited guidance on how to include cybersecurity requirements in contracts.

Selected Acquisition Program Contracts Do Not Always Include Cybersecurity Requirements, Acceptance Criteria, and Verification Processes

The acquisition programs we reviewed omitted cybersecurity requirements from contracts or did not clearly define cybersecurity requirements in their contracts. The government is less likely to get what it wants if it omits all or part of its cybersecurity requirements. As discussed earlier, DOD guidance states that cybersecurity requirements should be treated like other types of system requirements. Acquisition contracts should define requirements to the extent necessary to satisfy the needs of the agency, identify criteria for accepting or rejecting the work, and where applicable, establish how the government will verify that requirements have been met. The contracts for weapon systems we reviewed did not always include these cybersecurity elements, and DOD and contractor officials cited additional examples. Importantly, each of the acquisition programs we reviewed awarded their initial contracts in 2015 and 2016, which is after DOD issued its RMF policy in 2014 but before the military services issued detailed policies or guidance on incorporating RMF. The contract awards also preceded DOD's 2017 addition of a cybersecurity enclosure to its key acquisition instruction.

Selected Systems' Cybersecurity Requirements Were Not Always Included in Contracts

Three of the five weapon system contracts we reviewed had no cybersecurity requirements when they were awarded and we could not assess the completeness of two contracts' cybersecurity requirements.[31] For example, one of the programs had a cybersecurity strategy that identified the RMF categorization and described how the program would select security controls. However, when the contract was awarded, it did not include cybersecurity requirements in the statement of work, the system specification, or the contract deliverables.

Three of the five contracts we reviewed were modified after they were awarded to add cybersecurity requirements. One of the contracts included detailed cybersecurity requirements. However, the other two contracts included generic statements indicating the system should be developed consistent with DOD cybersecurity policies. Contractors we spoke to said it is common for requests for proposals to include generic statements regarding cybersecurity, such as, "be cyber resilient," or, "comply with RMF." The contractors said such statements do not provide enough information to determine what the government wants or how to design a system.

In contrast to cyber requirements, other types of system requirements contained significantly more detail. For example, one contract we reviewed specified the amount of vibration that the system had to withstand when being transported by air, land, and sea, including separate requirements when transported on aircraft with jet engines and propellers. It also included non-cybersecurity requirements related to dust, sand, fungus, and many other aspects of the system's design and performance. Another contract we reviewed specified general requirements like the system should not have any sharp edges that could injure personnel. Neither of these contracts, however, included detailed cybersecurity requirements.

Selected Contracts Do Not Identify Acceptance Criteria

The weapon system contracts we reviewed did not, at the time of award, define cybersecurity activities in objective terms with a clear basis for accepting or rejecting the system. If a vehicle is required to travel at least 60 miles per hour and it only reaches 55 miles an hour, the contractor has not met the requirement. Only one of the contracts we reviewed included detailed cybersecurity requirements and the requirements generally

[31] We did not assess cybersecurity contract requirements for two programs. One program included cybersecurity requirements, but we did not fully assess them because they were included in a classified document. We did not assess the contract for the other program due to the limited scope of the initial contract. The program used a phased approach so the initial design did not include all requirements. The contract had a mechanism for adding or changing requirements once the initial design was complete.

identified specific security controls that the system had to have rather than performance-based requirements. Officials from one program office said they attempted to use performance-based requirements, but could not agree to terms with the contractor. DOD and contractor officials said that many contract requirements focus on cybersecurity controls the system must have as opposed to desired outcomes such as preventing unauthorized users from accessing the system. However, as we have previously reported, the application of controls does not mean that a system is secure.[32] Controls must be implemented correctly and then tested for effectiveness.

Selected Contracts Do Not Establish How Cybersecurity Requirements Will be Verified

Among the contracts for the five selected programs, we did not see any examples identifying how program officials would verify cybersecurity requirements in the contracts at the time of award. DOD guidance and officials emphasized the importance of establishing criteria for measuring contractors' performance. Defining objective criteria ensures that cybersecurity requirements are unambiguous and provides a mechanism for determining whether the contractor met the requirement. For other system requirements, the contracts we reviewed generally identified performance-based requirements and how the government would verify that that those requirements had been met. For example, one contract we reviewed specified fuel efficiency requirements and then described the types of terrain and how fast the system would be going during tests. We did not see verification details specified for cybersecurity requirements. However, as noted above, only one contract we reviewed included detailed cybersecurity requirements.

Service Officials Cited Cybersecurity Requirements as a General Challenge

Several DOD and military service officials generally agreed that effectively contracting for cybersecurity is a challenge for acquisition programs. A senior DOD official said standardizing cybersecurity requirements is difficult and the department needs to better communicate cybersecurity requirements and systems engineering to the users that will decide whether or not a cybersecurity risk is acceptable. Another senior DOD official said the lack of clear performance criteria for cybersecurity requirements creates challenges for understanding and implementing better security. Navy officials cited an example of a program executive office levying a thorough and detailed list of cybersecurity requirements in a contract but said that was an exception within the service.

[32] GAO-19-128.

Most Service Guidance Does Not Address Contracting for Cybersecurity Requirements, Acceptance Criteria, and Verification Processes

Current military service guidance, except for the Air Force, does not address how acquisition programs should contract for weapon systems cybersecurity requirements, acceptance criteria, and verification, which DOD and program officials told GAO would be helpful. As noted above, the services developed a range of implementing guidance for RMF since DOD established the policy in 2014; however, including cybersecurity requirements in contracts is a key area where military service guidance continues to be generally missing or incomplete.

Army Policies and Guidance Do Not Reflect How to Include Cybersecurity Requirements in Contracts

The Army's policies and guidance discuss, at a high level, the need for cybersecurity requirements, but do not detail how acquisition programs should include cybersecurity requirements in contracts. The policies and guidance emphasize the need for RMF security controls and cybersecurity requirements in acquisition programs, consistent with DOD policies and guidance. However, the policies and guidance do not detail how acquisition programs should incorporate cybersecurity requirements, acceptance criteria, and verification into contracts. Army regulation, updated with major revisions in 2019, directs senior leaders to integrate cybersecurity in acquisitions and to ensure that contracts include specific requirements to provide cybersecurity for Army IT, including weapon systems.[33] However, the regulation provides no further detail on how to do so. Similarly, the Army's guidance on implementing RMF states that cybersecurity will be addressed in the requirements development phase of acquisition and that cybersecurity requirements should be treated like other system requirements. However, the guidance does not address how RMF should be incorporated into contracts.

In 2019, the Army also issued new guidance for acquisition programs' cybersecurity strategies, which help organize an acquisition program's activities to achieve cybersecurity requirements. Among other things, the guidance specifies content for a program's cybersecurity strategy, such as descriptions of cybersecurity requirements and plans for incorporating those requirement in contracts, but does not describe how acquisition programs should develop that content.

[33] Department of the Army, Headquarters, *Information Management: Army Cybersecurity*, Army Regulation 25-2 (Washington, D.C.: April 4, 2019).

Navy Policies and Guidance Do Not Reflect How to Include Cybersecurity Requirements in Contracts

The Navy's policies and guidance emphasize the need for cybersecurity to be integrated into the weapon systems acquisition process, but do not specify how to incorporate cybersecurity requirements in contracts. The Navy's policy governing acquisition program cybersecurity states that the Navy's implementation of RMF provides a construct to, among other things, ensure that cybersecurity is an integral part of the systems engineering process for Navy IT, which includes weapon systems acquisitions.[34] However, the policy and related guidance does not address how acquisition program staff are to incorporate cybersecurity requirements or security controls in contracts. The policy tasks program executive offices with responsibility for ensuring that, among other things, cybersecurity is a key element of program protection planning activities. Senior Navy officials said that DOD guidance on cyber survivability helps establish program requirements that inform system specifications, analysis, and the contractor's proposed solution. However, as discussed above, the challenge acquisition programs confront is distilling top-level requirements into system-specific performance requirements and specifications within contracts.

At the same time, however, Naval Air Systems Command (NAVAIR), which oversees five Navy program executive offices responsible for naval aviation programs, has developed guidance and templates to help acquisition programs better communicate their cybersecurity and RMF requirements to contractors. For example, NAVAIR developed standard contract language and associated processes to inform an acquisition program's statement of work that, among other things, would require a cybersecurity kick-off meeting involving government and contractor cybersecurity teams shortly after contract award. This meeting, as described in the standard contract language, is intended to complete the first two steps of RMF, categorization and control selection. A senior NAVAIR official involved in developing the guidance said the kick-off meeting helps secure agreement between the program office and the contractor on the list of applicable controls and on responsibility for control implementation, whether with the government or the contractor.

NAVAIR's statement of work standard also requires that a contractor deliver a cybersecurity strategy implementation plan shortly after contract award, detailing how the contractor will achieve the goals outlined in the programs' cybersecurity strategy. The NAVAIR official said

[34] Department of the Navy, Office of the Chief of Naval Operations, *U.S. Navy Cybersecurity Program*, OPNAVINST 5239.1D (Washington, D.C.: July 18, 2018).

implementation plans are a standardized, yet flexible, way for the government and the contractor to agree on an approach to cybersecurity that can be adjusted over time. The official also said that the guidance is directed toward cybersecurity staff assigned to acquisition programs, such as information systems security officers, who typically do not have contracting experience or training. NAVAIR's structured process for communicating with contractors through the cybersecurity kick-off meeting and the cybersecurity strategy implementation plan helps ensure a common understanding of the program's needs. The NAVAIR official said that while the guidance and templates could be tailored to other types of programs, the guidance is currently only promoted among NAVAIR programs. Broader adoption of these or similar practices across Navy acquisitions could help improve integration of cybersecurity in Navy weapon systems acquisitions.

Marine Corps Policies and Guidance Do Not Reflect How to Include Cybersecurity Requirements in Contracts

Similar to the Army and Navy, Marine Corps policy on cybersecurity and RMF implementation does not specify how to incorporate cybersecurity requirements in contracts.[35] The policy directs acquisition program managers and supporting staff to ensure that cybersecurity requirements are identified and that cybersecurity is integrated into the system design, development, integration, and implementation. The policy also states that RMF security controls function as security requirements and should be refined through systems engineering. However, the policy does not address how either cybersecurity requirements or RMF security controls should be incorporated into contracts. A senior Marine Corps official said that contracting is critical to effective cybersecurity and that, despite its efforts to date, this is one area where the Marine Corps acquisition community has room to improve.

Air Force Has Developed Guidance on Including Cybersecurity Requirements in Contracts

The Air Force has recently issued service-wide guidance specific to contracting for cybersecurity, in part by leveraging existing departmental policies and guidance. While the Air Force's policy for implementing RMF emphasizes the importance of using systems engineering to incorporate RMF security controls into system requirements and related documentation, it does not provide further detail on how these requirements should be incorporated in contracts.[36] However, In 2019,

[35] Department of the Navy, Headquarters Marine Corps, Deputy Commandant for Information (DC I) Command, Control, Communications, and Computers (C4), *United States Marine Corps Enterprise Cybersecurity Manual: 018 Marine Corps Assessment and Authorization Process (MCAAP)*, USMC ESCM 018 Version 6 (June 4, 2020).

[36] Department of the Air Force, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, AFI 17-101 (February 6, 2020).

the Air Force's Cyber Resiliency Office for Weapons Systems (CROWS) developed the Air Force Weapon System Program Protection and Systems Security Engineering Guidebook (hereafter, the CROWS Guidebook). The CROWS Guidebook consolidates references to different DOD and Air Force instructions and guidance into a single document but also provides more detailed explanations and suggestions for implementation. The other military services would benefit from a similar approach. Among other things, the CROWS Guidebook provides sample language that programs could include in their requests for proposals, statements of work, and other contract documents. For example, the guidance states that programs' statements of work should require contractors to use modeling and simulation to verify specifications and should ensure that the government has the opportunity to participate in all testing. It also provides a work breakdown structure for the program office to use in effectively managing cybersecurity and related systems engineering activities. Following the work breakdown structure, each activity has a description, how the activity is documented, and references to DOD, Air Force, and other instructions related to the activity. The CROWS Guidebook also encourages programs to tailor the approaches identified in the guidebook to their specific needs.

CROWS reissued its guidebook in March 2020 to include additional details and references on several topics, including a sample program protection plan template and a table mapping the RMF steps to the activities in the CROWS Guidebook's work breakdown structure. The update also reflected comments from industry representatives. An Air Force official assigned to the CROWS office said that it is necessary to incorporate cybersecurity and cyber resiliency, including RMF, into the systems engineering process. If not, the official said, cybersecurity and cyber resiliency will not be incorporated into requirements or put on contract, putting the program manager in the difficult position of trying to apply cybersecurity after the system design has been put under contract.

Conclusions

Since our 2018 report, DOD has made progress incorporating cybersecurity into the acquisition process. At the macro level, additional cybersecurity guidance and resources have helped to further ingrain cybersecurity practices into the DOD culture. However, additional guidance has not addressed an area where we found programs struggled—how to effectively translate cybersecurity concepts into detailed and specific cybersecurity requirements for contracts, on par with other system requirements. In particular, the services' guidance on incorporating cybersecurity into acquisitions does not address the way programs should include cybersecurity requirements in contracts with clear acceptance criteria and methods to verify requirements have been met. The Air Force has taken positive actions to remedy this by developing internal guidance on how to incorporate program-specific cybersecurity requirements. The Army, Navy, and Marine Corps would benefit from a similar approach. Just as the Air Force leveraged and consolidated existing policies and guidance, the Army, Navy, and Marine Corps have opportunities to adapt existing practices, such as those in the Air Force, to fit their respective acquisition community. Until these actions are taken, programs will continue to face cybersecurity risks and contracts may not include detailed and specific cybersecurity requirements.

Recommendations for Executive Action

We are making a total of three recommendations, including one to the Army and two to the Navy. Specifically:

The Secretary of the Army should develop guidance for acquisition programs on how to incorporate tailored weapon systems cybersecurity requirements, acceptance criteria, and verification processes into contracts. (Recommendation 1)

The Secretary of the Navy should develop guidance for acquisition programs on how to incorporate tailored weapon systems cybersecurity requirements, acceptance criteria, and verification processes into contracts. (Recommendation 2)

The Secretary of the Navy should take steps to ensure the Marine Corps develops guidance for acquisition programs on how to incorporate tailored weapon systems cybersecurity requirements, acceptance criteria, and verification processes into contracts. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this product to DOD for comment. In its comments, reproduced in appendix II, DOD concurred with our recommendations to the Army and Navy and partially concurred with our recommendation focused on the Marine Corps. In its partial concurrence, DOD did not disagree with the substance of our recommendation, and stated that our separate recommendations to the Marine Corps and Navy should be merged because those components operate under the same acquisition construct. While we recognize that fact, and addressed both recommendations to the Secretary of the Navy, we determined that separate recommendations to each component were appropriate because each maintains independent policies and guidance relevant to weapon systems cybersecurity. DOD also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Acting Secretaries of the Army and Navy, and the Commandant of the Marine Corps. 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 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 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
Chairwoman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

To address both objectives, we reviewed DOD and service level policies and guidance related to the implementation of cybersecurity for weapon systems in development.[1] DOD policies and guidance included DOD Instruction 8500.01, Cybersecurity; DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT); DOD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System; DOD Instruction 5000.02, Operation of the Defense Acquisition System; DOD Instruction 5000.82, Acquisition of Information Technology; DOD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework into the System Acquisition Lifecycle; DOD Cybersecurity Test and Evaluation Guidebook; the Joint Capabilities Integration and Development System Manual; the Cyber Survivability Endorsement Implementation Guide; the Defense Acquisition Guidebook; the Cybersecurity Strategy Outline and Guidance; and DOD handbooks on contracting activities.

Service level guidance included Army Regulation 25-1, Army Information Technology; Army Regulation 25-2, Army Cybersecurity; Army Pamphlet 25-1-1, Army Information Technology Implementation Instructions; Army Pamphlet 25-2-11, Cybersecurity Strategy for Programs of Record; Army Pamphlet 25-2-14, Risk Management Framework for Army Information Technology; OPNAV Instruction 5239.1D, U.S. Navy Cybersecurity Program; SECNAV Instruction 5239.3c, Department of the Navy Cybersecurity Policy; Navy Risk Management Framework Process Guide; Air Force Instruction 17-101, Risk Management Framework for Air Force Information Technology; Air Force Instruction 17-130, Cybersecurity Program Management; the Weapon System Program Protection and Systems Security Engineering Guidebook; and the United States Marine Corps Enterprise Cybersecurity Manual, 018 Marine Corps Assessment and Authorization Process (MCAAP).

We also conducted interviews with officials from multiple DOD organizations and components with responsibility for cybersecurity of weapon systems acquisitions including from the following organizations:

- Office of the Secretary of Defense organizations: Office of the Director, Operational Test and Evaluation; Office of the Chief Information Officer; Office of the Chairman of the Joint Chiefs of Staff; Office of the Under Secretary of Defense (Acquisition and Sustainment); Office of the Under Secretary of Defense (Research

[1] GAO-19-128.

and Engineering), including the Joint Federated Assurance Center; and the Defense Digital Service.

- Selected program offices reflecting a purposeful sample of five major defense acquisition programs. We identified five weapon system programs from the Army, Navy, and Marine Corps.[2] The programs we selected are developing different types of systems: a radar, an anti-jammer, a ship, a ground vehicle, and a missile. To select these programs, we initially identified major defense acquisition programs that conducted the Milestone B decision—the point where the program is normally approved to begin development—during or after 2014 because those programs had the potential to be subject to the risk management framework (RMF) process for incorporating cybersecurity into systems.[3] We then applied both programmatic and practical selection factors to create a sufficiently diverse sample. Programmatic selection factors included system type, contractor, and program schedule. Practical selection factors included the locations of the program office and the contractor's facility. For each program, we interviewed acquisition and contracting officials to understand how they integrated and managed cybersecurity throughout development, and we reviewed relevant acquisition and contract documentation for each program. The examples we cite are unique to each weapon system and are not applicable to all weapon systems.
- Selected organizations with cybersecurity expertise based on their research or roles advising DOD on weapon systems cybersecurity related topics, including the RAND Corporation and Sandia National Laboratory.
- Ten defense contractors, 10 legal or consultant organizations, and two defense industry trade groups.

Although the results of our review of selected programs, organizations with cybersecurity expertise, contractors, and industry organizations are not generalizable to all programs, organizations, or contractors, they are designed to reflect the experiences and perspectives of programs from across the services and a range of organizations and contractors.

[2] Although we initially selected Air Force programs for review, we were not able to include those programs in our scope primarily as a result of restrictions to classified information resulting from the Coronavirus Disease 2019 pandemic.

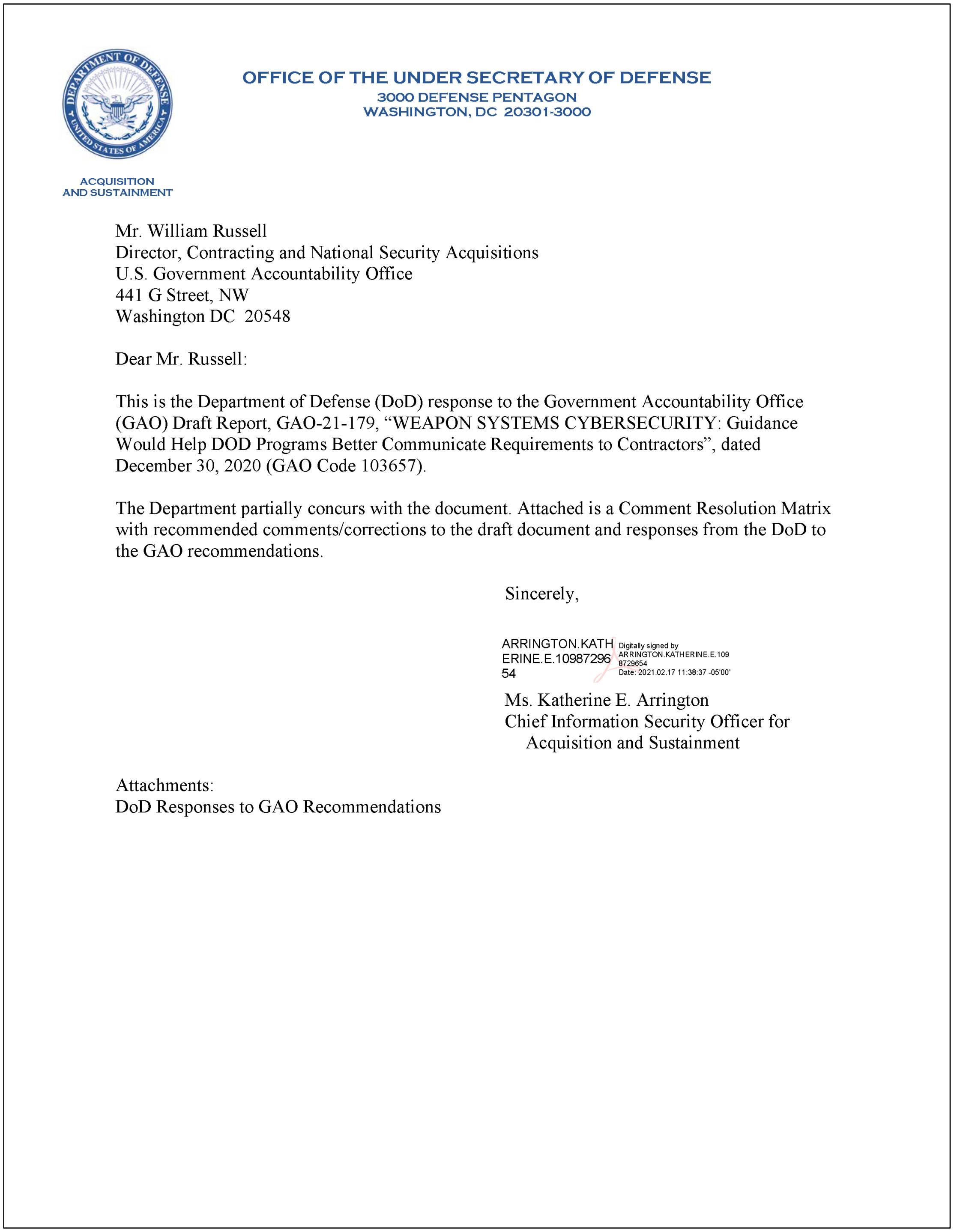
[3] Major defense acquisition programs are generally programs designated by the Secretary of Defense as such or that are estimated to require eventual total expenditure for research, development, test, and evaluation of more than $480 million, or for procurement of more than $2.79 billion, in fiscal year 2014 constant dollars.

The focus of this report is contracting for weapon systems cybersecurity. For that reason, we did not look in-depth at related issues, such as mission level analyses of cybersecurity vulnerabilities, alignment of cybersecurity activities to acquisition milestones, or the effectiveness of testing procedures.

In March 2020, during the course of this engagement, the President declared a national state of emergency as a result of the spread of the Coronavirus Disease 2019. Like other federal agencies, GAO implemented changes to curb the spread of the virus. Accordingly, we reduced the scope of our work so that our analysis did not depend on access to systems we use to store and process classified information sources. We plan to include these sources in future work.

We conducted this performance audit from July 2019 to March 2021 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: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

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-21-179, "WEAPON SYSTEMS CYBERSECURITY: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors", dated December 30, 2020 (GAO Code 103657).

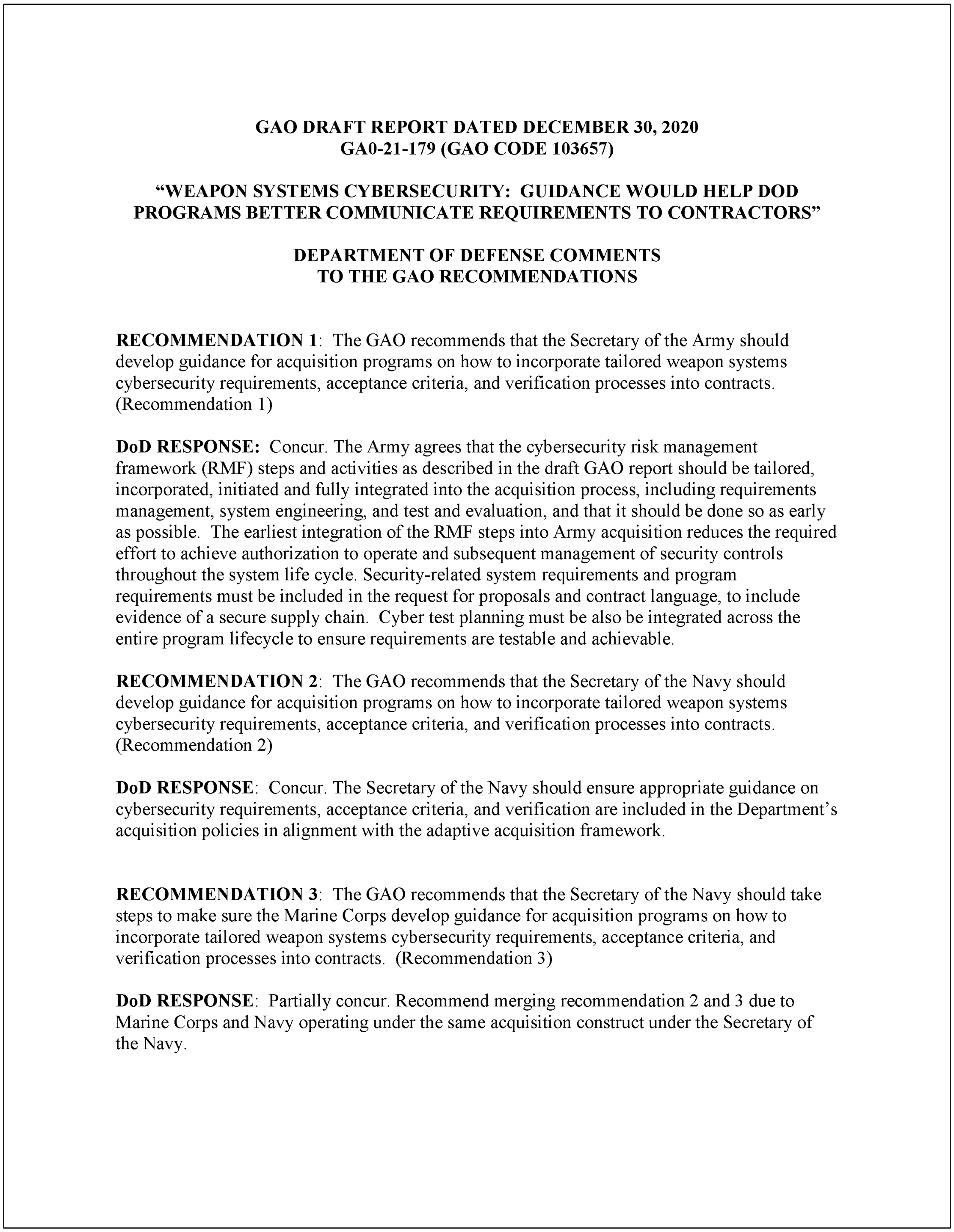
The Department partially concurs with the document. Attached is a Comment Resolution Matrix with recommended comments/corrections to the draft document and responses from the DoD to the GAO recommendations.

Sincerely,

ARRINGTON.KATHERINE.E.1098729654 Digitally signed by ARRINGTON.KATHERINE.E.1098729654 Date: 2021.02.17 11:38:37 -05'00'

Ms. Katherine E. Arrington
Chief Information Security Officer for
Acquisition and Sustainment

Attachments:
DoD Responses to GAO Recommendations



GAO DRAFT REPORT DATED DECEMBER 30, 2020
GA0-21-179 (GAO CODE 103657)

"WEAPON SYSTEMS CYBERSECURITY: GUIDANCE WOULD HELP DOD PROGRAMS BETTER COMMUNICATE REQUIREMENTS TO CONTRACTORS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of the Army should develop guidance for acquisition programs on how to incorporate tailored weapon systems cybersecurity requirements, acceptance criteria, and verification processes into contracts. (Recommendation 1)

DoD RESPONSE: Concur. The Army agrees that the cybersecurity risk management framework (RMF) steps and activities as described in the draft GAO report should be tailored, incorporated, initiated and fully integrated into the acquisition process, including requirements management, system engineering, and test and evaluation, and that it should be done so as early as possible. The earliest integration of the RMF steps into Army acquisition reduces the required effort to achieve authorization to operate and subsequent management of security controls throughout the system life cycle. Security-related system requirements and program requirements must be included in the request for proposals and contract language, to include evidence of a secure supply chain. Cyber test planning must be also be integrated across the entire program lifecycle to ensure requirements are testable and achievable.

RECOMMENDATION 2: The GAO recommends that the Secretary of the Navy should develop guidance for acquisition programs on how to incorporate tailored weapon systems cybersecurity requirements, acceptance criteria, and verification processes into contracts. (Recommendation 2)

DoD RESPONSE: Concur. The Secretary of the Navy should ensure appropriate guidance on cybersecurity requirements, acceptance criteria, and verification are included in the Department's acquisition policies in alignment with the adaptive acquisition framework.

RECOMMENDATION 3: The GAO recommends that the Secretary of the Navy should take steps to make sure the Marine Corps develop guidance for acquisition programs on how to incorporate tailored weapon systems cybersecurity requirements, acceptance criteria, and verification processes into contracts. (Recommendation 3)

DoD RESPONSE: Partially concur. Recommend merging recommendation 2 and 3 due to Marine Corps and Navy operating under the same acquisition construct under the Secretary of the Navy.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Raj Chitikila (Assistant Director), Andrew Berglund (Analyst-in-Charge), Brandon Booth, Mary Diop, Lori Fields, Laura Greifner, and Anne Louise Taylor 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