HSOAC | HOMELAND SECURITY OPERATIONAL ANALYSIS CENTER
An FFRDC operated by the RAND Corporation under contract with DHS

Research Report

CHAD HEITZENRATER, JAMES DIMAROGONAS, KYLE BUNCH, FRANK CAMM, RYAN CONSAUL, SARAH W. DENTON, QUENTIN E. HODGSON, ERIN N. LEIDY, LAURINDA L. ROHN, JAMES RYSEFF, YULIYA SHOKH, PADMAJA VEDULA

Government Acquisition of Cyber Technologies

Lessons Derived from Analysis of the Cybersecurity and Infrastructure Security Agency's Cyber Acquisition Processes

Effective and efficient cyber acquisition has proven to be a challenge for government organizations, including the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security (DHS). With respect to cybersecurity, CISA has a mandate to act in two roles: as national coordinator for critical infrastructure security and resilience and as the country's cyber defense agency.[1] In these roles, CISA acquires equipment and services to support numerous capabilities and must be able to plan, develop, execute, and deploy these capabilities expeditiously, driving down costs and schedule timelines while increasing technical performance for mission operators.

Like most organizations, CISA approaches acquisition by seeking to understand the requesting organization's needs, including resilience, and manage risks. (See the box on the next page for information on CISA's acquisition approach.) However, the current DHS acquisition approach has not provided CISA the ability to acquire technology rapidly enough while balancing risk tolerance. This is partly because of the complexity of the acquisition process itself and partly because of a lack of a shared understanding of how to tailor the process for different types of acquisitions.

Although DHS has adapted many U.S. Department of Defense (DoD) processes for its own use, more can be

KEY FINDINGS

- A successful approach to cyber acquisition must be rooted in solid acquisition practice.
- Flexibility is important to meet varied cyber acquisition needs.
- Requirements are foundational but are challenging to formulate.
- The cyber acquisition approach must be considered in relation to the goals.
- Background and expertise of staff play a key role in cyber acquisition.

CISA's Acquisition Approach

Acquisition of capabilities within CISA is governed by a series of policy directives, including DHS Directive 102-01[a] and DHS Instruction 102-01-001,[b] which establishes the ALF. The ALF seeks to ensure consistent and efficient acquisition management, support, review, and approval throughout DHS by linking requirements, resourcing, and other processes (such as systems engineering and enterprise architecture) in a four-phase process, through which each program must progress to deliver and field a new product or capability.[c] The existing process was heavily influenced by the DoD Joint Capabilities Integration and Development System process,[d] which itself has recently been tailored into the AAF to increase responsiveness and flexibility.

NOTE: AAF = Adaptive Acquisition Framework; ALF = Acquisition Lifecycle Framework.

[a] DHS, "Acquisition Management Directive."

[b] DHS, "Acquisition Management Instruction."

[c] DHS, "Acquisition Management Instruction," pp. 3–4. The four phases are (1) need; (2) analyze and select; (3) obtain; and (4) produce, deploy, support, and dispose. Five acquisition decision events are embedded in the ALF. These provide the acquisition decision authority an opportunity to assess whether a program meets certain requirements and is ready to proceed through the life-cycle phases. For additional information, see DHS, "Acquisition Management Instruction," pp. 39–49.

[d] Chairman of the Joint Chiefs of Staff, "Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System."

[e] For an overview of the AAF, see Defense Acquisition University, "Adaptive Acquisition Framework."

done to enable DHS and CISA to acquire technology rapidly while balancing risk tolerance. With initiatives currently underway across the government to improve cyber acquisition, we feel that the implications of these efforts can inform a broader discussion around the principles that underlie government cyber acquisition.

In support of these efforts, analysts from the Homeland Security Operational Analysis Center, a federally funded research and development center operated by the RAND Corporation, examined how different initiatives can support speed and flexibility in acquisition while maintaining an appropriate level of rigor based on the acquisition complexity. We explored approaches used in other departments and agencies to create a more flexible acquisition process and identified opportunities to gain efficacies and reduce timelines in the execution of acquisition programs of record, driving toward a more proactive acquisition environment. We also identified contributions and research insights on improving and streamlining cyber acquisition and considered portfolio-based approaches to managing programs of record.

This report captures our recommendations based on this research to make them available to a wider audience. This audience might include those interested in improving cyber acquisitions within CISA and DHS, as well as leaders and acquisition personnel in other organizations who might face similar issues and are looking for examples on which to base their own cyber acquisition improvement efforts.

Principles to Support the Acquisition of Cyber Technologies

In the course of our research, we identified several overarching insights and critical constraints that can help frame the discussion and provide contextual background to inform the recommendations provided in the next section:

- **A successful approach to cyber acquisition must be built on solid acquisition practice.** Although there are certainly cyber-specific acquisition challenges, many common cyber acquisition challenges are independent of the acquisition target. Executing acquisition processes effectively is key to cyber acquisition.
- **Flexibility is important for meeting varied cyber acquisition needs.** A single organization might seek to engage in multiple forms of cyber acquisition. For example, in CISA, there is interest in employing CISA-driven system design and development in addition to current efforts focused on procurement and integration of commercial, off-the-shelf capabilities or contracting out development. The different timelines, requirements, and expertise

needed for each of these activities underscores the need for multiple approaches to meeting acquisition needs.

- **Requirements are foundational but are challenging to formulate.** We found that many challenges with CISA's cyber acquisition process can be traced to the formation of requirements, which numerous stakeholders during interviews identified. This challenge serves as a foundational source of issues that are carried forward and pervade the process.
- **The cyber acquisition approach must be considered in relation to the goal.** Cyber technology is not a singular capability or outcome. Therefore, it is important that the goals for cyber acquisition be well defined and communicated to all stakeholders and that progress be measured and reported. A lack of shared understanding of outcomes and approaches across stakeholders, combined with the absence of measurements to confirm progress toward the agreed-on outcomes, can lead to delays and inefficiencies. Misalignment between the acquisition approach and desired outcomes can exacerbate acquisition challenges because changes in the threat environment or technology affect different programs and goals unequally. Organizations can use existing standards and frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework,[2] to guide their efforts to define, communicate, and measure cyber acquisition goals.
- **Background and expertise of staff play a key role in cyber acquisition.** Although an agency with a mission as broad as CISA's certainly benefits from diversity of staff, staff require a common understanding of key processes in order to build a collaborative cyber acquisition environment and create a shared vision for how to improve. At CISA, for example, the background and expertise of staff vary widely, resulting in different levels of understanding of key processes. As a result, many prevailing beliefs about program operation or outcomes were not borne out by our research.

Approach

This research employed a mixed-method approach that incorporated multiple sources and perspectives. The main parts of the methodology were as follows:

- **Data collection.** As a first step in this research, we performed an extensive data-collection effort that included
  - interviews with personnel from DHS and DoD and other agency leadership and practitioners
  - a literature review that encompassed government, academic, and commercial literature and analysis
  - a review of DHS and related external acquisition processes, such as those processes employed by DoD and within government innovation units
- **Data processing and analysis.** Using the collected data, we undertook two phases of analysis:
  - In phase 1, we employed coding and analysis to identify thematic gaps, past actions, and future recommendations gleaned from the interviews. This same approach was then also applied to literature, policy, and process documents from the data-collection effort.
  - In phase 2, outputs from phase 1 were combined and validated, employing pattern-coding techniques to observe common groupings and trace linkages between concepts
- **Recommendation development.** Following the processing and analysis of data, we conducted a virtual team workshop for the purpose of brainstorming, developing, and validating the lessons to be derived from our research.

Recommendations

Improvements in the process of acquiring cyber technology must start by addressing fundamental process and personnel issues in addition to cybersecurity-specific issues. With the principles just described

serving as a backdrop, our research identified ten core recommendations across five categories:

- Recommendations in the **policy and pathways** category address the structure of the acquisition framework itself and the realization of a multipathway acquisition approach identified in the project description.
- **Portfolio and contract management** recommendations expand on the multipathway approach through lessons learned about acquisition portfolio management and contractual execution.
- Recommendations for **requirements definition** identify some of the difficulties in defining requirements that form the foundational basis for CISA's cyber acquisitions.
- **Communication and measurement** recommendations provide suggested practices for process element interaction and the evaluation of process results. Measurement and evaluation are essential to process improvement as part of each recommendation.
- **Oversight and workforce** recommendations target process quality, process evaluation and feedback, cybersecurity, and governmentwide issues of recruitment, retention, and training that we found throughout our research.

Although some recommendations are tightly coupled, they are individually implementable; however, they provide a greater benefit if they are implemented as a whole. The set of recommendations is listed in the table.

Policy and Pathways

Ensure That Existing Acquisition Policy Is Fully Implemented

Organizations trying to adopt new, improved, and streamlined acquisition processes must start with a good understanding of how these can be implemented in the context of existing processes and practices. As an example, for CISA, this would entail fully implementing existing policy options, such as the DHS rapid acquisition policy, which the DHS Deputy Under Secretary for Management issued in February 2020.[3] This policy was designed to streamline existing documentation processes and "enables rapid delivery of capabilities to the field."[4] The policy was created to enable a component to achieve a decision to enter the produce, deploy, sustain, and dispose phase within two years by consolidating documentation requirements and reducing the number of acquisition decision events to two.

DHS's lack of experience and components' perceived lack of awareness of the rapid acquisition process appear to be contributing to underutilization of the policy within DHS. For CISA, full utilization of this policy for programs that meet its criteria

Summary of Recommendations

Category	Recommendation
Policy and pathways	Ensure that existing acquisition policy is fully implemented.
	Establish tailored pathways for cyber acquisition using lessons from DoD's AAF.
Portfolio and contract management	Develop and implement portfolio-based management practices.
	Maximize the use of varied contract vehicles for well-defined program elements.
Requirements definition	Correct any existing issues with requirements development.
	To increase flexibility, change how requirements are developed.
Communication and measurement	Strive to improve program communication throughout a system's life cycle.
	Institute an acquisition measurement initiative that addresses every step in the acquisition process, from initiation to sustainment and across development, engineering, and operations.
Oversight and workforce	Focus on the integration of technical and program management.
	Develop strategies to recruit, grow, and retain technical acquisition management expertise.

and require rapid deployment could reduce time to achieve deployment and encourage a "cultural shift" to more agility in the acquisition process.

Establish Tailored Pathways for Cyber Acquisition, Using Lessons from the U.S. Department of Defense's Adaptive Acquisition Framework

It was a premise of this research effort that novel, adaptive processes might be required to increase the efficiency of acquisition for cyber and information technology (IT). DoD's development of the AAF has established a precedent for a "pathway" approach, allowing the process followed by each acquisition to be adapted to meet the needs of that type of acquisition.[5] For example, we identified three principal means by which CISA reported need or interest in acquiring cyber technologies and IT, now or in the future. We refer to these pathways by their primary mechanism: *buy* (purchase an existing capability), *build* (develop the capability in-house), and *outsource* (contract with another entity to develop the capability to CISA-provided specifications).

Although the results of DoD's efforts are still to be seen,[6] our research uncovered early evidence and a widespread belief that a pathway construct is central to the efficient delivery of modern capabilities. In our interviews with DoD program personnel, we observed tailoring of the AAF pathways based on the type, complexity, and size of the effort, basing the approach on needs and underlying constraints of the acquiring organization or agency. This included unique partnerships between research and development entities, program offices, agile development practices, and user collaboration.

Portfolio and Contract Management

Develop and Implement Portfolio-Based Management Practices

To accommodate a more flexible acquisition process, organizations should implement portfolio-based management. A portfolio-based approach "provides a global view on resources and their distribution across individual projects according to strategic choices."[7] This construct shifts focus to mission needs and allows funding allocations and requirements to be targeted with more flexibility. Measuring progress at a portfolio level can also better connect department policy goals through individual projects. The sponsor of this research and multiple interviewees stated that this approach was a best practice.[8]

For CISA, this resulted in a set of recommendations to realize a portfolio-based approach. Other organizations could consider using a similar approach:

- **Define and codify a structure for portfolio management having portfolios of projects that cover longer time periods and projects with shorter iterations.** The current ALF process, in which requirements are fixed for a long duration, is not conducive to speed or agility. Shortening program timelines under a broader portfolio construct will support more-general capability requirements at the portfolio level with more-frequent and more-responsive feedback cycles at the program level, promoting agility in program direction.
- **Ensure that portfolios and programs are effectively scoped and capability driven.** Reducing the scope of programs could more appropriately focus key acquisition policy documentation requirements and could push oversight down to component officials, allowing agility when mission demands require it.
- **Utilize portfolios as an opportunity to explore different approaches to acquisition, such as nontraditional development and deployment.** The rigid structure of traditional acquisition implies a single acquisition approach per program, which can be too cumbersome for cyber acquisition. Operating as a portfolio can enable multiple approaches applied in tandem.

These recommendations are indicative of the key elements of portfolio management identified elsewhere and represent important considerations when weighing flexibility with rigor across an organization's acquisition approach.

Maximize the Use of Varied Contract Vehicles for Well-Defined Program Elements

Cyber and IT acquisitions, which vary in complexity and nature (e.g., turnkey, bespoke), require flexible contracting vehicles and approaches. The current DHS contracting process is widely considered cumbersome and too lengthy, lacking sufficient flexibility to respond to emerging needs. This appears to especially be true for service contracts, which appear to be prevalent within CISA.[9] Having a mixture of contracting vehicles to match the full spectrum of cyber acquisition needs allows an appropriate response to different organizations' cyber demands.

Several existing contract vehicles might help with the mixed nature of cyber acquisition:

- **catalogue-based approaches**, such as the National Aeronautics and Space Administration's governmentwide acquisition contract approved by the Office of Management and Budget for use across the federal government[10]
- **other transaction authority**, which is defined by what it is not: an "agreement . . . that is not a procurement contract, grant, or cooperative agreement."[11] This authority is intended to carry out activities that do the following:

  > (1) Support basic, applied, and advanced research and development that would promote homeland security; (2) Advance the development, testing and evaluation, and deployment of critical homeland security technologies; (3) Accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.[12]

- **establishment of collaborative contract vehicles within and across programs and portfolios.** This could include the establishment of larger, more-flexible options with broad scope (e.g., indefinite-delivery, indefinite-quantity; the catalogue-based vehicles discussed above).

We recognize that utilizing a larger variety of contract vehicles could add complexity to the acquisition process. This shift might require both culture and organizational change in that current practices are rooted in long-standing practices that are resistant to change. These limitations notwithstanding, an organization can benefit by leveraging and developing a variety of acquisition constructs and making them broadly available for use.

Requirements Definition

Correct Any Existing Issues with Requirements Development

Developing capability requirements in large government organizations is complicated and involves intersecting processes. DHS capability needs are documented and validated through the Joint Requirements Integration and Management System (JRIMS), with the Joint Requirements Council governing JRIMS execution.[13] The planning, programming, budgeting, and execution (PPBE) process is DHS's decisionmaking process for allocating resources,[14] during which DHS components submit their proposed annual budgets to be discussed within the department before a final department budget is created. Navigating this process involves the development of multiple documents that take time to prepare and get through the validation process. Getting those documents prepared and approved as expeditiously as possible is therefore critical.

One approach for reducing delays in such processes is to utilize document templates to facilitate requirements development within shorter timelines.[15] Organizations can use these templates and fill in the information for specific families of capabilities or programs that share certain attributes. A widely accessible library of recently approved documents might also help serve as examples and offer select staff training in the process of developing requirements documents.

Another approach is to ensure that the existing requirements development process is utilized effectively, with each organization working to ensure that priority requirements have been documented through its requirements development process and are prioritized in its resource allocation plan. This requires that requirements development itself is appropriately staffed and funded.

To Increase Flexibility, Change How Requirements Are Developed

Multiple interviewees in our research indicated that additional flexibility was needed in the processes used to develop and approve cybersecurity requirements. Several said that a key issue was the speed at which threats were evolving. They noted that defining requirements and developing the needed documentation can take months or even years, by which time the threat has evolved and the needs have changed.[16] Interviewees also stated that the requirements for cybersecurity programs need to be approached in a fundamentally different way from requirements for other programs and need to be more flexible to allow for the fact that needs will inevitably change and new ones will emerge.[17]

To increase flexibility, requirements should be developed at the capability level rather than focused on specific technologies. The requirements should be focused more on operational criteria (what a solution will do) than on technical parameters (how a solution is implemented). Such an approach would leave the more-specific, technical decisions to be made by program managers and others closer to the time of need. Requirements would still need to be measurable and testable but could be based on user acceptance criteria rather than on technical parameters. This recommendation requires a combination of education, greater adherence to existing guidance, and improvements in the processes to develop and approve requirements on these criteria.

Communication and Measurement

Strive to Improve Program Communication Throughout a System's Life Cycle

Regular communication among stakeholders and process participants contributes to shared purpose and understanding. This can be especially true for customers and sponsors of cyber and IT systems, whose input is essential to precise specification in a rapidly moving technology landscape.

In our research, we found that it was often unclear to those involved in the acquisition process who was making decisions at key points or what those decision processes entailed. Some stakeholders reported that portions of the process were impediments and that elements of the process were working against the interest of others.

Engaging stakeholders early is a leading practice in managing acquisition programs. In March 2022, the U.S. Government Accountability Office (GAO) reported that leading companies "solicit early feedback from customers for both hardware and software development" to develop sound business cases.[18] Early engagement has also been highlighted in software development. In March 2019, GAO noted that "previous GAO reports as well as other DoD and industry studies have also found that user involvement is critical to the success of any software development effort."[19]

In addition to improving customer engagement, stakeholders in the acquisition process must share a common vision and goals. Senior DHS officials we interviewed emphasized the importance of relationships and how early engagement could address challenges.[20] High-performing units we have observed in the past have used project initiation meetings to allow program managers, leadership, and oversight elements to talk through anticipated challenges and deviations.

Finally, to support communication of technical information, organizations should simplify and strengthen the analytical underpinnings of the acquisition process by using historical data and models for common acquisitions, rather than reevaluating everything anew, especially for programs that are strikingly similar. For example, we noted that CISA might identify opportunities to redeploy models for program data (projecting cost, schedule, and performance) and technical factors (e.g., threat models, testing approaches, and other engineering evaluations) to better identify and convey technical information throughout the acquisition life cycle.

Institute an Acquisition Measurement Initiative That Addresses Every Step in the Acquisition Process, from Initiation to Sustainment and Across Development, Engineering, and Operations

Establishing metrics to monitor programs across all the phases of the acquisition process (development,

engineering, and operations) can lead to significant improvements both in the process to acquire items and in the acquired items themselves. This practice was identified in both acquisition literature and in interviews with practitioners who said that they had successfully utilized metrics to drive process change. Metrics can perform key functions, including "(1) evaluating and understanding performance levels, (2) identifying critical processes that require attention, (3) documenting results over time, and (4) reporting information to senior officials for decision making purposes."[21]

Performance metrics play an important role in illuminating what should be in an organization's strategic plan and then determining how the organization has achieved its goals. Greenfield and her colleagues noted that a performance management system can convey priorities, support decisionmaking as it concerns strategic planning and resource allocation, and enable development and continuous improvement.[22]

We recommend that CISA institute a comprehensive acquisition measurement initiative that addresses every step in the acquisition process, from initiation to sustainment and across development, engineering, and operations to systematically capture execution metrics to drive process changes. Measurements related to both the cybersecurity of acquired systems and the systems' resulting cybersecurity posture are essential to driving organizational goals. We observed that some CISA entities capture data and are therefore better positioned than other entities are to understand and diagnose issues. However, others were not consistently acquiring such data or had data that might be relevant but were not widely used or shared with stakeholders. The implementation of a more comprehensive initiative would drive process improvements across programs in various phases of the acquisition life cycle.

Oversight and Workforce

Focus on the Integration of Technical and Program Management

Technical and managerial aspects of program management intersect in multiple ways, providing the rigor and evidence necessary for dependable, trustworthy systems through engineering and acquisition processes. Cyber- and IT-related systems often have their own special needs, which are served through one or any combination of these approaches:

- **Mature program cybersecurity risk management, moving toward a security engineering approach.** We observed that CISA's cybersecurity risk posture for acquisitions was heavily focused on reactionary approaches—both in the focus of the acquisition itself and in the acquisition process. This is not meant to imply that CISA and DHS programs are devoid of proactive security activities but to signal that security was usually considered largely outside development and late in the ALF, by which time options for system change are (generally) costlier, more time-consuming, and less effective. A more proactive approach in engineering cybersecurity in the systems up front will improve outcomes by improving system quality, reducing downstream vulnerability, and better managing overall cost.
- **Move to continuous evaluation of programs, streamlined for agility.** Requirements focused on operational needs that are continuously delivered require continuous testing and evaluation as well. There is a cost to delaying such efforts that is often overlooked in development, as is the fact that, in some cases, it "reduces overall program risk because the program regularly delivers some degree of useful capability in each release."[23] Continuous evaluation necessitates sharing approaches and outcomes across programs, which can help with refining both testing and costing approaches—especially for iterative development. Additionally, appropriately leveraging engineering input at program initiation and major decision points can benefit agile development, in which "the environment must facilitate close collaboration across multiple disciplines to support rapid development cycles."[24] This collaboration requires buy-in from the engineering community, as well as the solicitation and utilization of opera-

tional user feedback as part of nontraditional acquisition.

- **Codify supporting processes to augment acquisition guidance.** Successful and efficient execution of any acquisition system relies on codified processes and the conveyance of leadership intent and expectation to those responsible for execution.

Develop Strategies to Recruit, Grow, and Retain Technical Acquisition Management Expertise

Perhaps the most widely recognized and discussed issue both within DHS and across the other government entities we engaged was related to personnel—specifically, recruitment, growth, and retention. These topics were discussed in the context of a variety of negative outcomes, including a loss of institutional memory, challenges in talent management, lack of technology proficiency, challenges with obtaining and retaining clearances, and high turnover, all contributing to inefficiencies in the acquisition process. Multiple interviewees indicated that they did not feel that they had the staff they required to complete the program. Respondents said that they recognized that this was not only a cyber or technical issue, nor an acquisition issue, but one that affects the broader government workforce.

Despite efforts to streamline hiring in cyber and IT, significant workforce issues continue to exist.[25] Recognizing the broad scope and complexity of this subject, we focused on workforce growth and retention, identifying some ways in which they can be addressed through changes in the acquisition system:

- Develop and improve program managers' awareness of processes and standards. A lack of process awareness and misconceptions regarding the roles of various stakeholders contributed to a reported negative view of the process itself.
- Refine process definitions to raise awareness and improve clarity of process and guidance.
- Increase autonomy to allow crucial program decisions, such as those pertaining to goals, process tailoring, and level of requirements definition, to be made at the project level (within well-established bounds). Additionally, improve tooling for implementing these processes to help codify, standardize, and automate acquisition processes.
- Incentivize and reward desired outcomes (e.g., cost savings, rapid deployment).
- Cross-train acquisition and technical professionals through short-term activities as programs for long-term, cross-functional development. A more agile acquisition workforce, or a workforce capable of operating in a more agile fashion, requires professionals who can see a broader picture of the organization and operate in ways that reduce friction between constituent parts.
- Incentivize key personnel through promotions and educational opportunities.

Conclusion

We have provided actionable, supported recommendations that ultimately speak to challenges that CISA and other government organizations face in their broader acquisition systems. Although our methodology did not provide a sufficient basis for quantitative analysis, it allowed a broad, sweeping examination of best practices and key insights utilizing input from across components and other government agencies. Recognizing that there is no singular right way to conduct cyber acquisition, we sought to identify the critical issues that CISA and similar organizations face and to provide recommendations that reflect the collective insight of researchers and practitioners.

We recommend that organizations consider each of these actions for immediate implementation, as appropriate. We also wish to highlight the interconnected nature of our recommendations, as well as their foundational nature. Each can be mapped to one or more long-term acquisition trends as identified by Wong and his colleagues, and the fact that they can be mapped to this broad historical perspective speaks to both the enduring nature and persistent character of these challenges.[26]

Ultimately, success in cyber acquisition requires that these issues be addressed in a way that recognizes an organization's unique culture and context

while accounting for the nuances imparted by the nature of cyber acquisition. It is our hope that these recommendations will assist CISA and other organizations in making sustained improvements on both cyber and traditional acquisition challenges well into the future.

Notes

[1] CISA, *CISA Strategic Plan*.

[2] National Institute of Standards and Technology, *Cybersecurity Framework*. This framework categorizes cybersecurity functions as identify, protect, detect, respond, and recover.

[3] DHS, "Rapid Acquisition."

[4] DHS, "Rapid Acquisition," p. 1.

[5] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Operation of the Adaptive Acquisition Framework."

[6] This is reflected in other RAND research, such as that reported in McKernan et al., *Using Metrics to Understand the Performance of the Adaptive Acquisition Framework*; McKernan and her colleagues did not find evidence in AAF metrics because programs were not far enough along in the various pathways.

[7] Stettina and Hörz, "Agile Portfolio Management," p. 140.

[8] CISA official, interview with the authors, January 31, 2022.

[9] CISA official, interview with the authors, March 2, 2022.

[10] Solutions for Enterprise-Wide Procurement, homepage.

[11] Office of the Chief Procurement Officer, "Other Transactions for Research and Prototype Projects Guide," p. 29.

[12] DHS, "Other Transaction Authority," p. 2.

[13] DHS, "Joint Requirements Integration and Management System," pp. 2–3.

[14] DHS, "Planning, Programming, Budgeting, and Execution," p. 5.

[15] For example, templates for the JRIMS documents are provided in Joint Requirements Council, "Joint Requirements Integration and Management System (JRIMS) Document User's Guide," Appendixes A through H.

[16] CISA officials, interviews with the authors, February 23, 2022, and March 28, 2022.

[17] CISA officials, interviews with the authors, February 23, 2022, and March 25, 2022.

[18] Oakley, *Leading Practices*, p. 21.

[19] Ludwigson, *DOD Space Acquisitions*, p. 11.

[20] DHS officials, interview with the authors, February 28, 2022; DHS official, interview with the authors, November 18, 2021.

[21] DiNapoli, *Defense Acquisitions*, p. 16.

[22] Greenfield et al., *Performance Management and Assessment of Federally Funded Research and Development Centers*, pp. 9–10.

[23] Arnold and Yüce, "Black Swan Farming Using Cost of Delay"; Modigliani and Chang, *Defense Agile Acquisition Guide*, p. 36.

[24] Modigliani and Chang, *Defense Agile Acquisition Guide*, p. 15.

[25] Alms, "Much-Hyped Effort to Help DHS Land Cyber Talent Is Slow to Make Hires."

[26] Wong et al., *Improving Defense Acquisition: Insights from Three Decades of RAND Research*.

References

Alms, Natalie, "Much-Hyped Effort to Help DHS Land Cyber Talent Is Slow to Make Hires," Nextgov/FCW, August 26, 2022.

Arnold, Joshua J., and Özlem Yüce, "Black Swan Farming Using Cost of Delay: Discover, Nurture and Speed Up Delivery of Value," *Proceedings of the 2013 Agile Conference*, Institute of Electrical and Electronics Engineers, August 2013.

Chairman of the Joint Chiefs of Staff, U.S. Department of Defense, "Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System," Instruction 5123.01I, October 30, 2021.

CISA—*See* Cybersecurity and Infrastructure Security Agency.

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, *CISA Strategic Plan: 2023–2025*, September 2022.

Defense Acquisition University, "Adaptive Acquisition Framework," webpage, undated. As of October 31, 2023: https://aaf.dau.edu

DHS—*See* U.S. Department of Homeland Security.

DiNapoli, Timothy J., *Defense Acquisitions: Goals and Associated Metrics Needed to Assess Progress in Improving Service Acquisition*, U.S. Government Accountability Office, GAO-13-634, June 2013.

Greenfield, Victoria A., Sandra Kay Evans, Laura Werber, Samantha Cherney, and Lisa Pelled Colabella, *Performance Management and Assessment of Federally Funded Research and Development Centers: Lessons from Academic Literature and Practitioner Guidance*, RAND Corporation, RR-A737-2, 2022. As of October 31, 2023: https://www.rand.org/pubs/research_reports/RRA737-2.html

Joint Requirements Council, U.S. Department of Homeland Security, "Joint Requirements Integration and Management System (JRIMS) Document User's Guide," September 2018.

Ludwigson, Jon, *DOD Space Acquisitions: Including Users Early and Often in Software Development Could Benefit Programs*, U.S. Government Accountability Office, GAO-19-136, March 18, 2019.

McKernan, Megan, Jeffrey A. Drezner, Mark V. Arena, Jonathan P. Wong, Yuliya Shokh, Austin Lewis, Nancy Young Moore, Judith D. Mele, and Sydne J. Newberry, *Using Metrics to Understand the Performance of the Adaptive Acquisition Framework*, RAND Corporation, RR-A1349-1, 2022. As of October 7, 2022: https://www.rand.org/pubs/research_reports/RRA1349-1.html

Modigliani, Pete, and Su Chang, *Defense Agile Acquisition Guide: Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities*, MITRE Corporation, March 2014.

National Institute of Standards and Technology, U.S. Department of Commerce, *Cybersecurity Framework*, version 1.1, April 16, 2018.

Oakley, Shelby S., *Leading Practices: Agency Acquisition Policies Could Better Implement Key Product Development Principles*, U.S. Government Accountability Office, GAO-22-104513, March 10, 2022.

Office of the Chief Procurement Officer, U.S. Department of Homeland Security, "Other Transactions for Research and Prototype Projects Guide," April 19, 2022.

Office of the Under Secretary of Defense for Acquisition and Sustainment, U.S. Department of Defense, "Operation of the Adaptive Acquisition Framework," Department of Defense Instruction 5000.02, January 23, 2020, change 1 effective June 8, 2022.

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002.

Solutions for Enterprise-Wide Procurement, homepage, undated. As of November 9, 2023: https://www.sewp.nasa.gov

Stettina, Christoph Johann, and Jeannette Hörz, "Agile Portfolio Management: An Empirical Perspective on the Practice in Use," *International Journal of Project Management*, Vol. 33, No. 1, January 2015.

U.S. Code, Title 6, Domestic Security; Chapter 1, Homeland Security Organization; Subchapter III, Science and Technology in Support of Homeland Security; Section 185, Federally Funded Research and Development Centers.

U.S. Department of Homeland Security, "Other Transaction Authority," Management Directive 0771.1, July 8, 2005.

U.S. Department of Homeland Security, "Joint Requirements Integration and Management System," Directive 107-01, revision 00, March 8, 2016.

U.S. Department of Homeland Security, "Acquisition Management Directive," Directive 102-01, revision 03.1, July 28, 2015, incorporating change 1, February 25, 2019.

U.S. Department of Homeland Security, "Planning, Programming, Budgeting, and Execution," Directive 101-01, revision 01, June 4, 2019.

U.S. Department of Homeland Security, "Acquisition Management Instruction," Instruction 102-01-001, revision 01.3, March 9, 2016, incorporating change 3, January 21, 2021.

U.S. Department of Homeland Security, "Rapid Acquisition," Instruction 102-01-011, revision 0, February 2020.

Wong, Jonathan, Obaid Younossi, Christine Kistler LaCoste, Philip S. Anton, Alan J. Vick, Guy Weichenberg, and Thomas C. Whitmore, *Improving Defense Acquisition: Insights from Three Decades of RAND Research*, RAND Corporation, RR-A1670-1, June 16, 2022. As of August 17, 2022: https://www.rand.org/pubs/research_reports/RRA1670-1.html

About the Authors

Chad Heitzenrater is a senior information scientist at RAND. His work centers on cyber warfare, acquisition and development of secure systems, signals intelligence, and mission assurance in the context of emerging warfighting concepts. He has a D.Phil. in computer science.

James Dimarogonas is a senior engineer at RAND. He currently conducts research on next-generation information technologies, military acquisition and procurement, refugees and forced migration, military space, multidomain command and control, cyber and electronic warfare, tactical and strategic communications and networks, and nuclear command and control. He has a Ph.D. in systems science and applied mathematics.

Kyle Bunch is a senior engineer at RAND. He specializes in technology and policy for problems of national security. He has a Ph.D. in electrical engineering.

Frank Camm is an adjunct senior economist at RAND. His work has addressed the organization of DoD space activities and acquisition activities in the Air Force Management Command, formal implementation of large organizational changes in the departments of the Army and Air Force, techniques to reduce acquisition risk by speeding acquisition of defense systems, effective use of other transactions to make Air Force development and acquisition activities more agile, adaptation of the commercial best practice of category management to an Army setting, the role of cost and pricing structures in source selections and acquisition of services, changes in intellectual property and data rights practices to improve sustainment of legacy and new weapon systems in the Air Force, and cost-effective life-cycle sustainment of the F-22. He has a Ph.D. in economics.

Ryan Consaul is a senior international and defense researcher at RAND. His areas of expertise include acquisition management; information technology; financial systems; human capital; employee integrity; and issues of waste, fraud, and abuse. He has an M.A. in national security studies.

Sarah W. Denton is a senior policy analyst at RAND. Her work includes diversity, equity, and inclusion; capability assessments within DoD, the intelligence community, and DHS; technology assessments; planning, programming, budgeting, and execution; intelligence planning, programming, budgeting, and execution; and federal budgetary and acquisition processes. She is a Ph.D. candidate in science and technology studies.

Quentin E. Hodgson is a senior international and defense researcher at RAND. His work focuses on cybersecurity, cyber operations, critical infrastructure protection, risk management, and command and control. He has an M.Sc. in national resource management and an M.A. in international relations.

Erin N. Leidy is a senior technical analyst at RAND. Some of her areas of interest are emerging technology, science policy, cybersecurity, and technology implementation. She has an M.S. in technology and policy.

Laurinda L. Rohn is a senior policy researcher at RAND. Her research areas include homeland security, security cooperation, strategy and resources, the future operating environment, military operations, doctrine, force structure, and resource allocation. She has a Ph.D. in public policy analysis.

James Ryseff is a technical analyst at RAND. His work focuses on how such technologies and practices as artificial intelligence, cloud computing, cybersecurity, agile software methodologies, and large-scale data analysis affect policy problems. He has an M.S. in security studies.

Yuliya Shokh is a senior technical analyst at RAND. Her research focuses on intelligence and acquisition communities, the role of intelligence support in military and domestic operations, and Russia's military planning and its impact on regional security. She has an M.A. in military studies and diplomacy.

Padmaja Vedula is a senior information scientist at RAND. She specializes in systems architecture, cybersecurity, cyber policy and deterrence, emerging technologies, and digital transformation, and her other areas of interest include technology and social well-being, forced migration and refugee assimilation, human rights, and environmental governance. She has an M.I.P.P. in American foreign policy and an M.S. in computer applications.

About This Report

The Cybersecurity and Infrastructure Security Agency (CISA) asked the Homeland Security Operational Analysis Center (HSOAC) to examine current acquisition processes for cyber technologies to identify lessons learned and approaches that could lead to streamlined acquisitions of such technologies. This report summarizes the results of that analysis, capturing high-level lessons with wide applicability. The findings should be of interest to acquisition and requirements professionals in CISA and in the U.S. Department of Homeland Security (DHS) more broadly, as well as to any individuals or organizations who deal with information technology and other cyber acquisition processes, such as program managers.

This research was sponsored by the CISA chief acquisition executive and conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division, which operates the Homeland Security Operational Analysis Center (HSOAC).

Acknowledgments

We would like to thank the many subject-matter experts from DHS and the U.S. Department of Defense who provided insights for this research. These participants spoke on a nonattribution basis, and, although we cannot identify them by name, we are grateful for their insights.

We would also like to thank CISA's chief acquisition executive, David Patrick, and our action officers, Tim Runfola and Chasity Long, who provided helpful guidance and feedback throughout the project and connected us with important subject-matter experts.

We would also like to thank our reviewers, Edward Balkovich and Megan McKernan, for their review of the manuscript and their invaluable suggestions. We thank Emma Westerman, Kelly Klima, and Abbie Tingstad for their helpful guidance and feedback during the project. Finally, we would like to thank the RAND Research Editorial and Production staff who contributed to the production and dissemination of this report.

An FFRDC operated by the RAND Corporation under contract with DHS

The Homeland Security Act of 2002 (Public Law 107-296, as codified at 6 U.S.C. § 185) authorizes the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. The RAND Corporation operates HSOAC as an FFRDC for DHS under contract HSHQDC-16-D-00007.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. The HSOAC FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under task order 70RCSA21FR0000072, "CISA Information Technology (IT) Acquisition Lifecycle Framework (ALF)."

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information on the RAND Homeland Security Research Division, see www.rand.org/hsrd. For more information on this publication, see www.rand.org/t/RRA1671-2.

This research was published in 2023.