INSPECTOR GENERAL

U.S. Department of Defense

FISCAL YEAR 2023

TOP DOD MANAGEMENT CHALLENGES

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Mission

To detect and deter fraud, waste, and abuse
in Department of Defense programs and operations;
Promote the economy, efficiency, and effectiveness of the DoD; and
Help ensure ethical conduct throughout the DoD

Vision

Engaged oversight professionals dedicated
to improving the DoD

For more information about whistleblower protection, please see the inside back cover.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

October 14, 2022

I am pleased to issue our annual report on the Department's most serious management and performance challenges as required by the Reports Consolidation Act of 2000. As in the past, the DoD Office of Inspector General (DoD OIG) independently identified the challenges based on a number of factors. Those factors included an assessment of the Department's strategic documents, such as the National Defense Strategy and Strategic Management Plan; completed oversight work by the DoD OIG and other agencies; input from DoD officials; congressional hearings and legislation; and issues identified by research institutes and the media. The challenges that we identified are neither exhaustive nor ranked in order of significance or severity.

This year we identified eight challenges, which are generally consistent with the challenges we identified in recent years. In particular, we reintroduced the topic of data as a standalone challenge, this time focusing on the DoD's efforts to accelerate its transformation to a data-centric organization. Although we present the challenges by topic, we examined them through the lens of the DoD's ability to effectively and efficiently execute its mission. Consequently, aspects of a challenge, such as the impact of the COVID-19 pandemic, can apply to multiple topics.

In addition to describing the challenges, we discuss recent actions taken by the DoD to address them; assess the DoD's progress in each challenge area; and cite planned, ongoing, and completed oversight work as applicable. The challenges we identified serve as the organizing principle for our DoD OIG annual oversight plan, to help us focus on audits and evaluations relevant to the DoD's most important performance and management challenges. Both the challenges and the oversight plan are key to the execution of our DoD OIG mission to detect and deter fraud, waste, and abuse in DoD programs and operations; promote the economy, efficiency, and effectiveness of the DoD; and help ensure ethical conduct throughout the DoD.

Particularly as the DoD provides substantial support to Ukraine, we look forward to continuing to conduct independent and objective oversight that helps the DoD execute its mission effectively, operate efficiently, and sustain the trust and confidence of the American people.

Sean W O'Donnell

Sean O'Donnell
Acting Inspector General

A Marine Corps AH-1Z Viper helicopter takes off from the USS Kearsarge during a live-fire exercise over the Atlantic Ocean. (U.S. Navy photo)

Summary of Management and Performance Challenges Facing the DoD

FISCAL YEAR 2023

Sailors with Naval Beach Unit Seven rehearse for an amphibious landing in Zambales, Philippines. (U.S. Marine Corps photo)

Executive Summary

The DoD OIG is required by law to report annually the most significant management and performance challenges facing the DoD. The challenges are identified using input from various sources, including oversight work of the DoD OIG and other organizations; congressional hearings and legislation; input from DoD officials; research institute analyses; and issues raised by the media. The DoD's progress to address challenges is also considered. The resulting independent report seeks to inform Congress and the public of the challenges affecting the DoD.

The FY 2023 Top DoD Management Challenges are:

1. Building Enduring Advantages for Strategic Competition
2. Strengthening Cyberspace Operations and Securing Systems, Networks, and Data
3. Maintaining Superiority Through a Resilient Defense Industrial Base
4. Improving Financial Management and Budgeting
5. Adapting to Climate Change, Accelerating Resilience, and Protecting the Environment
6. Protecting the Health and Wellness of Service Members and Their Families
7. Recruiting and Retaining a Diverse Workforce
8. Accelerating the Transformation to a Data-Centric Organization

The numerical designators for each challenge do not represent order of significance or severity. All identified challenges impact the DoD's ability to optimally execute its mission—to provide the military forces needed to deter war and protect the Nation's security.

CHANGES FROM THE FY 2022 TOP DOD MANAGEMENT CHALLENGES

The foremost differences from last year's report include the reframing of several challenges, integration of four previous standalone challenges to two, and the reintroduction of a standalone challenge on the theme of data. The change in the overall number of challenges from 10 to 8 does not reflect resolution of previously identified challenges.

Last year's challenge on "Maintaining the Advantage in Strategic Competition," and "Assuring Space Dominance, Nuclear Deterrence, and Missile Defense," were combined and reframed to "Building Enduring Advantages for Strategic Competition," which is consistent with the DoD's integrated strategic review approach underpinning the 2022 National Defense Strategy. Similarly, this year's challenge on "Maintaining Superiority Through a Resilient Defense Industrial Base" reflects the merger of two previous standalone challenges that focused on the supply chain and acquisition.

This year, "Accelerating the Transformation to a Data-Centric Organization," highlights the importance of the DoD Data Strategy, its implementation, and likely barriers. While the focus of the challenge is on efforts to accelerate the transformation, technological dominance and the collection and use of data affect all challenges to some degree. Data and associated systems permeate every aspect of the DoD and are integral to leaders making informed decisions for executing operations and measuring effectiveness of DoD programs, processes, and operations. Technological dominance and effective use of data are paramount for the DoD to succeed against strategic competitors that are investing heavily in new technologies, from major weapon systems to artificial intelligence.

STRATEGIC ENVIRONMENT

The strategic environment is contested and the DoD's ability to ensure its dominance will partly rest on how effectively it can address the challenges we present here. The domestic and global context affects the DoD's ability to accomplish its mission and effectively overcome the threats of today and tomorrow.

Domestically, the DoD faces manpower, financial, and operational pressures. Recruiting and retention of Service members and civilians is hampered by diminishing confidence in the military and a Government-wide decrease in morale and employee engagement.[1] Pandemic-induced uncertainty and economic pressures, further exacerbated by the fallout from Russia's assault on Ukraine, are increasing costs and decreasing purchasing power. The demands on the DoD are increasing as less traditional stressors like the COVID-19 pandemic response and the increased frequency and severity of extreme weather events strain readiness and resilience.

On the global front, the People's Republic of China (PRC) and Russia are leading the charge in hardening an anti-U.S. axis, seeking to disrupt the existing order. Whether through incentives, coercion, misinformation, or outright invasion, they seek to expand their spheres of influence and undermine U.S. standing and capabilities. The PRC's military transformation and sustained and sizable investment in quantum computing, artificial intelligence, and other technologies are likely to change how future wars are fought. Security cooperation is a growing area of competition, especially with nations such as the PRC, and although the United States has a competitive advantage, it is being challenged. It will be essential for the DoD to advance and safeguard its partnerships, particularly in the Indo-Pacific.

[1] "2021 Best Places to Work in the Federal Government Rankings," July 2022.

SUMMARY OF THE FY 2023 MANAGEMENT CHALLENGES

The DoD OIG is presenting eight challenges that it considers the most pressing matters facing the DoD in the upcoming fiscal year.

Management challenge 1, "Building Enduring Advantages for Strategic Competition," addresses factors that impact the DoD's ability to sustain and strengthen deterrence and competitive advantages, particularly against our most consequential strategic competitor, the PRC. Key to this challenge is continuing to build partnerships, balancing ongoing operations with sustainment and modernization, developing and fielding new capabilities at a faster rate.

Management challenge 2, "Strengthening Cyberspace Operations and Securing Systems, Networks, and Data," addresses the DoD's ability to protect and defend communication and computing systems, networks, devices, and data. Key to this challenge is strengthening cyber capabilities, improving cyber hygiene, and modernizing systems and software.

Management challenge 3, "Maintaining Superiority Through a Resilient Defense Industrial Base," focuses on the DoD's and the Defense Industrial Base's interdependence and associated risks. Key to this challenge is effectively using existing acquisition flexibilities, mitigating the effects of providing stockpiled weapons and supplies to Ukraine, and expanding the domestic and partner capacity for critical materials, such as microchips and minerals.

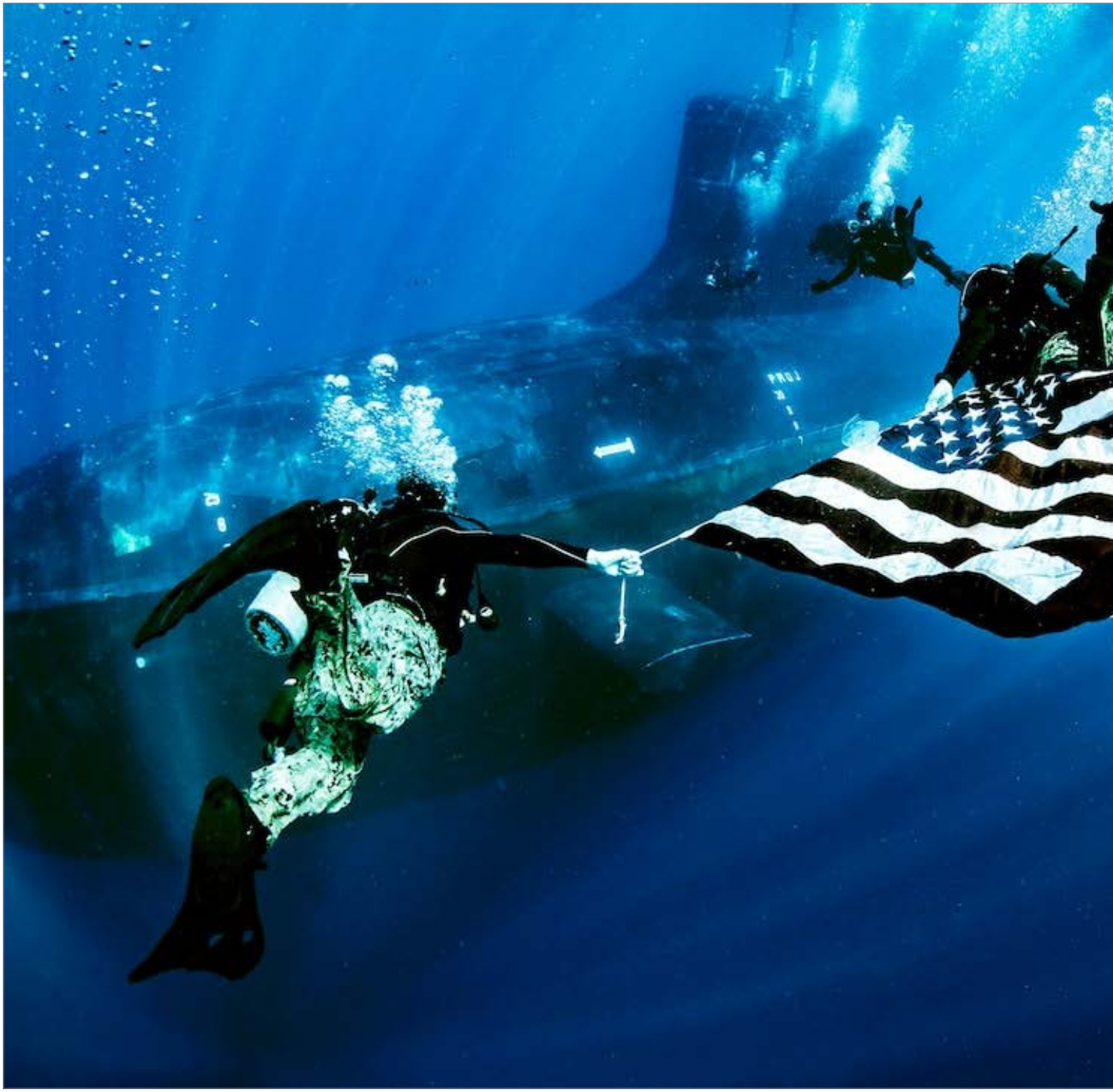
Management challenge 4, "Improving Financial Management and Budgeting," addresses barriers that affect the DoD's ability to attain a clean audit opinion. Key to this challenge is the lack of swift and aggressive changes to accounting and financial management processes, inability to improve internal controls and implement corrective actions in a timely manner, and continued use of legacy systems that do not comply with Federal requirements.

Management challenge 5, "Adapting to Climate Change, Accelerating Resilience, and Protecting the Environment," addresses three lines of effort of the DoD's Climate Adaptation Plan: making climate-informed decisions, training and equipping a climate-ready force, and building resilient installations and infrastructure. Key to this challenge is expanding climate literacy and training, integrating climate effects into operations, and addressing installations' maintenance and improvement backlog.

Management challenge 6, "Protecting the Health and Wellness of Service Members and Their Families," addresses readiness of health care personnel, mental health services, substance misuse, suicide prevention, and women's health. Key to this challenge is the adverse impact of the pandemic on health care providers and beneficiaries, the stigma associated with receiving care for conditions such as mental illness, and inadequate resources for women's health needs including during deployment.

Management challenge 7, "Recruiting and Retaining a Diverse Workforce," focuses on the DoD having the right people today and in the future to execute its mission. Key to this challenge is competition for talent, decreasing interest in military service, smaller pool of qualified candidates, inadequate talent management, and lack of complete and accurate data to measure diversity and inclusion.

Management challenge 8, "Accelerating the Transformation to a Data-Centric Organization," focuses on the importance and challenges of using data to inform DoD decisions and improve operational effectiveness. Key to this challenge is the DoD's ability to overcome cultural barriers, effectively implement its data strategy, and adopt innovation and best practices.



Sailors assigned to Naval Special Warfare Group 8 display the flag while performing dive operations from a fast attack submarine in the Atlantic Ocean. (U.S. Navy photo)

Challenge 1. Building Enduring Advantages for Strategic Competition

INTRODUCTION AND OVERVIEW

The 2022 National Security Strategy identified the People's Republic of China (PRC) as the most consequential strategic competitor and pacing challenge for the DoD.[2] As the DoD sharpens its focus on the PRC accordingly, maintaining the capacity to deter or defeat existing and potential threats requires continual vigilance, planning, and resources.

The DoD aims to secure the Nation's defense through integrated deterrence, campaigning, and actions that build enduring advantages. However, the DoD's ability to maintain its advantages is complicated by factors that include competing with adversaries for defense and security partners; balancing the execution of ongoing operations with sustainment and modernization; harnessing the potential benefits of emerging technology; and maintaining a capable and survivable strategic defense and deterrent capability. Although counterterrorism remains an important part of the DoD's mission, the challenge this year focuses on highest priority threats.

COMPETING FOR DEFENSE AND SECURITY PARTNERS AND BUILDING ENDURING ADVANTAGES

The United States and its partner nations gain strategic advantages from alliances and security partnerships.[3] Like the United States, the PRC and Russia aim to partner with nations to improve their organic defense and security capabilities. They undermine U.S. efforts by selling arms, offering economic and security assistance, and providing military training and equipment quickly, cheaply, and with fewer restrictions. They also offer military education to influence partner-nation military personnel and emerging military leaders. The DoD faces the challenge of demonstrating the value of its security cooperation model and position as the partner nation of choice.

The DoD has achieved mixed results in developing long-lasting improvements in building defense and security capability and capacity with partner nations. For example, after the collapse of the Soviet Union, the DoD and NATO's Partnership for Peace helped former Soviet states develop the

[2] The White House, "National Security Strategy," October 12, 2022.

[3] The Heritage Foundation, 2020 Index of U.S. Military Strength, "The Competitive Advantages and Risks of Alliances," October 2020.

institutional capacity and military capabilities to sustain themselves and become NATO allies.[4] In Afghanistan, the DoD trained and equipped Afghan forces, but was unable to develop the institutional capacity necessary for the Afghan military to absorb and sustain U.S. investments, particularly as the United States reduced its presence and withdrew from the country.[5]

The DoD security cooperation enterprise continues to mature and draw on lessons learned. Nevertheless, challenges remain in the DoD's ability to provide partners with tailored, cost-effective assistance that yields enduring improvements in defense and security. This is particularly true of partners in developing countries with weak institutions and fragile economies.[6] In future security cooperation activities, the DoD must apply the important lessons learned from past successes and failures in building defense capability. In September 2022, the DoD OIG issued a special report on lessons learned from security cooperation activities in Afghanistan, Iraq, and Africa.[7]

BALANCING EXECUTION OF CURRENT OPERATIONS WITH SUSTAINMENT AND MODERNIZATION

The DoD is responsible for planning and executing operations while also maintaining aging equipment and modernizing the Joint Force. These demands often compete for the same resources, requiring the DoD to decide on acceptable tradeoffs and risks, as well as which next-generation capabilities to pursue. The DoD must develop and field new capabilities at a faster rate to maintain its strategic advantage. However, the high costs of current operations, maintenance of legacy systems, and sustainment of a worldwide footprint present an obstacle to achieving those capabilities.[8]

Globally, the high operational pace continues to wear heavily on legacy equipment and incur significant maintenance costs. According to a 2020 Government Accountability Office (GAO) report, select DoD aircraft experienced an increase in operating and sustainment costs. For example, the F/A-18E/F fleet experienced an increase in annual operating and sustainment costs of $1.13 billion, which represents an average increase of $750,000 per aircraft. The increased costs were attributed to system improvements, high flight hours, and extensive maintenance associated with extending the service life of the aircraft, among other reasons.[9]

The U.S. military is spending less on procurement and more on maintenance, with the current pace of operations and maintenance requiring a significant investment at the expense of procurement.[10] Putting this into perspective, at the height of the Cold War, the share of military spending devoted to operations and maintenance was about 28 percent, compared to 42 percent in 2021, while weapons procurement fell from 30 percent to 19 percent.[11] According to the Future of Defense Task Force 2020 report, the DoD is underinvesting in modern technologies and overinvesting in legacy systems that do not have the lethality and survivability to be effective against competitors.[12] By 2030, up to 70 percent of

4 National Guard Bureau, "Long-term Relationships Drive State Partnership Program Success," July 26, 2022.

5 PRISM, National Defense University, "Introduction: Defense Institution Building: A New Paradigm for the 21st Century," November 20, 2017.

6 Small Wars Journal, "Implementing Security Cooperation Reforms: Challenges and Practical Approaches for USAFRICOM," June 19, 2020.

7 Report No. DODIG-2022-142, "Special Report: Lessons Learned from Security Cooperation Activities in Afghanistan, Iraq, and Africa," September 29, 2022.

8 According to the Defense Acquisition University, the DoD generally defines legacy systems as those systems in which the DoD has a substantial investment of both time and money. A legacy system is usually a system that is past its original expected service life and for which the DoD has a replacement system under development.

9 Report No. GAO-21-101SP, "Weapon System Sustainment Aircraft Mission Capable Rates Generally Did Not Meet Goals and Cost of Sustaining Selected Weapon Systems Varied Widely," November 19, 2020.

10 Bloomberg, "Legacy Weapons are Eroding the Military's Edge," June 7, 2021.

11 Ibid.

12 House Armed Services Committee, "Future of Defense Task Force Report 2020," September 23, 2020.

DoD platforms and weapons systems will be legacy systems if the U.S. defense posture maintains its current trajectory, and dependence on these legacy systems is likely to persist despite an exponential increase in innovation and emerging technology capabilities, particularly in areas such as artificial intelligence, biotechnology, and quantum computing.[13] In its March 2022 update, the Future of Defense Task Force noted that "the fight to retire outdated legacy systems is just beginning" and that budgeting and acquisitions processes are still "painfully slow and unnecessarily convoluted."[14] As we note later in this challenge, continuing resolutions can also impact the DoD's ability to acquire new systems efficiently and effectively.

The DoD's global footprint consists of deployed units and hundreds of permanent or semi-permanent bases. U.S. bases, along with deployed ships, aircraft, and personnel, provide global deterrence and rapid response capabilities, but at a substantial cost. Between 2016 and 2019, the DoD spent an average of $22 billion per year on building, operating, and maintaining U.S. bases overseas.[15] For example, over the same period, the operation and maintenance of bases in Japan cost the DoD an average of $5 billion annually.[16] The DoD has requested $25 billion for overseas costs in FY 2023. While the PRC and Russia do have bases outside their territorial footprint, they do not maintain nearly as many bases or standing forces outside their boundaries as the United States. The PRC and Russia are investing in future weapons and technologies, including long-range anti-aircraft and anti-ship weapons and cyber capabilities that aim to undermine the DoD's long-term advantage.

The rapid pace, high cost, and unpredictable nature of technology development make it difficult for the DoD to determine which next-generation capabilities—such as artificial intelligence, cyber, and hypersonic missiles—will provide the most significant return on investment. For FY 2023, the DoD requested roughly $130 billion in research, development, test, and evaluation funding for future capabilities. In some cases, the DoD has limited options to research, test, and evaluate new capabilities due to the urgency of life-cycle replacement, such as the nuclear triad, where all three segments require modernization. The rapid pace of technology development and the ability of adversaries to develop relatively inexpensive ways to counter expensive U.S. defense systems mean that the DoD cannot simply outspend adversaries to secure battlefield dominance.

REALIZING THE BENEFITS OF EMERGING TECHNOLOGY

The Under Secretary of Defense for Research and Engineering identified 14 critical technology areas considered vital to maintaining U.S. national security.[17] Many of these critical technologies are developed outside the traditional Defense Industrial Base (DIB) or involve dual-use technologies. Microelectronics, space technology, and advanced computing and software, are some of the dual-use technologies developed outside of the traditional DIB.

Reliance on dual-use technologies carries risks associated with market pressures, as revealed by the COVID-19 pandemic and subsequent supply

13 Ibid.

14 House Armed Services Committee, "Future of Defense Task Force: Report on Implementation," March 15, 2022.

15 Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, "Operation and Maintenance Overview," February 2020.

16 Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, "Operation and Maintenance Overview," Fiscal Years 2018-2021.

17 Under Secretary of Defense for Research and Engineering Memorandum, "USD(R&E) Technology Vision for an Era of Competition," February 1, 2022.

shortages and delays. Because the DoD is not the sole or dominant force in the market, it must adopt a whole-of-government approach to minimize risks.

For other critical technology areas such as biotechnology, quantum science, and future-generation communications, the private sector assumes the lead in development, but the DoD works closely with industry, academia, and across the U.S. Government to leverage commercial development and production for defense needs. Still, other areas, such as hypersonic systems and directed energy, are more reliant on the traditional DIB and require the DoD to take a leading role in research and development efforts.

The challenge for the DoD is developing new strategies to move at the pace of innovation. Research, development, and acquisition of emerging technologies require new approaches that can be carried out on a smaller scale, without having to be codified or applied across the Department. Artificial intelligence and machine learning development is highly iterative. DoD mission teams working on this emerging technology and their acquisition support offices are learning how to work at the speed of commercial development within the existing framework.[18]

MAINTAINING A CAPABLE AND SURVIVABLE STRATEGIC DEFENSE AND DETERRENT CAPABILITY

The United States is losing its strategic advantage in nuclear deterrence, missile defense, and space operations. In September 2021, the Commander of the U.S. Strategic Command declared that the PRC's rapid qualitative and quantitative expansion of military capabilities requires the DoD to make immediate and significant planning and capability shifts.

AGING NUCLEAR DETERRENCE PLATFORMS AND INFRASTRUCTURE

The DoD is at a point where service life limitations, coupled with underinvestment in existing nuclear deterrence platforms and infrastructure, leave no margin for error to meet national security objectives. The United States faces two nuclear-capable near-peers that can unilaterally escalate a conflict to any level, in any domain, with any instrument of national power. The DoD has the difficult task of managing risks related to readiness and capabilities of current nuclear platforms and systems while also allocating sufficient resources to develop and field new platforms and systems. For example, the Chief of Naval Operations stated in January 2022 that fiscal challenges and budget disputes, such as continuing resolutions, threaten the on-time delivery of the first four *Columbia*-class nuclear submarines—a "program with zero margin for delays."[19]

According to the DoD's annual report to Congress on "Military and Security Developments Involving the People's Republic of China," the PRC intends to have at least 1,000 nuclear warheads by 2030.[20] It is rapidly constructing new intercontinental ballistic missile fields and fielding new road-mobile systems. This rapid growth in the PRC's nuclear arsenal increases the complexity of the PRC nuclear threat. If the DoD does not modernize its nuclear systems to maintain capabilities that exceed those of our adversaries, or if the DoD fails to deliver these systems on schedule to avoid overextending the service life of legacy systems, it may compromise the United States' strategic advantage.

[18] Report No. DODIG-2022-049, "Evaluation of Contract Monitoring and Management for Project Maven," January 6, 2022.

[19] Statement of the Chief of Naval Operations before the House Appropriations Committee Subcommittee on Defense, January 12, 2022.

[20] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China–Annual Report to Congress," November 3, 2021.

AGING MISSILE DEFENSE TECHNOLOGY

In May 2022, the Director of the Missile Defense Agency stated that U.S. adversaries are developing more advanced ballistic, hypersonic, and cruise missile systems and making them more mobile, survivable, reliable, accurate, and capable of achieving longer ranges.[21] The Director added that current and future missile threats pose the growing technical challenges of high velocity, heavy maneuver, large numbers, and the exploitation of combination attacks involving unmanned aerial vehicles. PRC and Russia are developing hypersonic missiles that travel at exceptional speed and with unpredictable flight paths—advanced capabilities that challenge the DoD's existing defensive systems.[22] Additionally, hypersonic weapons operate in an area that neither space-based sensors nor ground-based radars are designed to detect.

SECURING THE ADVANTAGE IN SPACE

The DoD relies heavily on space to support air, sea, land, and cyber operations, but has faced increased competition in that domain in the past 5 years. In June 2022, the Chief of Space Operations said, "Space underpins all instruments of national power," and it is a "critical doorway to war" for all the Military Services.[23] As the PRC and Russia now possess sophisticated counter-space assets, the DoD can no longer assume unimpeded access to space for operations. While the DoD has made progress in being able to counter these threats, the DoD must modernize legacy satellites with 21st century capabilities to ensure it can freely access and safely operate in space.

The Defense Intelligence Agency's April 2022 report, "Challenges to Security in Space," stated that both the PRC and Russia will field more advanced counter-space systems this decade.[24] These systems, some of which are already in use, will include ground- and space-based kinetic and directed-energy weapons, as well as electronic warfare systems that can disrupt a satellite and jam its signals. In January 2022, a PRC satellite towed a derelict satellite into a different orbit and, since invading Ukraine, Russia has regularly jammed GPS signals in Ukraine.[25] Both the PRC and Russia continue to research and develop sophisticated capabilities that could serve civilian or military purposes and undermine U.S. national interests and security.

CONCLUSION

The PRC and Russia continue to assert their presence and influence around the world, while building cooperative defense and security relationships to undermine U.S. strategic advantages. Security cooperation partnerships enable pooling of resources and capabilities, intelligence sharing, and achievement of strategic aims. The DoD must strengthen and expand its network of reliable and capable partnerships, particularly in the Indo-Pacific. The high costs of maintaining a global footprint, conducting a range of operations, and sustaining legacy systems while investing in modernization require careful tradeoff analyses and decisions. Ultimately, building the Department's enduring advantages is the fundamental management challenge.

---

21 Statement of the Director, Missile Defense Agency, before the Senate Armed Services Committee Strategic Forces Subcommittee, May 18, 2022.

22 Office of the Secretary of Defense, 2019 Missile Defense Review.

23 Air & Space Forces Magazine, "Space 'Underpins All Instruments of National Power,' Raymond Says," June 17, 2022.

24 Defense Intelligence Agency, "2022 Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion," April 2022.

25 Center for Strategic and International Studies, "Space Threat Assessment 2022," April 2022.

Airmen train on the new Vision 60 "Robot Dog" at Minot Air Force Base, North Dakota. (U.S. Air Force photo)

Challenge 2. Strengthening Cyberspace Operations and Securing Systems, Networks, and Data

INTRODUCTION AND OVERVIEW

To effectively protect and defend the DoD Information Network (DODIN)—the globally interconnected set of information capabilities and communication and computing systems and services—the DoD must address the factors impeding the DoD's progress toward achieving the goals of its cyber and digital modernization strategies. The DoD continually faces sophisticated cyber attacks from adversaries, terrorist groups, and hacktivists who aim to exploit vulnerabilities on DoD networks and systems. Recent and ongoing cyber attacks and advanced persistent threats (APTs), like the Apache Log4J and SolarWinds Orion which exploited software weaknesses, highlight the need for the DoD to strengthen its cyber defenses.

The DoD is aware of the persistent challenges discussed in previous Top DoD Management Challenges. To achieve the cyber goals outlined in the 2018 DoD Cyber Strategy, the DoD should continue to focus on strengthening cyber capabilities, improving cyber hygiene, and modernizing systems and software.

STRENGTHENING CYBER CAPABILITIES

Recognizing the importance of enhancing cyber capabilities, the DoD requested more than $11.2 billion in FY 2023 to adapt to advanced persistent threats, protect and defend the DODIN, maximize improvements to offensive and defensive capabilities, build a strong cyber workforce, and develop capabilities for effective information sharing.

While the DoD has taken steps to improve its ability to protect networks, systems, and data, the cyber threat is constantly evolving. In February 2022, the Cybersecurity and Infrastructure Security Agency reported that, during 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed a global increase in sophisticated, high-impact ransomware—malicious software designed to block access to a computer system until a sum of money is paid—incidents

against critical infrastructure organizations, including the DIB.[26] According to a March 2022 article from McKinsey & Company, hackers are becoming more innovative and leveraging advanced tools, including artificial intelligence, machine learning, and automation, to accomplish their objectives.[27]

The DoD cannot protect itself without a highly skilled cyber workforce. McKinsey & Company estimated that, in March 2022, there were 3.5 million cybersecurity positions open worldwide. This level of demand for cyber professionals makes it difficult for the DoD to be competitive. The DoD has taken steps to attract new cyber talent and retain its current cyber workforce by offering recruitment and relocation incentives. However, the DoD and private industry are competing for the same cyber talent, and private sector offers are typically more lucrative. Therefore, it is critical for the DoD to adopt innovative ways and consider incentives to attract new talent and retain existing cyber professionals.

The DoD has made improvements in integrating tactical networks to enhance interoperability and information sharing between military departments. The 2022 National Defense Strategy expands this concept of enhanced interoperability and information sharing between the United States and its allies to create an integrated deterrence capability. The DoD and U.S. allies and partners are strongest when they can seamlessly work together and share information. The DoD has two programs focused on improving the DoD's interoperability and information sharing—the DoD Joint All-Domain Command and Control (JADC2) and the Joint Cyber Warfighter Architecture programs.

Despite the many advantages offered by these programs, the DoD must consider new challenges that these capabilities will create. For example, the Joint Force will benefit from JADC2 capabilities only if the DoD adopts a more collaborative approach to owning, sharing, and protecting data. For instance, the Air Force developed the Advanced Battle Management System (ABMS) to improve its decision-making processes for combat operations by acquiring, transmitting, and processing data between the Army, Navy, Air Force, and allied forces. However, according to the GAO, there are no formal plans for the ABMS Program Office to obtain mature technologies or conduct additional cost and affordability analyses to determine whether the Air Force should continue to maintain its traditional command-and-control systems until its replacement is operational. Without a viable plan for developing and deploying ABMS, the Air Force will fall short in its attempt to improve its current combat operations processes.

Cyber attacks are a preeminent threat to our national security, and the DoD must prepare accordingly. If malicious cyber actors can move within DoD networks, they could steal some of the Government's most valuable defense information and technologies, and disable cyber defenses.

IMPROVING CYBER HYGIENE

The oversight community continues to identify challenges with the DoD's cyber hygiene—the set of practices and steps intended to manage common cybersecurity risks—which affect not only the DoD, but also the networks and systems of the DIB and its cyber supply chain.

[26] Cybersecurity and Infrastructure Security Agency, Alert No. AA22-040A, "2021 Trends Show Increased Globalized Threat of Ransomware," February 9, 2022 (revised February 10, 2022).

[27] McKinsey & Company, "Cybersecurity trends: Looking over the horizon," March 10, 2022.

In a series of audits, the DoD OIG identified systemic cybersecurity weaknesses in DoD contractor networks that, if not corrected, would prevent contractors from protecting controlled unclassified information (CUI) stored on their networks. Based on the recommendations from these audits, the DoD continues to improve cyber hygiene by identifying and remediating cyber vulnerabilities.

To certify that information on contractor networks is protected, the DoD launched the Cybersecurity Maturity Model Certification 2.0 program in 2021. However, the program is still under review for inclusion in the Defense Federal Acquisition Regulation Supplement, a process that might not be complete until December 2023. Without a mature program to verify that DIB contractors are implementing appropriate cybersecurity practices and processes to protect CUI stored on their networks, the DoD cannot ensure that DoD CUI is safe from malicious cyber actors who specifically target contractor networks and systems. Furthermore, a January 2022 Federal News Network article stated that the 2.0 version of the program, "better aligns with federal standards and requirements, but falls well short of being the 'bold change' President Biden called for in his much-touted May [2021] cybersecurity executive order."[28] With an increased focus on expanding public and private partnerships and expanding the DIB, the DoD will need to ensure proper protection of its information.

The DoD is taking further steps to improve its cyber hygiene by developing system design principles to support a zero-trust architecture (ZTA) model—a security model based on an acknowledgement that threats exist both inside and outside traditional network boundaries. A ZTA model eliminates implicit trust in any one user, device, or service. In essence, it allows users full access, but only to the essential functions necessary to perform their duties. Using a ZTA model requires continuous verification with real-time information from multiple sources to determine access and other system responses. In August 2022, the DoD Chief Information Officer stated that the DoD is committed to implementing a ZTA model across the DoD by 2027. He admitted that 2027 is an ambitious goal, but stated that "the adversary capability we're facing leaves us no choice but to move at that level of pace."[29]

The DoD reactively responds to APTs as they occur by developing procedures that the DoD should follow to assess the effect of the threats on DoD networks and systems. APTs refer to an adversary with sophisticated levels of expertise and significant resources that allow the adversary to generate opportunities to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information, or to undermine or impede critical aspects of a mission, program, or organization. While the DoD has procedures for assessing the impact of APTs and provides step-by-step instructions on how to address APT compromises, it does not always complete the steps necessary to prevent malicious cyber actors from advancing their footprint within the DODIN.

Cybersecurity experts estimate that organizations could defeat 90 percent of cyber attacks by implementing basic cyber hygiene. The results of poor cyber hygiene cause a domino effect throughout DoD network environments

[28] Federal News Network, "The Pentagon's new cybersecurity model is better, but still an incremental solution to a big challenge," January 17, 2022. Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

[29] FedScoop, "CIO Sherman: DOD is committed to fully implementing zero trust by 2027," August 24, 2022.

that could open backdoors for malicious cyber actors to access and launch debilitating cyber attacks. Therefore, the DoD must prioritize the cyber hygiene of its networks and systems and ensure that DIB contractors are continuously implementing cybersecurity protections.

MODERNIZING SYSTEMS AND SOFTWARE

On February 1, 2022, the DoD published its Software Modernization Strategy. The strategy states that, "The department's adaptability increasingly relies on software and the ability to securely and rapidly deliver resilient software capability. That is a competitive advantage that will define future conflicts."[30] In a DoD News article from March 2022, the Deputy Chief Information Officer for Information Enterprise emphasized the importance of the cloud and harnessing the power of cloud computing to build applications continuously and improve cybersecurity.

However, implementing the strategy will be challenging. The offices of the Chief Information Officer and the Under Secretaries of Defense for Acquisition and Sustainment and Research and Engineering, as well as the software modernization senior steering group, are all involved in efforts to operationalize the strategy. According to a February 2022 FedScoop article, the DoD's Chief Software Officer stated that a key enabler of achieving the goals in the strategy will be collaboration between 29 software factories and the creation of "enterprise shared services."[31] The article further states, "How that sharing will work is still an unanswered question… The deployment of shared services cuts across budgetary and cultural silos." This will require a "hybrid model" with different Military Departments taking the lead on different aspects of the shared services.

Nearly all DoD weapon systems depend on software to perform critical functions. The DoD's increasing reliance on software presents opportunities for adversaries to gain unauthorized access, alter data, disrupt operations, or compromise communications by corrupting system components. To combat new threats to system survivability, the DoD must continually monitor and improve cyber resiliency throughout a weapon systems' life cycle to be confident that systems are able to prevent, mitigate, and recover from attacks.

In March 2021, the GAO reported that the DoD continues to face challenges with contracting for cybersecurity in weapon systems after identifying several DoD programs that did not include cybersecurity requirements in contracts.[32] The GAO reported that the DoD acquisition programs that they reviewed omitted cybersecurity requirements from the contract or did not define cybersecurity, and recommended that the DoD ensure that cybersecurity requirements are included and defined in acquisition programs. To create resilient systems, the DoD needs to improve cybersecurity requirements, including software assurance, in program contracts. Software assurance is the level of confidence that software functions only as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle.

Cybersecurity risks throughout the supply chain have the potential for harm or compromise when cybersecurity risks

[30] DoD News, "DoD Publishes New Software Modernization Strategy," March 27, 2022.

[31] FedScoop, "DoD publishes new software modernization strategy, memos on code," February 4, 2022.

[32] Report No. GAO-21-179, "Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors," March 4, 2021.

posed by suppliers, their supply chains, and their products or services go undetected.[33] Cybersecurity Supply Chain Risk Management is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. In February 2022, the DoD issued an action plan that identified challenges with managing the cyber supply chain. Although the DoD is working to enhance the assessment of the cybersecurity practices of the highest priority suppliers and integrators, and improve the cybersecurity monitoring of priority suppliers and integrators, adversaries are continually increasing their campaigns to infiltrate DoD networks and systems. In June 2022, the GAO reported that 14 of the 25 DoD information technology programs it reviewed did not have a system security plan addressing information and supply chain risk management of communications technology.[34] The report stated that "[u]ntil DoD ensures that these programs have such plans, they are less likely to be able to manage supply chain risks and mitigate threats that could disrupt operations."

In February 2022, the GAO reported that the DoD continues to face challenges with having usable data to train artificial intelligence capabilities and integrating trained artificial intelligence into existing weapon systems that were not designed for it.[35] At a March 2022 meeting of the Armed Forces Communications and Electronics Association, the National Security Agency Technical Director stated that using fifth-generation (5G) technology for military and national security applications requires interoperable and secure standards and policies that will define how capabilities work together.[36] He also stated that the DoD is working to understand how it will integrate DoD services with 5G technology. Although the DoD is making strides to implement 5G wireless communication technology capabilities, the DoD must consider the long-term implications of falling behind adversaries in the race to deploy 5G communication technologies across its networks.

CONCLUSION

The cyber challenges discussed in this chapter are not new to the DoD. To respond effectively to our aggressive and innovative adversaries, the DoD must be equally aggressive and innovative with our cyberspace operations and capabilities to defend and protect the Nation's most sensitive information and technologies. Strengthening the DoD's cyber capabilities to adapt to the evolving pace, scale, and complexity of cyber threats from adversaries is critical to protecting the DoD's systems, networks, devices, and data. The DoD must also share information internally, with other Federal agencies, and with partners and allies to protect against APTs. Improving the DoD's cyber hygiene reduces the risk of strategic competitors and malicious cyber actors exploiting vulnerabilities, which is key as the DoD increases its cyber capabilities and the DIB expands. Modernizing DoD systems and software, as well as using new technologies to monitor and adjust to emerging threats, is vital for improving and defending DoD cyberspace operations.

[33] National Institute of Standards and Technology Special Publication 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

[34] Report No. GAO-22-105330, "Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning," June 14, 2022.

[35] Report No. GAO-22-104765, "Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems," February 17, 2022.

[36] FCW.com, "5G has military promise but security concerns are still being untangled," March 10, 2022.

A Marine lowers supplies from a helicopter to a Navy submarine off the coast of California. (U.S. Marine Corps photo)

Challenge 3. Maintaining Superiority Through a Resilient Defense Industrial Base

INTRODUCTION AND OVERVIEW

The DIB is vital to national security because it provides many of the goods and services the DoD relies upon, from major weapon systems and ammunition to everyday commercial items. In FY 2021, the DoD contracted with the DIB for goods and services totaling $444 billion. The DIB encompasses manufacturers, commercial and organic service providers, technology innovators, labs and research organizations, and other suppliers linked together by complex global supply chains. The DoD recognizes the importance of the DIB and the challenges it faces, and produced several assessments that exposed risks to supply chains and offered action plans to mitigate them. However, information gaps remain about the effectiveness of some acquisition policies. The effects of the COVID-19 pandemic, inflation, overreliance on foreign suppliers, Russia's ongoing war with Ukraine, and an aging organic industrial base, have heightened DoD and public awareness of the fragility of the supply chain and risks to the DIB.

TRANSPARENCY AND RELIABLE INFORMATION IS NEEDED TO ENABLE A RESILIENT AND COMPETITIVE DIB

The DoD relies on the DIB's innovation to develop advanced capabilities that provide advantages necessary for the DoD to achieve its objectives. Congress granted the DoD authority to tailor acquisition strategies and contracting mechanisms to rapidly adopt and field capabilities. The DoD has employed middle-tier acquisition (MTA) and other transaction authority (OTA) to achieve faster development and delivery of capabilities. The MTA and OTA facilitate faster development and delivery of advanced capability and promote use of non-traditional vendors. However, their full benefit is difficult to assess due to insufficient program data, lack of existing performance indicators and analysis, and database limitations that impede transparency.

MTA is a rapid acquisition approach that focuses on delivering capability in 2 to 5 years. The DoD is increasing its use of the MTA pathway with 131 programs as of October 2022. However, the DoD struggles to rapidly field capabilities within budget that meet user needs because the DoD lacks sufficient program data related to cost, schedule, and performance that would enable adequate management oversight. In a 2022 report, the GAO determined that MTA programs did not have consistent cost information and plans in place to gain sufficient technical information for follow-on efforts, such as further development, testing, or production. Also, some programs missed key events that could challenge planned fielding schedules.[37]

The intent of OTAs is to provide the DoD access to state-of-the art technologies, increase competition, and broaden the DIB by reducing barriers to working with the DoD. Although OTAs are an innovative way to develop prototype technologies and products, the DoD faces ongoing challenges with reporting and tracking OTAs, thereby limiting transparency. In 2021, the DoD OIG reported problems tracking OTA information and determined that the Federal Procurement Data System–Next Generation was not set up to track certain types of OTAs.[38] Without accurate information on OTAs, the DoD cannot perform the necessary oversight to ensure that programs are achieving the expected benefits, such as expanding the DoD's access to new technologies or expanding the DIB.

STRAINED SUPPLY CHAINS AND HIGH INFLATION HAVE TESTED THE DIB'S RESILIENCE

Pandemic-strained supply chains, ongoing weapons transfers to Ukraine, and inflationary pressures have raised concerns about the DoD's military readiness and the ability to replenish depleted stockpiles. Newly proposed legislation, such as the Securing American Acquisitions, Readiness, and Military Stockpiles Act of 2022, seeks to give the DoD enhanced procurement authorities to quickly replenish defense stockpiles.

At the 2022 Defense News Conference, the Under Secretary of Defense for Acquisition and Sustainment stated that he was worried about the effect of inflation on small suppliers and firm-fixed-price (FFP) contracts. He stated that FFP contracts are the most commonly used contract type for anyone doing business with the Government. FFP contracts are not subject to any price adjustments, and the contractor bears full responsibility for all costs and resulting profit or loss. Therefore, if an FFP contract was signed in 2020, the contractor is subject to a 10-percent inflation rate increase in 2022. The Under Secretary further stated that the DoD needs to stabilize the supply chain by offering multiyear contracts for munitions, not just for ships and airplanes, to assure industry of its commitment and invest in building redundancy to increase supply chain resilience and reduce the impact of problems that may occur with limited sources of supply.[39]

Historically high inflation has tested the DIB's ability to fulfill long-term commitments to the DoD. The DIB receives hundreds of billions

[37] Report No. GAO-22-105230, "Weapon Systems Annual Assessment: Challenges to Fielding Capabilities Faster Persist," June 2022.

[38] Report No. DODIG-2021-077, "Audit of Other Transactions Awarded Through Consortiums," April 21, 2021.

[39] DoD News, "Defense Official Speaks on Supply Chain Investments, September 7, 2022.

of dollars in contract actions to develop and maintain warfighting capabilities and some of these contract actions require long-term commitments of 5 years or more. For example, the Navy's plan to develop and build the *Columbia*-class ballistic missile submarine has required decades of commitment from the contractor, which began in 2011 with the original contract award. The Navy plans to field the first submarine in 2030, but the current wave of inflation has significantly increased prices for submarine construction materials and introduced risks to the program. In this particular case, the Navy was able to account for the material price escalation, but the uncertainty induced by inflation highlighted the risks of establishing long-term contracts. The DIB may hesitate to contract with the DoD unless price escalation clauses are included in contracts to mitigate effects of inflation.

ESTABLISHING A ROBUST NETWORK OF TRUSTED DOMESTIC AND ALLIED SUPPLY CHAINS

Strategic and critical materials such as microchips, semiconductors, and rare earth minerals enable the unique capabilities of U.S. weapon systems and those of our allies, while providing the essential inputs to expand the industrial base and maintain technical superiority over our adversaries. The DoD has identified five risk factors that affect the strategic and critical materials sectors upon which it relies to secure its advantages: (1) concentration of supply, (2) single-source suppliers, (3) price shocks, (4) human capital gaps, and (5) conflict minerals and organized crime. Although these risks to the supply chain are not new, they have been exacerbated by the COVID-19 pandemic and invasion of Ukraine.

In February 2022, the Deputy Secretary of Defense established the position of Assistant Secretary of Defense (Industrial Base Policy) (ASD[IBP]) to be the principal advisor to the Under Secretary of Defense for Acquisition and Sustainment. The ASD(IBP) is working to develop a strategy to address the DoD's challenges establishing a robust network of trusted domestic and allied supply chains for the DIB. In July 2022, the GAO identified that the DoD does not have sufficient information to determine whether industrial base risks have been mitigated and what additional resources or actions may be needed.[40] Specifically, the GAO determined that the DoD struggles to clearly identify milestones, performance measures, resources, and implementation plans for mitigating industrial base risks.

Multiple DoD OIG audit reports over the last 2 decades have highlighted why sole-source contracts continue to be a problem. For example, the DoD OIG determined that sole-source contracts for depot maintenance led to the DoD paying at least $71.9 million in cost escalation because the cost of the maintenance exceeded the amount awarded in the contracts.[41] In another example, the DoD OIG determined that TransDigm executed a business model focused on the acquisition of companies that specialize in highly engineered sole-source spare parts, which constrained the DoD's ability to make fair and reasonable price determinations.[42] The report also highlighted that in a sole-source environment, contracting officers face challenges when trying to obtain necessary data to identify excessive pricing

[40] Report No. GAO-22-104154, "Defense Industrial Base: DOD Should Take Actions To Strengthen Its Risk Mitigation Approach," July 7, 2022.

[41] Report No DODIG-2022-104, "Audit of Sole-Source Depot Maintenance Contracts," July 21, 2022.

[42] Report No DODIG-2022-043, "Audit of the Business Model for TransDigm Group Inc. and its Impact on Department of Defense Spare Parts Pricing," December 13, 2021.

because of gaps in Federal and DoD policies. To address the lack of policies, officials from Office of the Under Secretary of Defense for Acquisition and Sustainment submitted several legislative proposals to address sole-source challenges. However, Congress did not approve the legislative proposals. Without the ability to bridge the policy gaps and other opportunities to make fair and reasonable price determinations, sole-source contracting will remain a challenge for the DoD.

In July 2021, the House Armed Services Committee's Defense Critical Supply Chains Task Force released a report that identified significant supply chain risk with microelectronics and rare earth minerals.[43] Microelectronics are a key component in many of the DoD's advanced capabilities, including precision-guided munitions, hypersonic weapons, and satellites. Most microelectronics production, assembly, packing, and testing occurs overseas, primarily in the Asia-Pacific region. The DoD continues to rely on allies like Taiwan and South Korea for sourcing, but the proximity of these nations to China, which continues to conduct destabilizing activities in the area, could disrupt the DoD's supply chain and ability to procure microelectronics.[44]

Congress recently passed the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022, to strengthen domestic supply chains and decouple from foreign suppliers, but it will take years to establish domestic capabilities that are cost-competitive and sustainable. In a May 2022 report, the DoD OIG determined that the DoD did not establish trusted supply chain and operational security standards related to procuring custom microelectronics by January 1, 2021, as required by the FY 2020 National Defense Authorization Act.[45] The DoD is still developing the standards and instructions necessary to implement a quantifiable assurance method to procure custom microelectronics.

In May 2022, the DoD issued a microelectronics (ME) vision consisting of seven interconnected objectives, including ensuring timely access to secure and affordable ME technology; increasing ME innovation and accelerating transition into DoD systems; and influencing interagency and national efforts to grow ME capabilities.[46] However, the DoD has not developed a holistic strategy or an implementation and transition plan that identifies specific responsibilities for reducing reliance on foreign suppliers.

The dependency on foreign suppliers extends to critical minerals, which are the building blocks for modern technologies essential to national security. For example, neon is critical in the chip production process and Russia and Ukraine produce 70 percent of the world's neon. Russia's war in Ukraine could cause global production of neon to fall short of demand or limit access to neon, creating significant vulnerabilities if the conflict in Ukraine continues. While the Office of the ASD(IBP) is tracking supply chain constraints and market volatility for a variety of critical materials and supplies, it has not developed performance measures to track the DoD's progress on mitigation efforts to increase domestic production and reliance on allies to advance the supply chain and the DIB.

[43] United States House Armed Services Committee, "Report of the Defense Critical Supply Chain Task Force," July 22, 2021.

[44] Report No. DODIG-2022-084, "Evaluation of the Department of Defense's Transition From a Trusted Foundry Model to a Quantifiable Assurance Method for Procuring Custom Microelectronics," May 2, 2022.

[45] Ibid.

[46] Defense Microelectronics Cross-Functional Team, "U.S. Department of Defense Microelectronics Vision," May 2022.

MODERNIZING THE ORGANIC INDUSTRIAL BASE

The Organic Industrial Base (OIB) is composed of DoD-owned and -operated maintenance depots, shipyards, fleet readiness centers, air logistics centers, and arsenals that maintain and repair critical weapon systems and equipment. The OIB is essential for national defense because it enables the DoD to maintain core logistics capabilities that are Government-owned and Government-operated. This ensures that the DoD has a ready and controlled source of technical competence and resources necessary to respond effectively and quickly to large-scale combat operations, national defense contingency situations, and other emergency requirements. However, the DoD risks not being able to fully maintain its core logistics capabilities because of underinvestment in critical facilities and equipment.

In October 2021, the Acting Assistant Secretary of Defense for Sustainment testified that years of underinvestment have led to a significant degradation in the OIB's infrastructure.[47] The United States Code requires the Military Department Secretaries to invest a percentage of funds in their depots based on work done at the depots in the preceding 3 fiscal years. However, this investment has not been enough to modernize and maintain the OIB.

Degradation of DoD depot facilities and equipment has adversely affected the DoD's readiness and incurred extra costs. In 2019, the GAO reported that 12 out of 21 depots the GAO assessed were in poor condition and the average age of depot equipment at 15 depots exceeded the equipment's expected useful life.[48] The GAO concluded that these deficiencies in infrastructure have affected repair times, depot efficiency and capacity, and have incurred hundreds of millions in extra costs. In addition, the report indicated that the Military Departments have developed multiple preliminary long-term improvement plans to address the neglected OIB, but the Military Departments have generally not implemented the plans as originally envisioned. The Military Departments consider the plans a first step, not the result, and they are developing more complete modernization plans. The DoD OIG is currently auditing the Navy's planning efforts related to environmental threats to naval dry docks.

CONCLUSION

The DoD relies on the products, services, and innovation provided by the DIB to accomplish its mission. The DoD must capture the information necessary to determine whether MTAs and OTAs achieve the expected benefits. The COVID-19 pandemic and inflation have exposed the fragility of supply chains and the DoD's dependence on foreign suppliers for critical materials and supplies. In addition, the DoD's slow progress to modernize the OIB jeopardizes material support of critical weapons systems. A healthy DIB and trusted supply chains are essential to DoD mission success.

[47] Statement of the Acting Assistant Secretary of Defense (Sustainment) before the House Committee on Armed Services Subcommittee on Readiness, October 28, 2021.

[48] Report No. GAO-19-242, "Actions Needed to Improve Poor Conditions of Facilities and Equipment that Affect Maintenance Timeliness and Efficiency," April 29, 2019.

Financial officers from units around the Indo-Pacific Command area of operation gathered at the United States Pacific Command for a Finance Symposium at Fort Shafter, Hawaii. (U.S. Army photo)

Challenge 4. Improving Financial Management and Budgeting

INTRODUCTION AND OVERVIEW

Accurate, auditable reporting of DoD financial and budgeting information helps the American public and Congress understand and trust that the DoD is a good steward of public funds. However, after more than 15 years of performing audit readiness and remediation efforts, the DoD and most of its Components are still years away from clean audit opinions.

In FY 2021, the DoD OIG completed or oversaw the completion of 26 financial statement audits, 17 of which received disclaimers of opinion because the DoD was unable to provide sufficient evidence for the auditors to produce an opinion. While the DoD has made progress, as demonstrated by taking corrective action that allowed the DoD OIG and independent public accounting firms (IPAs) to close 808 prior-year notices of findings and recommendations (NFRs), there is still significant progress to be made. Auditors reissued 2,678 prior-year NFRs, and issued 690 new NFRs for a total of 3,368 open NFRs. These NFRs provide the DoD with information about problems found during the financial statement audits and recommend ways to resolve the problems. The DoD acknowledges that financial statement audits yield value far beyond the audit opinions as they identify vulnerabilities in IT systems; improve data reliability and visibility for decision-making and budget execution; and help the Department improve its operations and gain efficiencies. However, progress is hampered by the lack of timely action to resolve material weaknesses and by reliance on legacy information technology systems without appropriate controls. Progress further slows as unplanned contingencies require the DoD to realign resources on short-notice.

TIMELY REMEDIATION OF WEAKNESSES

As outlined in the DoD OIG report, "Understanding the Results of the Audit of the DoD FY 2021 Financial Statements," the DoD must make swift and aggressive changes to its accounting and financial management business processes to obtain and sustain auditability. Senior leaders within the DoD recognize the need to improve these processes, including the Secretary of Defense, who stated in November 2021, "We must work harder to institute stronger internal controls and prove in every way that we are being good

stewards of taxpayer dollars."[49] Although the DoD has shown some progress in improving business processes and closing NFRs, the DoD has generally not met its top-level goals to remediate material weaknesses and significant deficiencies. In FY 2021, the DoD OIG and IPAs identified 166 material weaknesses and 51 instances of non-compliance with laws and regulations, contracts, and grant agreements for DoD Components.

For FY 2022, the DoD established three financial management focus areas to target material weaknesses: (1) improve Fund Balance with Treasury, (2) establish user access controls, and (3) create a supportable universe of transactions and improved financial reporting internal controls. Based on the June 2022 Financial Improvement and Audit Remediation (FIAR) Report, substantial work remains. For the first focus area, the DoD continues to improve the accuracy of the Fund Balance with Treasury, but unsupported balances remain in DoD accounts. For the second focus area, DoD officials stated that they plan to address material weaknesses related to access control and segregation of duties through a cybersecurity domain that allows agencies to securely access resources across existing systems and platforms, but do not plan to complete these actions until FY 2028. Finally, for the third focus area, the DoD is still working to compile and validate a complete list of all relevant systems that feed the DoD's financial systems, and does not plan to complete the actions until FY 2028.

While the full scope financial statement audits started in FY 2018, the DoD has known many of these focus areas were roadblocks to its auditability since at least 2005; 17 years later these problems remain. Timely resolution of material weaknesses and continuous improvement of business processes and systems will help ensure that the DoD can obtain a clean audit opinion.

RELIANCE ON LEGACY FINANCIAL SYSTEMS AND INTERNAL CONTROL WEAKNESSES PERSIST

The DoD will continue to face challenges related to financial management and budgeting due to its size and complexity, shortcomings in its current business processes, and reliance on legacy systems. The DoD financial statement preparation process is complex and often involves multiple layers of accounting and financial feeder systems.[50]

The DoD currently manages nearly 300 feeder systems, which often do not capture data in a standardized way or effectively integrate with other systems. For example, the Air Force has 30 feeder systems that use both manual and automated processes to enter financial transactions in two general ledger systems.[51] Due to system weaknesses, the Air Force systems require officials to create manual entries (referred to as journal vouchers) to report transactions. In cases where transactions do not post in a timely manner or are incorrect, the Defense Finance and Accounting Service has to perform additional work to ensure that the DoD general ledger is accurate and auditable.

Replacing and consolidating legacy systems is difficult given the size and scope of the DoD. Some of the legacy systems are from the 1960s and were not designed or updated with financial statement support in mind. Although the DoD

[49] "Statement by Secretary of Defense Lloyd J. Austin III on the DoD's Fourth Annual Department-Wide Financial Statement Audit," November 15, 2021.

[50] Financial feeder systems include accountable property systems of record, sub-ledgers, and management information systems. These systems feed financial information via multiple processes including automated interfaces, manual interfaces, and journal vouchers. The DoD uses 299 feeder systems.

[51] One is a legacy system, and the other is an enterprise resource planning system.

acknowledges the associated risks, it historically underestimates the time necessary to retire legacy systems or to integrate the requirements into newer systems, often extending retirement dates. For example, in a February 2022 report, the GAO concluded that the Air Force did not develop a migration plan from its legacy system to its replacement system.[52] The GAO noted that although the Air Force had efforts under way to address certain financial and information technology-related deficiencies, the Air Force did not have a comprehensive strategy, with appropriate performance metrics, for its financial system modernization efforts and related financial reporting.

The DoD also extended the retirement dates for nine legacy systems from September 2020 to September 2021. However, as of April 2022, none of the nine systems were retired. Furthermore, there were at least 140 systems noncompliant with certain Federal financial management system requirements, but the DoD does not consider these systems as legacy because the DoD does not plan to retire them until FY 2036. The continued use of legacy systems that do not comply with Federal requirements inhibits the ability of the DoD and its Components to produce auditable financial statements, and the failure to properly categorize and retire these systems will continue to impede the DoD's ability to achieve a clean audit opinion.

Replacing legacy financial and feeder systems also ensures network security and enables the DoD to consistently generate timely, accurate, and useful information. The DoD assumes significant risk to its operations and assets when system controls are ineffective. To increase the value of audit feedback, the DoD Components must consider the system audit findings and recommendations more broadly. For example, DoD Components should proactively incorporate corrective action plans into other systems. Simply addressing a finding in one area or Component is not enough. Rather, DoD Component leadership must ensure that the vulnerabilities identified in one system do not exist in other systems.

While the DoD prioritized remediating certain system material weaknesses the last 3 years, the DoD has not significantly improved its systems. Consequently, the DoD OIG reissued four system-specific material weaknesses in FY 2021.

ACCOUNTING FOR SUPPLEMENTAL CONTINGENCY FUNDING

The DoD routinely faces contingencies and unbudgeted needs based on its global mission. While DoD personnel can plan in anticipation of potential contingencies, they cannot budget for them before they occur. In the case of a contingency, the DoD must quickly realign funds and resources unless Congress appropriates funding specifically for the contingency. Generally, supplemental funds face higher levels of scrutiny due to the amount and time-sensitive nature of the contingency. For example, in the past few years the DoD responded to contingencies such as the COVID-19 pandemic, Operation Allies Welcome, and the conflict in Ukraine. The DoD received $15.6 billion for the COVID-19 pandemic, $8.5 billion for Operation Allies Welcome, and $34.4 billion for Ukraine as of October 2022. The DoD continues to provide weapon systems, supplies, and munitions to Ukraine.

[52] The Department of the Air Force started to transition users to the new system in 2005 and as of the end of FY 2022, the transition is not complete.

Due to current material weaknesses associated with its business processes and legacy systems, the DoD has faced challenges in accurately tracking and reporting these supplemental funds and resources using existing processes. As an example, the DoD OIG determined that Defense Health Agency (DHA) personnel did not accurately report $1.1 billion in Coronavirus Aid, Relief, and Economic Security (CARES) Act funding. Specifically, DHA personnel recorded the CARES Act funding in the same account as the annual appropriation instead of using the required emergency account. By not reporting the funds as emergency funds and combining the funds with the annual appropriation, DHA personnel were unable to determine which set of funds they used, causing inaccurate reporting, and increasing the risk of using more CARES Act funds than appropriated.

Recently the DoD has shown incremental progress when accounting for supplemental, contingency funding. In July 2022, the DoD OIG determined that personnel from the Office of the Under Secretary of Defense (Comptroller)/ Chief Financial Officer, DoD, were taking actions to help ensure that the DoD Components are aware of, and are completing, the reporting requirements for the Ukraine supplemental funds.[53] The DoD OIG determined that personnel from the Under Secretary's office held weekly meetings with the DoD Components to discuss the expectations and requirements related to Ukraine supplemental funds and implemented some best practices identified while accounting for CARES Act pandemic funds.

CONCLUSION

The road to a clean audit opinion is long. The DoD has been working toward a clean opinion for more than 30 years and estimates that it will not obtain a clean opinion for at least another 7 years. The DoD has massive undertakings involving long-term corrective action plans stretching to the latter part of this decade. As outlined in its June 2022 FIAR Report, the DoD noted its current progress and acknowledged the significant amount of work remaining.[54] To make the progress necessary to achieve a clean audit opinion, all levels of the DoD must remain diligent in their efforts to develop and implement corrective action plans for identified findings and recommendations, especially those that improve the production of reliable financial information.

[53] Report No. DODIG-2022-112, "Management Advisory: The DoD's Use of Ukraine Supplemental Appropriations Act, 2022 Funds," July 8, 2022.

[54] For a comprehensive list of work remaining, see June 2022 DoD Financial Improvement and Audit Remediation Report section II. Status of Corrective Actions.

Soldiers participate in 2022 DIAMOND SABER exercise at Fort Dix, New Jersey, which prepares finance personnel to conduct funding, payments, disbursing, accounting and auditability operations in an expeditionary environment.

Source: The U.S. Army.

Sailors secure an oil boom to a pier during oil spill response training in Sasebo, Japan. (U.S. Navy photo)

Challenge 5. Adapting to Climate Change, Accelerating Resilience, and Protecting the Environment

INTRODUCTION

The DoD has identified climate change as a major national security issue that will increase operational demands, degrade installation and infrastructure resilience, create health risks, and require changes in plans and equipment. The DoD is already feeling the effects of climate change, with increasing intensity and frequency of hurricanes, wildfires, floods, and droughts impacting DoD facilities. At the same time, the effects of DoD operations can harm the environment and the health and safety of DoD and non-DoD personnel, as evidenced by fuel leaks at the Red Hill Bulk Fuel Storage Facility at Joint Base Pearl Harbor-Hickam, Hawaii, and the presence of per- and polyfluoroalkyl substances, commonly called PFAS chemicals, in groundwater around military installations. Consequently, the DoD is working to enhance resilience to climate effects and reduce greenhouse gas emissions and their impact on the environment.

In September 2021, the DoD released its Climate Adaptation Plan, a roadmap to ensure the DoD maintains the ability to operate under changing climate conditions, while preserving operational capability and enhancing and protecting the natural and man-made systems essential to the DoD's success.[55] The DoD's Climate Adaptation Plan is ambitious given the DoD's current carbon footprint, operational requirements, and fiscal constraints. There are unique barriers associated with operationalizing the plan's five lines of effort (LOE)—this chapter focuses on the first three LOEs.

OPERATIONALIZING THE CLIMATE STRATEGY

Climate change is reshaping the geostrategic, operational, and tactical environments with significant implications for U.S. national security and defense. Increasing temperatures; changing precipitation patterns; and more frequent, intense, and unpredictable extreme weather conditions caused by climate change are exacerbating existing risks and creating

[55] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Department of Defense Climate Adaptation Plan," September 1, 2021.

new security challenges for U.S. interests."[56] The Climate Adaptation Plan, associated Military Departments' climate plans, and the DoD Climate Adaptation Plan 2022 Progress Report highlight the DoD's strategic goals, risks, and key performance measures.[57]

LOE 1: CLIMATE-INFORMED DECISION-MAKING

A climate-literate workforce is a key enabler to integrating environmental factors into the DoD's planning and governance processes. The DoD is integrating climate literacy into professional development and advanced training, but it will take time to develop expertise across the DoD. Personnel at all levels must understand the principles and effects of climate change to properly incorporate them into everyday operations, regional engagement and logistics plans, and doctrine. The DoD has established multiple working groups focused on strategies to improve climate literacy and enterprise decision making.

As part of enterprise decision making, the DoD conducts climate assessments that analyze climate effects on military installations, missions, and capabilities. Climate assessments must be based on the best available, validated, and actionable climate science that informs the most likely climate change outcomes.[58]

These evolving assessments must be informed by experts in the DoD workforce who are using artificial intelligence and simulations to analyze relevant data from across the DoD, other government agencies, and our allies. Reliable data is imperative to understanding the effects of climate change and identifying the changes needed to enhance DoD installations and infrastructure resilience. Planners must examine, and mitigate as necessary, any potential impacts on supply chains, infrastructure, funding, and operational readiness. Additionally, as DoD leaders prioritize and approve resources for climate initiatives, the DoD needs to effectively manage deliverables and outcomes. The DoD OIG has two ongoing audits focused on facility resilience and adaptation planning to address climate change and extreme weather at installations in the southeastern United States and California.

The DoD must quickly build climate literacy and integrate climate effects into operational and installation planning. DoD leaders must support these efforts by continuing to improve climate literacy, maximizing the use of environmental data modeling and establishing performance metrics to ensure the DoD achieves its climate-related goals.

LOE 2: TRAIN AND EQUIP A CLIMATE-READY FORCE

The DoD must be able to train safely and fight in every environment, with equipment that can operate in extreme conditions. Mission success will depend on planning and operational adaptability that accounts for climate-related complexities and ensures that equipment can operate in extreme environments.

The increasing frequency and duration of high temperatures and little or no rainfall have created drought conditions, which can prevent the DoD from conducting field exercises due to

---

[56] Office of the Under Secretary of Defense for Policy (Strategy, Plans, and Capabilities), "Department of Defense Climate Risk Assessment," October 2021.

[57] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Department of Defense Climate Adaptation Plan 2022 Progress Report," October 4, 2022.

[58] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Department of Defense Climate Adaptation Plan," September 1, 2021. DoD Directive 4715.21, "Climate Change Adaptation and Resilience," effective January 14, 2016, and updated on August 31, 2018, ties climate change adaptation to mission readiness and states that the DoD must be able to adapt current and future operations. To meet the requirements of the Directive, the DoD performs climate assessments. In a climate assessment, the DoD must identify the effects of climate change on the DoD mission and consider those effects when developing plans and implementing procedures.

personnel safety concerns and increased risk of wildfires. Water scarcity can also adversely affect food sources, and, in a worst case scenario, could stress economic and social conditions in unstable countries, resulting in civil unrest and humanitarian crises. Similarly, rising sea levels related to the melting polar ice caps and the resulting storm surges are increasingly affecting areas not previously at risk. High winds and flooding can cause significant damage to property and equipment, disrupt normal operations, and degrade readiness. Melting ice also complicates the security environment in the Arctic, opening new areas for adversaries to explore and exploit.[59] The DoD's participation in annual exercises in the Arctic provides valuable experience and lessons-learned for conducting multi-domain operations while simultaneously demonstrating the U.S. commitment to a free, peaceful, stable, and open Arctic region.[60]

The DoD is also challenged to improve awareness of analytical tools available to aid DoD climate adaptation efforts, such as identifying the climate hazards to which DoD installations are most exposed. This is difficult because of constantly changing data. A recent DoD OIG evaluation found that U.S. military installation leaders at six Arctic and sub-Arctic installations did not conduct installation resilience assessments and planning required by DoD directive and public law.[61] The installation leaders were unfamiliar with military installation resilience planning requirements, processes, and tools. Therefore, they did not comply with requirements to identify current and projected climate-related environmental risks, vulnerabilities, and risk reduction measures, or incorporate these considerations into plans and operations.

The DoD must continue to incorporate data into environmental threat analyses, train in all climates or simulate operations to determine how to best operate in changing climates and extreme weather, and continue to develop and field equipment designed to withstand extreme environments.

LOE 3: RESILIENT BUILT AND NATURAL INFRASTRUCTURE

The DoD's readiness and operational success depend on the resilience of its infrastructure in changing climate conditions. The DoD has over 450 military installations in the United States and over 750 military installations in more than 80 nations. Each installation has unique characteristics and may have unique vulnerabilities due to the effects of climate change. The effects of climate change have highlighted the need for the DoD to develop installation resilience plans.[62]

Historically, the DoD has struggled to maintain facilities, resulting in a maintenance and improvements backlog. Maintenance delays make facilities more vulnerable to premature deterioration, can introduce potential health

[59] Office of the Under Secretary for Policy (Strategy, Plans, and Capabilities), "Department of Defense Climate Risk Assessment," October 2021.

[60] Secretary of Defense prepared remarks to Senate Committee on Appropriations Subcommittee on Defense, May 3, 2022.

[61] Report No. DODIG-2022-083, "Evaluation of the Department of Defense's Efforts to Address the Climate Resilience of U.S. Military Installations in the Arctic and Sub-Arctic," April 13, 2022. DoD Directive 4715.21, "Climate Change Adaptation and Resilience," January 14, 2016, and Section 2864, title 10, United States Code (10 U.S.C. § 2864 [2020]), "Master Plans for Major Military Installations."

[62] Military installation resilience is defined in 10 U.S.C. § 101(e (8) as: "the capability of a military installation to avoid, prepare for, minimize the effect of, adapt to, and recover from extreme weather events, or from anticipated or unanticipated changes in environmental conditions, that do, or have the potential to, adversely affect the military installation or essential transportation, logistical, or other necessary resources outside of the military installation that are necessary in order to maintain, improve, or rapidly reestablish installation mission assurance and mission-essential functions."

issues, and increase the cost of repairs. The DoD must determine whether to invest in maintaining and upgrading current facilities and infrastructure or in new, more resilient facilities and infrastructure.

According to a January 2022 GAO report, the DoD manages more than 500,000 facilities worldwide with an estimated aggregate replacement value of about $1.3 trillion.[63] The GAO found that nearly 30 percent of DoD facilities have exceeded their expected lifespans, with many facilities dating to World War II. These aging facilities may present health and safety concerns. In 2020, the DoD reported $137 billion in deferred maintenance and that it expects the backlog to increase.

This line of effort includes updating existing infrastructure to current building standards to ensure continuity of operations, developing installation resiliency plans, and seeking alternative energy solutions to ease the DoD's requirement for petroleum–all of which are reflected in the Military Services' climate adaption plans.[64] According to the Army Climate Strategy, the Army has 950 renewable energy projects that supply 480 megawatts of power to the Army.[65] The Army plans to continue deploying microgrids, develop hybrid options as a bridging solution to fielding an all-electric Army non-tactical vehicle fleet by 2035, and pursue enough renewable energy generation and battery storage capacity to self-sustain critical missions on all Army installations by 2040.[66] Similarly, the Navy wants to increase resilience through projects such as smart grids, microgrids, and increasing the efficiency of engines to reduce demand for fuel. The use of microgrids and hybrid and electric vehicles requires significant infrastructure investments and trusted sources of supply to provide sufficient raw materials and batteries to the DoD. Furthermore, the DoD must conduct robust testing to ensure that these solutions will work in austere conditions and ensure acquisition planning includes programming for sustainment.

The DoD has steadily increased the use of the Defense Climate Assessment Tool to assess exposure, sensitivity, and adaptive capacity of DoD installations.[67] The tool uses data from past extreme weather events (such as hurricanes and tornados) and the effects of future changes in sea levels, riverine flooding, drought, heat, land degradation, energy demand, and wildfires to produce hazard indicators. The hazard indicators from the Defense Climate Assessment Tool help shape installation resiliency plans, inform infrastructure project prioritization and funding decisions, and improve the DoD's long-term strategies include environmental factors. The DoD plans to complete climate assessments for all major U.S. installations and overseas installations by January 2023.

The DoD must also ensure sustainability of natural infrastructure in and around DoD installations and preserve the health of the local ecosystem. This requires cooperation

63 Report No. GAO-22-104481, "Defense Infrastructure: DoD Should Better Manage Risks Posed by Deferred Facility Maintenance," January 31,2022.

64 Department of the Army, "United States Army Climate Strategy," February 2022.

Department of the Navy, "Department of the Navy Climate Strategy," May 2022.

Department of the Air Force, "Department of the Air Force Climate Action Plan," October 2022.

65 Office of the Assistant Secretary of the Army (Installations, Energy, and Environment), "United States Army Climate Strategy," February 2022.

66 A microgrid is an independent energy system that serves a specific local area, can use multiple sources of renewable energy, and is controlled by a software-based system. Microgrids are usually connected to traditional electric grids, but can operate independently during an earthquake or other natural disaster.

67 Defense Climate Assessment Tool Fact Sheet, April 2021.

with local, state, and Federal partners. These partnerships will enhance environmental remediation and protections, while ensuring the DoD's continued access to training ranges; and ensure the health and safety of DoD personnel, family members, and the public living around military installations.

CONCLUSION

DoD operations and installations are continually exposed to the risks and effects of climate change, which can create operational challenges and degrade readiness. In a February 2022 Message to the Force, the Secretary of Army wrote, "[a]s the planet warms, the polar ice caps melt, and extreme weather becomes commonplace, the Army must adapt its installations, acquisition programs, and training to be able to operate in a changing environment and reduce greenhouse gas emissions." Although the DoD has long recognized the potential impacts of climate change, actions to improve DoD structures, improve energy resiliency, and protect the environment remain unaccomplished. The DoD must effectively integrate climate considerations into its operational plans, programs, policies, and tools to build resilience against the effects of climate change and ensure future readiness.

Team members at the McKinley Climatic Laboratory at Eglin Air Force Base, Florida, use machines to create snow to prepare for environmental testing.

Source: Arnold Engineering Development Complex Public Affairs.

A Soldier reunites with family at Fort Bragg, North Carolina, after returning home from deployment. (U.S. Army photo)

Challenge 6. Protecting the Health and Wellness of Service Members and Their Families

INTRODUCTION AND OVERVIEW

The DoD's most essential resource is its people. Ensuring that 2 million Service members and their 2.6 million family members are taken care of is critical to readiness and maintaining trust and confidence in the DoD.

The DoD has made some progress to address the health and wellness needs of Service members and families, such as issuing a revised Military Housing Privatization Initiative Tenant Bill of Rights, reducing prices at commissaries, increasing the basic allowance for housing in select areas, and expanding spousal employment. However, according to a March 2022 GAO report, the DoD continues to face challenges in improving the quality of housing for Service members and their families, partially due to the inability to make changes to projects without agreement from private companies.[68] The DoD's challenges are not limited to quality housing and include many concerns, including those we discuss this year—readiness of health care personnel, mental health services, substance misuse, suicide prevention, and women's health.

DEGRADED READINESS OF HEALTH CARE PERSONNEL

The COVID-19 pandemic increased the operational tempo for DoD health care personnel, contributing to staffing shortages, staff burnout, and degraded personnel readiness. The U.S. Surgeon General recognizes that a range of factors affect burnout rates among health workers, including excessive workloads, administrative burdens, limited input in scheduling, and lack of organizational support. These factors affect the readiness and welfare of DoD health care personnel.

In an August 2021 congressional hearing, the Chief of Naval Operations stated that pandemic-related deployments and support for the nationwide vaccination effort resulted in reduced health care services

[68] Report No. GAO-22-105866, "Privatized Military Housing: Update on DOD's Efforts to Address Oversight Challenges," March 31, 2022.

for beneficiaries.[69] In April 2022, the DoD OIG reported that existing health care staff shortages were exacerbated by a combination of increased workload and availability of staff caused by the DoD's response to the pandemic and continued support for global missions.[70] The DoD is working on actions to implement the DoD OIG's recommendations from the April 2022 report, such as updating policy to include maximum consecutive hours to be worked, maximum shifts per week, and coverage of duties when absent. Continuing its oversight of this important problem, in July 2022, the DoD OIG announced a multi-Federal agency OIG project that seeks to inform decision makers of the extent of health care staff shortages and best practices used by each Federal agency, including the DoD, to attract and retain staff. In this review, the DoD OIG will also determine the effect of health care staff shortages on military readiness and strategies to mitigate shortages during future pandemics.

A May 2022 RAND Corporation research report found that burnout rates among military health care provider populations in the DoD were above 25 percent across multiple studies.[71] According to RAND, military health care provider burnout warrants in-depth qualitative research and its mitigation should be an organizational priority. Section 731 of the FY 2021 National Defense Authorization Act requires the Secretary of Defense to create a COVID-19 Military Health System Review Panel and to submit a report to Congress in June 2021 that included recommendations for force structure and staffing. The DoD submitted an interim report to Congress on April 22, 2022, and is working to submit a final report by December 30, 2022.

Maintaining adequate health care staffing and taking measures to avoid staff burnout are critical to medical readiness and delivering quality health care. Additionally, understanding the pandemic's impact on the welfare of health care personnel will help to ensure that the DoD can meet the quality care standards that DoD Service members and beneficiaries deserve.

CONTINUED SHORTFALLS IN MENTAL HEALTH SERVICES

Before the COVID-19 pandemic, the DoD faced shortfalls in meeting the demand for mental health services. The pandemic highlighted the impact of the shortfalls on DoD beneficiaries, especially as demand increased. In January 2022, in response to a congressional request, the DoD estimated that it needed an additional 1,050 behavioral health providers to meet the pre-pandemic demand for behavioral health services.[72] The DoD will need to reassess its requirements based on pre-existing need and increased demand resulting from the COVID-19 pandemic.

Research to determine the effect of the pandemic on the mental health of Service members and their families shows a rising need for mental health care. In its 2021 Health of the Force report, the Army highlighted the direct effects of the pandemic on the mental health of Service members, finding that most Soldiers reported COVID-19 stressors, fears, and concerns.[73] The report stated that half of Soldiers reported negative financial impacts because of the

[69] Statement of the Chief of Naval Operations before the House Appropriations Subcommittee on Defense, April 29, 2021.

[70] Report No. DODIG-2022-081, "Evaluation of Department of Defense Military Medical Treatment Facility Challenges During the Coronavirus Disease-2019 (COVID-19) Pandemic in Fiscal Year 2021," April 5, 2022.

[71] RAND Corporation, "Burnout: Definition, Prevalence, Risk Factors, Prevention, and Intervention Literature Reviews," 2022.

[72] Behavioral Health Requirements of the Department of Defense. USD(P&R) Response to House Report 116-442, Page 150, Accompanying H.R. 6395, the "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," January 12, 2022.

[73] U.S. Army Public Health Center, "2021 Health of the Force," April 18, 2022.

pandemic and those Soldiers were more likely to screen positive for depression or anxiety. During the pandemic, military spouse unemployment worsened, as 17 percent of military spouses reported having lost their job. Compounding financial stresses, the 6 percent of military families who relied on free or reduced cost lunch programs were at risk of food insecurity due to school closures.

According to an August 2020 report, the DoD OIG determined that the DoD did not consistently meet timeliness standards for access to mental health care for active duty Service members and their families.[74] For example, in June 2019, active duty Service members and their families referred to the TRICARE network at Naval Health Clinic Oak Harbor waited an average of 57 days for behavioral health counseling and therapy intake, and 79 days for psychiatry. Although the DoD agreed with the recommendations in the report, officials stated that implementation of corrective actions either were delayed by the COVID-19 pandemic or will be implemented when new TRICARE managed-care support contracts are awarded in 2023.

To help meet demand for mental health services over the past few years, the Defense Health Agency authorized the increased use of telehealth capabilities, as evidenced by increased expenditures for telehealth services from $4.0 million in FY 2019 to more than $150 million in FY 2020. The use of telehealth for mental health increased dramatically during the early stages of the pandemic and the overall use of mental health services increased through telehealth and in-person. The DoD OIG has an ongoing project to identify and describe potential program integrity risks associated with telehealth services offered through the DoD TRICARE program.[75]

As the Military Health System evolves, the DoD must continue to assess the pandemic's effects on mental health and develop and implement policies, programs, and initiatives that will ensure it can provide appropriate care to its Service members and beneficiaries.

ENCOURAGING TREATMENT FOR SUBSTANCE MISUSE

Effectively identifying and treating Service members with substance misuse problems remains a challenge for the DoD. A DoD OIG report found that stigma exists surrounding the acceptance of behavioral health treatment and its perceived negative effect on a Service member's career.[76] Substance misuse refers to the harmful or hazardous use of psychoactive substances, including alcohol and illicit drugs. According to an October 2019 publication from the National Institute on Drug Abuse, while Service members used illicit substances at lower rates than the general population, binge drinking rates in the military exceeded those among the general population.[77] In March 2022, the DoD OIG determined that Military Service health care providers did not perform annual alcohol screenings in a timely manner, and the Defense Health Agency and Military Services did not provide timely intake assessments or treatment for alcohol misuse.[78] The DoD OIG additionally determined that the DHA and Military Services did not provide intake assessments or treatment

[74] Report No. DODIG-2020-112, "Evaluation of Access to Mental Health Care in the Department of Defense," August 10, 2020.

[75] DoD OIG Announcement Memorandum, "Evaluation of the Department of Defense's Telehealth Services," December 13, 2021.

[76] Report No. DODIG-2022-071, "Audit of Active Duty Service Member Alcohol Misuse Screening and Treatment," March 10, 2022.

[77] National Institute on Drug Abuse, "Substance Use and Military Life Drug Facts," October 23, 2019.

[78] Report No. DODIG-2022-071, "Audit Of Active Duty Service Member Alcohol Misuse Screening And Treatment," March 10, 2022.

for alcohol misuse in a timely manner according to DHA or Service guidance. Of the 270 cases reviewed, 36 percent of Service members who were diagnosed with an alcohol use disorder did not receive their recommended treatment within established 7- and 28-day timeframes. Additionally, in three instances, Service members who were diagnosed with an alcohol use disorder did not receive their recommended treatment.

Receiving treatment is important, but treatment is complicated by the associated stigma. The DoD has issued policy to address the stigma related to substance misuse treatment, but the negative perception persists. The August 2021 Veterans Affairs/DoD Clinical Practice Guideline states that asking Service members to come forward for treatment for alcohol misuse is complicated by DoD guidance that substance use treatment must occur during a formal enrollment in mandatory care with the Service member's commander being involved in treatment.[79] Additionally, personnel databases track Service member treatment, creating a stigma that assignments and career progression may be affected. The Army established a substance abuse treatment program in 2019, specifically for Soldiers who did not have alcohol-related disciplinary problems. The program has already produced positive results by increasing the readiness of Service members for potential deployment and by decreasing the rate of emergency services for substance misuse.

Addressing the stigma associated with seeking and receiving treatment for substance misuse will continue to challenge the DoD. Without effective solutions, the DoD risks the health and readiness of Service members who may benefit from treatment and are at an increased risk of harming themselves, others, or military operations.

SUICIDE PREVENTION EFFORTS IN THE DOD

The DoD has increased its efforts in the area of suicide prevention, and there was a 15-percent decrease in suicides from 2020 to 2021, according to the Defense Suicide Prevention Office.[80] However, there were still 328 active duty Service member suicides in 2021.[81] The FY 2021 National Defense Authorization Act required the use of multidisciplinary teams to review each death by suicide at the installation or command level. The review is an effort to gather more complete and accurate accounts of the lives and circumstances surrounding the Service members who died by suicide and to inform prevention efforts based on the lessons learned at the command.

Additionally, in March 2022, the Secretary of Defense established an independent panel to review suicides in the military focusing on nine installations, including three in Alaska and one in South Korea.[82] The panel, composed of experts across multiple disciplines, commenced its work in May 2022, and began visiting the bases in August 2022. The panel will look specifically at bases and commands with a high number of recent suicides, and will report any findings to the Secretary of Defense and Congress by early 2023.

[79] Department of Veterans Affairs and Department of Defense, "VA/DoD Clinical Practice Guideline for the Management of Substance Use Disorders," Version 4.0, August 2021.

[80] Defense Suicide Prevention Office, "Department of Defense (DoD) Quarterly Suicide Report (QSR) 4th Quarter, CY 2021."

[81] Under Secretary of Defense for Personnel and Readiness, "Department of Defense Annual Report on Suicide in the Military–Calendar Year 2021."

[82] Secretary of Defense Memorandum, "Establishment of the Suicide Prevention and Response Independent Review Committee," March 22, 2022.

The DoD OIG has evaluated the DoD's suicide prevention efforts. In 2021, the DoD OIG reported on the DoD's implementation of suicide prevention resources for transitioning Service members.[83] The DoD OIG found that the DoD's overall approaches and services for arranging continuity of care for transitioning Service members receiving mental health care within the DoD are insufficient, resulting in interruption of care for Service members transitioning their health care from the DoD to the Veteran's Health Administration. The break in care may put Service members at risk of not receiving the health care they need, including care for suicide prevention. Suicide prevention remains a priority for the DoD, and will be an area of oversight for the DoD OIG in FY 2023.

ADDRESSING WOMEN'S HEALTH ISSUES

The DoD faces the challenge of addressing health issues that uniquely affect female Service members and beneficiaries. The roles of female Service members have expanded to direct combat and more frequent deployments to austere environments. According to a 2020 Defense Health Board report, the DoD should do more to address the health challenges that female Service members face, such as musculoskeletal injuries, reproductive and urogenital tract conditions, postpartum depression, eating disorders, and sexual violence care.[84] Not addressing health care matters that impact women may affect how long women remain in the military or whether they volunteer to join in the first place. According to a poll conducted by the Office of People Analytics, just 5 percent of women aged 16 to 21 surveyed in the summer of 2021 said that they definitely would or probably would serve in the military in the next few years.[85]

The Defense Health Board report also stated that the physiological differences in men and women translate to differential performance and injury risk for some common military tasks. Considering these differences, in March 2022, the Army revised the Army Combat Fitness Test to better support gender- and age-normed performance by replacing an exercise that measures core strength in Soldiers.[86] The revision to the Army Combat Fitness Test is a positive step to address the physiological uniqueness of female Service members. However, there is still much work to be done in increasing access to gender-customized equipment, such as properly fitting sports bras, backpacks, protective armor, footwear, and insoles necessary to address musculoskeletal injury prevention in female Service members.[87]

Another area of women's health that warrants attention from the DoD is reproductive and urogenital care. According to the Defense Health Board report, urogenital conditions are among the top reasons for medical encounters and evacuations of deployed female Service members. Pregnancy, gynecologic concerns, and postpartum complications also present unique challenges to female Service members and beneficiaries. Although the Military Health System provides health care services to treat the majority of reproductive and urogenital conditions, there are still areas where the DoD can improve care, such as providing more preventative measures for deploying female

[83] Report No. DODIG-2022-030, "Evaluation of the Department of Defense's Implementation of Suicide Prevention Resources for Transitioning Uniformed Service Members," November 9, 2021.

[84] Defense Health Board, "Decision Brief: Active Duty Women's Health Care Services," November 5, 2020.

[85] Office of People Analytics, "Summer 2021 Propensity Update," May 18, 2022.

[86] U.S. Army Public Affairs, "Army Implements ACFT based on scores, RAND Study, and Soldier Feedback," March 23, 2022.

[87] Defense Health Board, "Decision Brief: Active Duty Women's Health Care Services," November 5, 2020.

A Soldier holds his daughter after a redeployment ceremony at Fort Stewart, Georgia, August 29, 2022.
Source: U.S. Army

Service members and providing more health care services for female Service members while deployed. The report acknowledges that the availability and scope of women's health services vary significantly and recommends the DoD standardize care services.

In addition, there is a stigma associated with obtaining mental health care for more women-specific conditions, such as postpartum depression, and for conditions diagnosed in both men and women, such as eating disorders. While the DoD has discussed postpartum depression in the Veterans Affairs/DoD Clinical Practice Guideline, there is no standard policy to address it.[88] Additionally, studies suggest perceived stigmatization and the career-ending consequences of an eating disorder diagnosis lead to under-reporting and under-diagnoses of eating disorder symptoms.[89] Variability in military screening protocols result in the stark differences in the reported prevalence of diagnosed eating disorders, and there is no specific policy from the DoD or Defense Health Agency on the preferred or required assessment of eating disorders.[90]

Finally, sexual violence and harassment remains an issue for female Service members. The DoD's continued inability to stop sexual violence may make recruitment difficult. The Defense Health Board pointed out that female Service members are more susceptible to sexual violence and that

[88] "VA/DoD, "Clinical Practice Guideline for the Management of Major Depressive Disorder," Version 3.0, 2016.

[89] Defense Health Board, "Decision Brief: Active Duty Women's Health Care Services," November 5, 2020.

[90] Ibid.

the low conviction rate following interpersonal or sexual violence can cause long-term negative effects on Service members' physical and psychological health if not addressed in an efficient and productive manner. Although the DoD is actively combatting sexual violence through a variety of programs and awareness campaigns, the problem persists.

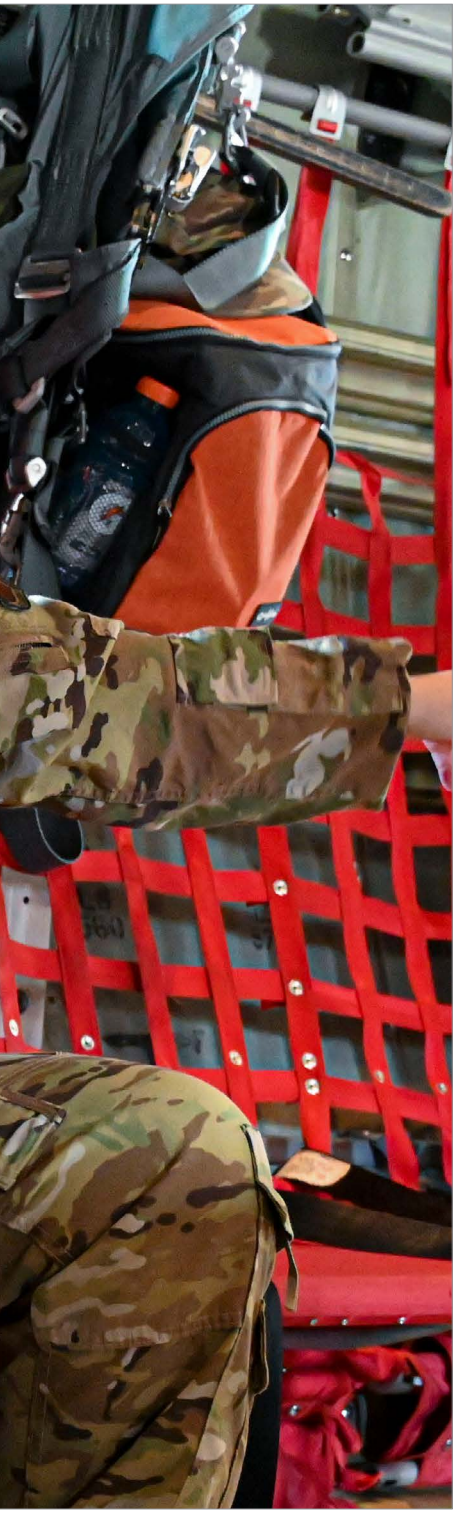
The DoD has established sexual and health education campaigns, established walk-in contraceptive clinics, and made the Decide + Be Ready mobile app available to female Service members.[91] Preventing sexual harassment and sexual assault and providing medical care for female Service members in deployed and non-deployed settings are essential to DoD readiness and the DoD's ability to recruit and retain female Service members.

CONCLUSION

Providing for the health and well-being of Service members and their families is critical to recruitment, retention, readiness, and bolstering trust and confidence in the DoD. The DoD must ensure adequate staffing of health care personnel and provide comprehensive care to women in deployed and non-deployed settings. The DoD must also work toward eliminating stigmas surrounding mental health and substance abuse care, and toward further reducing Service member suicides. Additionally, addressing health care matters that impact women may affect how long women stay in the military or whether they volunteer to join.

[91] Decide + Be Ready is a contraceptive decision-making mobile application for servicewomen.

A student with the "S.H.E. Can" STEAM Aviation Camp, a camp designed for students with an interest in aviation and seeks to empower young women to succeed in science, technology, engineering, art and mathematics disciplines, tour an Air Force C-130J Super Hercules. (U.S. Air Force photo)



Challenge 7. Recruiting and Retaining a Diverse Workforce

INTRODUCTION AND OVERVIEW

The DoD faces challenges recruiting and retaining a diverse workforce with the right mix of skills and capabilities to accomplish its mission. In April 2022, the Secretary of Defense stated, "Strategies mean little without the right people to execute them. To recruit and retain the most talented workforce, we must advance our institutional culture and reform the way we do business."[92] Having a diverse, highly skilled military and civilian workforce is essential to warfighting success. However, shifting societal norms and declining trust in, and familiarity with, the DoD have made it difficult for the DoD to meet its Total Force goals. Additionally, the DoD's recent efforts to improve diversity, equity, inclusion, and accessibility have exposed challenges related to strategic workforce planning and data collection.

RECRUITING THE DOD WORKFORCE

The DoD has long had to compete with the private sector to recruit top talent, but according to the Under Secretary of Defense for Personnel and Readiness, in recent years the competition has increased and the pool of young people eligible for Military Service has decreased.[93] The Under Secretary also stated that a strong economy has made it difficult to recruit qualified candidates and:

> A critical component to building enduring advantage is maintaining the flow of highly qualified recruits through the accession pipeline. We must invest in human capital initiatives to compete for, hire, develop, and retain highly skilled experts in the ever-changing national talent landscape.[94]

[92] Statement of the Secretary of Defense before the Senate Armed Services Committee, April 7, 2022

[93] Statement of the Under Secretary of Defense for Personnel and Readiness before the Senate Armed Services Committee Subcommittee on Personnel, April 27, 2022.

[94] Ibid.

RECRUITING FOR THE MILITARY

As of June 2022, the DoD reported that military recruitment was down 23 percent from the DoD's target number.[95] In August 2022, the Secretary of the Army stated that the Army had recruited about 52 percent of its goal (60,000 active duty enlistments) and would likely be short about 12,000 to 15,000 recruits by the end of FY 2022.[96] Ultimately, the Army was 15,000 short of the goal and the other Services had to reach into FY 2023 delayed entry candidate pools to meet FY 2022 goals.[97] While the COVID-19 pandemic complicated recruitment efforts, there were other significant contributing factors, such as a reduced desire to serve, reduced trust in DoD, and inability to meet physical fitness and medical requirements.

According to a 2021 Military Family Support Programming Survey of 8,638 active duty Service members, retirees, dependents, and veterans, 63 percent would recommend military life to someone considering joining the military, compared to 75 percent in 2019.[98] According to an NBC News.com article, another survey, found that only 13 percent of Americans in the target age range for recruiting had parents who had served in the military, down from about 40 percent in 1995.[99] Military Departments consider parents to be one of the biggest influencers for service. Additionally, in a different survey, military families identified poor housing conditions as a significant concern and a leading reason why they would not recommend joining the military.[100]

In addition to data indicating a reduced interest in serving, the DoD's screening for physical fitness, medical, education, and drug use further reduces the number of potential recruits. In May 2022, the Army Chief of Staff testified before Congress that only 23 percent of Americans ages 17 to 24 are qualified to serve without waivers, compared to 29 percent in prior years.[101] According to a September 2022 Army Times article, recent Army data showed that 70 percent of potential recruits are disqualified due to obesity, low test scores, or drug use.[102] In prior years, disqualifications ranged from 30 to 40 percent. The data showed that the propensity for women to serve also declined from 10 percent in 2018 to 5 percent in 2021.

RECRUITING FOR A CIVILIAN WORKFORCE

Improving recruitment and retention of the civilian workforce is one of three Agency Priority Goals outlined in the DoD's Strategic Management Plan for FYs 2022 – 2026. The DoD competes for talent with the private sector, where additional benefits and flexibilities can be used to recruit the highly qualified workers it seeks. To be more competitive with the private sector, the DoD uses direct hire authorities and pay flexibilities to fill positions within critical job sectors, such as finance, cybersecurity, science, and technology. The supplemental pay flexibility allows science and technology reinvention laboratories to

95 NBC News.com, "Every branch of the military is struggling to make its 2022 recruiting goals, officials say," June 27, 2022.

96 CNBC.com, "The Army has so far recruited only about half the soldiers it hoped for fiscal 2022, Army secretary says," August 12, 2022.

97 Stars and Stripes, "Army misses recruiting goal; other services squeak by," October 1, 2022.

98 Military Family Advisory Network, "2021 Military Family Support Programming Survey," July 2022.

99 NBC News.com, "Every branch of the military is struggling to make its 2022 recruiting goals, officials say," June 27, 2022.

100 Military.com, "Military Families Less Likely to Recommend Joining Up, Survey Finds," July 14, 2022.

101 Statement of the Department of the Army before the Senate Committee on Armed Services, May 5, 2022.

102 Army Times, "Test scores drop, disqualification rates rise at Army recruiting shops," September 15, 2022.

independently establish supplemental pay rates based on market conditions to help attract, recruit, and retain a high-caliber workforce. Still, the incentives may not be as attractive as private-sector compensation, especially in emerging mission areas, such as hypersonics, cybersecurity, and data science.

The DoD must continue updating its policies and programs to recruit qualified individuals in mission-critical areas, such as career and technical education and science, technology, engineering, and math (STEM), and achieve its strategic human capital goals and operational requirements. The DoD STEM Strategic Plan for FY 2021 – FY 2025, published in February 2021, establishes a vison to, "Inspire, cultivate, and develop exceptional STEM talent through a continuum of opportunities to enrich our current and future DoD workforce poised to tackle evolving defense technological challenges."

The Office of the Under Secretary of Defense for Research and Engineering is leading a holistic approach, which includes K-12 programs, partnerships with universities, and recruitment incentives. The DoD OIG has an ongoing project on post-secondary DoD STEM education programs that will, in part, assess the impact of the programs on the STEM career and internship candidate pool.

The DoD must improve the general public's awareness of opportunities and benefits of civilian service in the DoD. In a 2022 study, the RAND Corporation found that most prospective Army civilian employees were unaware that civilian jobs with the Army even exist, and many held misconceptions about Army civilian employment.[103] The recommendations of the study were to raise awareness of Army civilian job opportunities, prepare recruiting and hiring officials to allay potential applicants' misperceptions about Army civilian employment (involuntary deployment and exposure to combat), and strengthen the Army Civilian brand. The report recommended emphasizing career and geographic mobility; a wide, diverse range of potential careers; job security and stability; good benefits; good work-life balance; and a chance to serve Soldiers and the Nation.

RETAINING THE DOD WORKFORCE

In addition to the challenges of recruiting new talent, the DoD continually faces retention issues in the Total Force. Some elements discussed in the previous section on recruiting are also relevant to the DoD's ability to retain existing talent. According to the Under Secretary of Defense for Personnel and Readiness, retention has been impacted by a tight labor market, high operational tempo, compensation constraints, and lack of career-broadening experiences and training for civilians.[104]

RETAINING SERVICE MEMBERS

The DoD Strategic Management Plan established several goals focused on addressing retention of Service members. In a September 22, 2022 memorandum, the Secretary of Defense applauded the DoD's progress in taking care of the force, but wrote that more could be done for Service members and their families. The memorandum outlined actions that the DoD has taken, such as supporting a 4.6 percent basic pay increase, temporarily increasing basic housing allowances in high cost areas, fully funding commissaries, increasing accountability in response to sexual harassment and assault,

[103] RAND Corporation, "Improving the Department of the Army's Marketing for Recruitment, Hiring, and Retention of Civilians in Critical Occupations," 2022.

[104] Statement of the Under Secretary of Defense for Personnel and Readiness before the Senate Armed Services Committee Subcommittee on Personnel, April 27, 2022.

improving availability and reducing costs of child care and health care, and expanding spousal employment flexibilities.

Despite these initiatives, the DoD still faces challenges retaining Service members in specialties, such as cybersecurity, intelligence, Special Forces, and communications. The DoD has traditionally offered reenlistment bonuses, special skills pay, and educational loan repayment, but it may need to try other non-traditional approaches. The U.S. Marine Corps' Inaugural Commandant's Retention Program for FY 2023 is a good example. It streamlined the retention process and enhanced incentives for the top-performing first-term Marines. As a result, 1,268 of the 2,468 Marines selected to participate as part of the program submitted for reenlistment, an increase of 92.7 percent compared to the prior year.

The DoD must adopt policies and programs to mitigate attrition and address critical skill gaps to ensure that the DoD is able to achieve mission-critical objectives and readiness goals in the future.

RETAINING CIVILIAN EMPLOYEES

In November 2021, the Deputy Secretary of Defense requested that the Defense Business Board (DBB) conduct an independent review to examine and recommend specific approaches and actions to improve talent management in the DoD civilian workforce. The DBB's report, issued in May 2022, made three key observations: (1) civilian development is not seen as a priority in DoD culture, (2) talent data is a strategic asset and the way the DoD approaches talent data lags behind the private sector and is flawed, and, (3) the organizational structure of the Under Secretary of Defense for Personnel and Readiness is not postured to manage talent effectively.[105] The report cited the DoD's "outdated" talent management practices and lack of strategy to upskill or reskill civilians. The report also determined that there is a disparity in the DoD's investment in training and developmental opportunities for civilians, as compared to Service members. The DoD must change its current programs, processes, and systems to build an enduring advantage.

The report highlighted the Defense Acquisition University's efforts to address current training and education needs and strengthen professional development as a "bright spot." The university offers DoD personnel a wide range of online classes and continuous learning modules across a suite of disciplines, such as program management, finance, contracting, logistics, with training plans and career models to identify which classes lead to certification or positions at a higher grade.

The DBB's report further highlighted factors outside of the DoD's control, such as the domestic shortage of STEM workers, but emphasized that the DoD needs to prioritize talent management, shift its culture from managing the position to managing the person, and develop talent.

IMPROVING DIVERSITY AND INCLUSION

The Secretary of Defense made diversity and inclusion a priority for the DoD and reinforced that message many times. Promoting diversity and inclusion fosters innovation and ensures the work force best represents the population that it serves. The DoD has commissioned multiple working groups to address diversity and inclusion within the DoD, including the 2020 DoD Board of Diversity and

[105] Defense Business Board, "Strengthening Defense Department Civilian Talent Management," May 12, 2022.

Inclusion and the 2011 Military Leadership Diversity Commission (MLDC). Reports from these working groups presented similar observations and provided recommendations. In September 2022, the DoD OIG reported on the DoD's implementation of the recommendations from the 2011 MLDC.[106] In the report, the DoD OIG determined that the DoD and the Services implemented 6 of the 18 recommendations identified in the 2011 MLDC report, with the remaining 12 recommendations only partially implemented. Additionally, the DoD OIG determined that the DoD could not determine what progress has been made and what remains to be accomplished because of a lack of defined policy, roles and responsibilities, and data collection.

The recent establishment of the DoD Office of Diversity, Equity, and Inclusion, and several legislative mandates highlighted the DoD's lack of needed data related to diversity and inclusion. Section 554 of the FY 2021 National Defense Authorization Act requires the DoD to provide data to the DoD OIG, including allegations and related information pertaining to prohibited activities. However, the DoD has challenges collecting and managing data on prohibited activities. In addition, the DoD must improve its collection and use of racial, ethnic, and gender data. For example, in May 2022, the DoD OIG issued a management advisory to inform the Under Secretary of Defense for Personnel and Readiness that race codes used in the Military Health System Data Repository did not comply with DoD policies and that there were more than 36 million non-compliant records.[107]

CONCLUSION

The DoD's challenges with recruiting and retaining a diverse and inclusive Total Force affect its ability to meet strategic objectives. The DoD must implement cultural, organizational, and operational change to ensure that recruiting, retention, and diversity goals are met. The DoD must adapt innovative approaches to attract critical skillsets; better manage DoD talent by providing growth and development opportunities, including upskilling and reskilling; and continue to focus on fostering a diverse and inclusive Total Force. A civilian and military workforce that mirrors the diversity of the American people only strengthens the DoD.

[106] Report No. DODIG-2022-144, "Evaluation of the DoD's Implementation of the Military Leadership Diversity Commission's 2011 Report Recommendations and the DoD Diversity and Inclusion Strategic Plan for 2012 to 2017," September 30, 2022.

[107] Report No. DODIG-2022-099, "Management Advisory: The Military Health System Data Repository Contained Noncompliant Race Coding Values and Categories," May 24, 2022.

Tactical Air Control Party Airmen from the 1st Air Support Operations Group utilize data links established between Precision Strike Teams and the Air Operations Center to relay real-time targeting information to A-10C Thunderbolt II pilots as part of Exercise CHAOS QUAKE, Moody Air Force Base, Georgia. (U.S. Air Force photo)

Challenge 8. Accelerating the Transformation to a Data-Centric Organization

INTRODUCTION AND OVERVIEW

The DoD is among the world's largest producers and consumers of data. No other organization has a broader mission or scope. The DoD conducts transactions in areas such as joint all-domain operations, acquisition and sustainment, budget and financial management, intelligence and security, personnel and readiness, policy, reform, and research and engineering. The DoD has the world's largest workforce, is one of the largest health care providers, operates a multibillion-dollar global supply chain, and manages one of the largest inventories of facilities and installations. Every DoD function, policy, program, or activity can benefit from the effective use of data.

The DoD's ability to improve outcomes related to performance, financial management, support to Service members and their families, and many other areas rests on the availability of reliable data. Given data's importance, the DoD must treat data as a strategic asset and prioritize its management. To accelerate its transformation to a data-centric organization, the DoD must create a data-informed culture, operationalize the DoD data strategy, and keep pace with data innovations and best practices.

CREATING A DATA-INFORMED CULTURE

Building a data-driven culture involves changing the mindset, instincts, and habits of the DoD workforce. A data-informed culture understands that data and reporting are not the result; rather, the value of data comes from exploring it, analyzing it, and developing information from it to improve decision speed and outcomes. Successful outcomes rely on a performance-based culture, availability of accurate and comprehensive data sources, and a willingness to incrementally improve over time. The enhanced use of data can also create advantages from otherwise unanticipated or secondary uses of existing data sets. This cultural change requires commitment from leadership, a shared vision with specific objectives, and effective communication.

In May 2021, the Deputy Secretary of Defense issued a memorandum, declaring data a strategic asset and stressing that leaders must ensure data are "visible, accessible, understandable, linked, trustworthy, interoperable, and secure."[108] The memorandum directed the DoD to apply five data decrees and several actions to accelerate the DoD's enterprise data edge. The five data decrees focus on sharing data, publishing data assets, using automated data interfaces, storing data, and implementing best practices. The memorandum further communicated the commitment and expectations of senior leadership and outlined the responsibilities and authorities of the DoD Chief Data Officer, a position created in 2018.

In 2022, the DoD established the Chief Digital and Artificial Intelligence Officer (CDAO) position to further support the data strategy.[109] The CDAO reports directly to the Deputy Secretary of Defense and is the senior official responsible for "strengthening and integrating data, artificial intelligence, and digital solutions." The CDAO and CDO are responsible for accelerating the DoD's transition to a data-centric organization.

The F-35 Program, a multiservice and multinational acquisition to develop and field a fifth-generation strike fighter aircraft, serves as an example of the barriers that the DoD must overcome to build a data-informed culture. In 2019, the DoD OIG determined that F-35 Program officials did not maintain a Government record of government-furnished property (GFP), including part names and quantities, unit acquisition cost, and location.[110]

For more than 16 years, the DoD did not implement procedures to properly account for and manage Government property. The prime contractor and its subcontractors maintained the only record of GFP. This impeded the DoD's ability to readily account for and manage assets, which could have affected the DoD's ability to meet its operational readiness goals. Although the DoD OIG recommended in 2019 that the F-35 Program Office perform a full inventory of GFP, as of October 2022, the inventory had not been completed.

OPERATIONALIZING THE DOD DATA STRATEGY

In 2020, the DoD published its first agency-wide data strategy.[111] The data strategy established the DoD's transition to being a "data-centric organization that uses data at speed and scale for operational advantage and increased efficiency." The data strategy replaced separate data strategies from DoD Components, incorporated principles and lessons learned from earlier strategies and prevailing expertise, and established seven goals for the DoD to become data-centric. It identified three focus areas for early progress: (1) joint all-domain operations, (2) senior leader decision support, and (3) business analytics.

The data strategy is an ambitious approach that requires Department-wide support and resources. The implementation of Joint All-Domain Command-and-Control (JADC2) and the Advancing Analytics platform, commonly referred to as Advana, offer insight into obstacles.

JADC2 is the DoD's concept to connect sensors and communications from all of the Military Services—Army, Marine Corps, Navy, Air Force,

[108] Deputy Secretary of Defense Memorandum, "Creating Data Advantage," May 5, 2021.

[109] Deputy Secretary of Defense Memorandum, "Establishment of the Chief Digital and Artificial Intelligence Officer," December 8, 2021.

[110] Report No. DODIG-2019-062, "Audit of Management of Government-Owned Property Supporting the F-35 Program," March 13, 2019.

[111] "DoD Data Strategy: Unleashing Data to Advance the National Security," September 30, 2020.

and Space Force—into a single network. It enables the Joint Force to "sense," "make sense," and "act" on information across the battlespace by quickly using automation, artificial intelligence, predictive analytics, and machine learning.[112] The JADC2 concept requires secure information sharing, common data standards and architectures, and unified and faster development and implementation processes. To date, the DoD has encountered challenges in maturing JADC2 due to policies, authorities, operational procedures, coordination, design, funding, and management.[113]

Advana is a data platform meant to help the DoD translate common enterprise data into actionable insights, decisions, and outcomes by making data widely accessible, understandable, and usable across the enterprise. Advana brings in information from 120 systems and provides access to enterprise data and structured analytics to tens of thousands of users. While Advana provides significant benefits to the DoD, it has also identified issues with completeness, accuracy, and standardization of source data. In FY 2021, the DoD OIG determined that DoD Component personnel could not reconcile the population of Defense agency transactions in Advana, including Fund Balance with Treasury transactions, to their respective financial statements.[114]

As discussed in the challenge on "Improving Financial Management and Budgeting," there are also complex layered accounting and financial feeder systems.[115] The DoD currently manages nearly 300 feeder systems, which often do not capture data in a standardized way or effectively integrate with other systems.

JADC2 and Advana support the aims of the data strategy, but they also offer lessons that can inform the way forward. Both efforts exposed challenges with data sharing and once the data is shared, it reveals challenges with the completeness, accuracy, and interoperability of the data.

KEEPING PACE WITH INNOVATION AND BEST PRACTICES

The DoD needs to keep pace with the increasing variety and sources of data. This need includes adjusting and modernizing the DoD's architecture, standards, governance, talent, and culture to use data effectively. It also includes identifying potential applications of data to feed innovation and improve business practices across activities. Keeping pace will be difficult because the DoD has traditionally invested in large, monolithic systems, programs, and processes to achieve economies of scale. Adopting agile practices, such as lean design, short product development cycles, and market validation, could be appropriate.

As previously mentioned, Advana is an example of the DoD integrating data innovation and best practices to derive value for the DoD. It supports new capabilities, such as GAMECHANGER, which is an artificial intelligence and natural language processing application. It can processes vast amounts of policymaking data to identify relevant higher guidance and department regulations within

112 Defense.gov, "DoD Announces Release of JADC2 Implementation Plan," March 17, 2022.

113 Nationaldefensemagazine.org, "Challenges Loom for Joint All Command and Control," August 12, 2020. CSIS.org, "Pathways to Implementing Comprehensive and Collaborative JADC2," September 27, 2022.

114 DoD OIG, "Understanding the Results of the Audit of the FY 2021 DoD Financial Statements," May 18, 2022.

115 Financial feeder systems include accountable property systems of record, sub-ledgers, and management information systems. These systems feed financial information via multiple processes including automated interfaces, manual interfaces, and journal vouchers. The DoD uses 299 feeder systems.

seconds. Advana also uses unattended Robotic Process Automation bots to gather information from feeder systems to automate processes and identify inconsistencies or errors in data. Therefore, the DoD has made strides to innovate and automate processes, but this trend needs to continue to further gain efficiencies in transforming data into a strategic asset.

CONCLUSION

The pace of the DoD's transformation to a data-centric organization will depend on its ability to overcome cultural barriers, effectively implement its data strategy, and adapt. Building a culture that treats data as a strategic asset, shares data and collaborates across organizational boundaries, and develops business processes and standards with data in mind, will take time. The implementation of the strategy will require measurable action plans and policies, focused management and accountability, and sufficient funding. The DoD's investment in Advana and other data initiatives, coupled with the adoption of JADC2, will position the DoD to capitalize on the benefits of data-informed decision-making. However, data analytics will not be fully effective until data quality and governance improve. It is encouraging that the DoD leadership recognizes that data producers must prioritize resources to make data accessible for broader consumption while also maintaining data quality.

The U.S. Army Engineer Research and Development Center's Cold Region Research Engineering Laboratory mathematician logs data during U.S. Northern Command Exercise ARCTIC EDGE 2022 at Joint Base Elmendorf-Richardson, Alaska

Source: The U.S. Army.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098