INSPECTOR GENERAL

U.S. Department of Defense

FISCAL YEAR 2022

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

Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

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 15, 2021

Each Inspector General (IG) is required by the Reports Consolidation Act of 2000 to prepare an annual statement summarizing what the IG considers to be the "most serious management and performance challenges facing the agency" and to assess the agency's progress in addressing those challenges. According to the law, each "agency head may comment on the IG's statement, but may not modify the statement." The IG's statement must be included in the Agency Financial Report.

The DoD Office of Inspector General (OIG) independently identifies these challenges based on a variety of factors, including our independent research, assessment, and judgment; previous oversight work completed by the DoD OIG and other oversight organizations; congressional hearings and legislation; input from DoD officials; and issues highlighted by the media that are adversely affecting the DoD's ability to accomplish its mission.

The FY 2022 Top DoD Management Challenges are reframed or updated from prior years. This year, the DoD OIG has individual challenges addressing environmental stresses, adapting acquisition and contracting management, and retaining and recruiting the workforce. In addition, the challenges related to technological dominance and data as a strategic asset, that were discussed last year, remain challenges to the DoD and are discussed as part of many challenges this year. Across all of the challenges identified, the DoD has been working to resolve or mitigate the challenge areas. In addition to describing the challenges, the DoD OIG also discusses the recent actions taken by the DoD to address these challenges; assesses the DoD's progress in each challenge area; and cites planned, ongoing, and completed oversight work related to the challenges.

This document is forward-looking. The DoD OIG uses this document in its oversight planning process, seeking to ensure that the DoD OIG's projects address the most significant performance and management challenges facing the DoD. These challenges are not listed in order of importance or by magnitude and all are critically important. The DoD OIG will continue to assess these challenges and conduct independent oversight 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. We look forward to working with the DoD to help address these important challenges.

Sean O'Donnell
Acting Inspector General

Sailors aboard Arleigh Burke-class guided-missile destroyer USS O'Kane (DDG 77) conduct a man overboard drill on June 23, 2021. The USS O'Kane was conducting routine maritime operations in the Pacific Ocean. (U.S. Navy photo)

Summary of Management and Performance Challenges Facing the DoD

FISCAL YEAR 2022

A Soldier with 1st Battalion, 1st Special Forces Group (Airborne), prepares to load a CH-53E Super Stallion with 1st Marine Aircraft Wing during Castaway 21.1 on Ie Shima, Okinawa, Japan, on March 17, 2021. (U.S. Marine Corps photo)

Executive Summary

Every year, the DoD OIG identifies the top management and performance challenges facing the DoD. These challenges are based on the DoD OIG's independent research, assessment, and judgment; previous oversight work and oversight work of other organizations; congressional hearings and legislation; input from DoD officials; and issues raised by the media. The DoD OIG also considers and assesses the DoD's progress in addressing these challenges. This annual report provides Congress and the DoD's civilian and military leaders with the DoD OIG's independent assessment of the management and performance challenges affecting the DoD.

The FY 2022 Top DoD Management Challenges are:

1. Maintaining the Advantage in Strategic Competition
2. Assuring Space Dominance, Nuclear Deterrence, and Missile Defense
3. Strengthening DoD Cyberspace Operations and Securing Systems, Networks, and Data
4. Reinforcing the Supply Chain While Reducing Reliance on Strategic Competitors
5. Increasing Agility in the DoD's Acquisition and Contract Management
6. Improving DoD Financial Management and Budgeting
7. Building Resiliency to Environmental Stresses
8. Protecting the Health and Wellness of Service Members and their Families
9. Recruiting and Retaining a Modern Workforce
10. Preserving Trust and Confidence in the DoD

The challenges are not listed in order of priority or importance, but are instead organized as follows. Challenges 1 through 3 relate to the DoD's mission and how it executes that mission across multiple domains. Challenges 4 through 6 relate to how the DoD buys and pays for what it needs to accomplish the mission. Challenge 7 is about the installations from which the DoD operates and how those installations must be protected. Finally, challenges 8 through 10 focus on the health, hiring, and composition of the DoD civilian and military workforce.

STRATEGIC ENVIRONMENT

The DoD operates across all domains—sea, land, air, space, and cyberspace—in an increasingly contested and complex environment. As the DoD continues to shift from counterterrorism to strategic competition, it must reaffirm and strengthen alliances and partnerships. Furthermore, to maintain or reassert a competitive advantage, the DoD seeks to balance modernization of legacy systems with investments in new technologies. Investing in and rapidly incorporating key capabilities is necessary to deter and defeat a range of national security threats from nation states to independent actors. With continued investment in new technologies and capabilities, the DoD must demonstrate that it is a good steward of taxpayer money by producing reliable financial statements and measuring the effectiveness of its investments.

The DoD also faces a challenging domestic environment, with continued health, social, and operational effects from the coronavirus disease–2019 (COVID-19) pandemic. The health and safety of DoD personnel remains a priority, as they face threats from substance abuse, climate change, exposure to environmental hazards, and poor housing conditions. In addition, DoD senior leaders, Congress, and the Administration have renewed or increased their focus on combating sexual harassment and sexual assault, disparate treatment, and extremism in the ranks.

The DoD faces a complicated strategic environment requiring its attention to each challenge in order to defend the United States while taking care of DoD personnel and their families. Furthermore, the DoD must ensure that it does not compromise the trust of the American people.

CHANGES FROM THE FY 2021 TOP DOD MANAGEMENT CHALLENGES

This year, the DoD OIG refocused and separated challenges from the FY 2021 Management Challenges. The DoD OIG chose to separate the discussion of challenges in the DoD's acquisition and contract management from the challenges in the DoD's supply chain and industrial base. The DoD OIG refocused last year's challenge on strengthening resiliency to nontraditional threats to hone in on climate change and other environmental stresses, while discussions of the COVID-19 pandemic occur in several challenges. The DoD OIG speaks to challenges in recruiting and retaining a modern workforce as a stand-alone challenge this year, where in past years it was integrated into multiple challenges. Finally, instead of separate challenges on building and sustaining the DoD's technological dominance and on transforming data into a strategic asset, the DoD OIG integrated these themes into other challenges.

Technological dominance and the collection and use of data remain important considerations for the DoD. Technological dominance is paramount for the DoD to succeed against strategic competitors that are investing heavily in new technologies, from major weapon systems to artificial intelligence. As the DoD becomes more interconnected through information sharing and cloud computing, the need for accurate data grows. Data and data systems permeate every aspect of the DoD and are integral to leaders making informed decisions for executing operations; deciding what to buy; conducting financial management and budgeting; and measuring effectiveness of DoD programs, processes, and operations. Throughout the challenges, the DoD OIG discusses the role and importance of technological dominance and data.

Several challenges from the FY 2021 Top DoD Management Challenges continue for FY 2022. These challenges include the continued shift to strategic competition, assuring space-based and nuclear operations, cybersecurity, financial management and budgeting, protecting the health and well-being of DoD personnel and Service members' families, and ensuring ethical conduct.

SUMMARY OF THE FY 2022 MANAGEMENT CHALLENGES

The DoD OIG considers these 10 challenges to be the most critical issues facing the DoD in FY 2022. The DoD OIG will use these challenges to inform its oversight work in the next fiscal year, as outlined in the DoD OIG FY 2022 Oversight Plan.

The first challenge, "Maintaining the Advantage in Strategic Competition," highlights the DoD's continuing need to maintain and build alliances and partnerships to counter aggression from strategic competitors. As the counterterrorism mission evolves, the DoD must find new ways to ensure that those security objectives are met while aligning resources to meet strategic competition objectives. Strategic competitors, including China and Russia, continue to expand their influence and reach across the Indo–Pacific, Arctic, Europe, Middle East, and Africa. Through U.S. and allied power projection, joint exercises, and operations, the DoD aims to deter aggression from strategic competitors. Maintaining the U.S. military's advantage while balancing strategic competition and countering global terrorism requires the DoD to focus on enhancing collaboration, developing skillsets and training for evolving missions, and advancing new technologies.

The second challenge, "Assuring Space Dominance, Nuclear Deterrence, and Missile Defense," highlights the DoD's challenges of investing in new capabilities in these areas while also sustaining legacy systems to protect U.S. national security interests. As legacy systems become more outdated and strategic competitors continue to expand their capabilities, it is increasingly important for the DoD to update and replace its systems with new technologies and capabilities. The DoD is challenged with ensuring that contractors provide timely replacements that are tested and effective and ensuring that DoD personnel maintain proficiency in legacy systems while learning to use new systems effectively.

The third challenge, "Strengthening DoD Cyberspace Operations and Securing Systems, Networks, and Data," focuses on the importance of having the right cyber capabilities, interoperable systems, and strong cyber hygiene. The DoD's ability to assess and protect its systems, networks, devices, and data is at risk of not keeping pace with adversaries' abilities to compromise DoD technology. The DoD aims to protect not only itself but also the supply chain and industrial base that support the DoD. Ensuring adequate cybersecurity requires that the DoD develop and field new capabilities and identify and remediate cyber vulnerabilities, but the DoD continues to struggle to accomplish this. Through recent innovations such as cloud computing, artificial intelligence, and fifth-generation (5G) technology, the DoD is focusing on deploying and using cutting-edge technology to maintain a competitive advantage.

The fourth management challenge, "Reinforcing the Supply Chain While Reducing Reliance on Strategic Competitors," addresses the vulnerabilities from decreased manufacturing in the United States. In key industries,

such as shipbuilding and microelectronics, domestic capabilities are insufficient or lack necessary resources, leaving the United States outpaced by foreign entities. The COVID-19 pandemic highlighted reliance on foreign sources of supply and reinforced the need for increased collaboration with domestic industries and U.S. allies for a more robust supply chain. The DoD has acted to reinforce the supply chain and support key industries through the use of unique authorities, such as the Defense Production Act. The vulnerabilities with small and midsize businesses that rely on DoD contracts require innovative solutions. Continued focus on important industries, partnerships with allies, and small and midsize businesses will be essential for a strong supply chain that can meet the DoD's needs.

The fifth challenge, "Increasing Agility in the DoD's Acquisition and Contract Management," recognizes the actions taken to reform the acquisition process and use unique types of agreements to increase agility and flexibility. Changes in recent years to expand the definition of a commercial item continue to make it difficult for the DoD to ensure that it is paying a fair and reasonable price for the items it buys. This difficulty in establishing that a price is fair and reasonable increases when there are limited suppliers or just one supplier for an item. Without adequate competition, the DoD may pay a higher price than it otherwise could. These reforms, agreements, and expanded definitions have produced mixed results and require data and analysis to measure their effectiveness and ensure that the DoD is achieving the desired results.

The sixth challenge, "Improving DoD Financial Management and Budgeting," addresses the longstanding financial management challenges that continue to impair the DoD's ability to produce timely and reliable financial statements. Through the annual audits, the DoD gains insights into how its systems, business practices, and processes hinder its ability to effectively conduct financial management and budgeting. For example, the DoD continues to use manual processes rather than automated and sustainable processes, which complicates financial and budget management because the DoD relies on more than 250 information systems. The DoD has made some progress in improving its financial management and budgeting, which resulted in auditors reducing or downgrading previously identified material weaknesses. However, a continued focus on implementing corrective actions, accountability, and ensuring accurate data and sustainable business practices is essential for addressing this longstanding challenge.

The seventh challenge, "Building Resiliency to Environmental Stresses," identifies the effects of environmental stresses on DoD training and operations and the health and safety of DoD personnel. Climate change, extreme weather, environmental pollutants, and environmental protections will continue to affect the DoD's ability to train and operate on land, sea, and in the air. Extreme weather events, such as freezing temperatures in normally warm parts of the United States and hurricanes, caused extensive damage to DoD infrastructure that is costly to repair. The DoD must respond to environmental stresses and ensure that it mitigates the risks and costs to DoD operations, military installations, and personnel.

The eighth challenge, "Protecting the Health and Wellness of Service Members and Their Families," highlights one of the most important

readiness factors for the DoD, the health of the Joint Force. The DoD continues to struggle with ensuring a medically ready force, maintaining required combat health care skills, providing adequate treatment for victims of sexual assault, and addressing behavioral health problems such as substance abuse and suicide. With the COVID-19 pandemic ongoing, and through lessons-learned, the DoD must continually evaluate the needs of medical workers and the facilities in which they work, and ensure that critical medical stock piles are replenished. Finally, military housing remains a concern, and the DoD continues to take actions to ensure that Service members and their families have access to a safe and well-maintained home.

The ninth challenge, "Recruiting and Retaining a Modern Workforce," discusses the importance of recruiting and retaining a modern and diverse workforce capable of addressing the DoD's many requirements. The DoD must compete with the private sector for personnel in the science and technology-related fields and needs the flexibility to attract and retain those skills. The DoD's need for talent in the cyber workforce is especially important as malicious actors continue to attack and exploit DoD systems and the DoD expands cyber operations. In addition, with the growing focus on diversity, the DoD must address the underrepresentation of women and minorities in senior leader positions in both the civilian and military workforce. A talented and diverse workforce will help the DoD prevail in protecting national security interests.

The tenth challenge, "Preserving Trust and Confidence in the DoD," focuses on the critical issues of sexual harassment and sexual assault, disparate treatment, and extremism within the DoD and their negative effect on how DoD personnel and the public perceive the Department. The DoD has struggled to combat sexual harassment and sexual assault in its ranks. The military has taken actions to reduce racial or ethnic bias in its promotion processes, but continued attention and assessment of actions taken is needed to mitigate disparate treatment. Finally, the DoD must continue to develop methods for reporting and identifying extremism in the ranks while considering how to respect free speech. There are cross-cutting factors that further undermine the DoD's progress in addressing these challenges. These factors include making progress in collecting and analyzing appropriate data, offering the right training and measuring that training's effectiveness, and ensuring transparency and accountability over the investigative processes for sexual assault and sexual harassment, disparate treatment, and extremism. By addressing these challenges, the DoD can strengthen the trust and confidence that DoD personnel and the public have in the DoD.

Soldiers from the 173rd Airborne Brigade rehearse exiting CH-47 Chinooks of the 12th Combat Aviation Brigade in preparation for night air assault missions during exercise Swift Response 21, part of the DEFENDER-Europe 21 series of exercises at Chech Airfield, Bulgaria, on May 11, 2021. (U.S. Army photo)

Challenge 1. Maintaining the Advantage in Strategic Competition

INTRODUCTION AND OVERVIEW

In a written statement for his January 2021 confirmation hearing, the Secretary of Defense said, "The continued erosion of U.S. military advantage vis-à-vis China and Russia, in key strategic areas, remains the most significant risk the [DoD] must address. If left unchecked, this continued erosion could fundamentally challenge our ability to achieve U.S. national security objectives—and limit [the] DoD's ability to underpin other U.S. instruments of power."[1] The U.S. Government must coordinate the elements of national power—including the diplomatic, informational, military, and economic sectors—to safeguard U.S. national interests and maintain the competitive advantage.

The Administration's Interim National Security Strategic Guidance, issued in March 2021, calls for the United States to renew its enduring advantages to meet today's challenges from a position of strength. Strategic competitors, principally China and Russia, have invested heavily in efforts intended to check U.S. strengths. China and Russia have made strides to influence and project power in the Indo–Pacific, Arctic, Europe, Middle East, and Africa, which must be countered by the DoD and its allies and partners. In addition to strategic competitors, the DoD faces the evolution of counterterrorism operations and the fall of the Afghanistan government. As the DoD continues to focus on strategic competition, it must evolve its counterterrorism operations, choosing where to maintain a presence and where to accept more risk.

To maintain the U.S. advantage in an era of strategic global competition, the DoD must revitalize its alliances and partnerships, maintain efforts to counter violent extremists, and accelerate development and adoption of new technology to maintain the DoD's competitive advantage.

[1] U.S. Senate, Committee on Armed Services, Advance Policy Questions for Lloyd J. Austin, Nominee for Appointment to be Secretary of Defense.

REVITALIZING AND MAINTAINING ALLIANCES AND PARTNERSHIPS

The 2021 Interim National Security Strategic Guidance identifies the reinvigoration and modernization of U.S. alliances and partnerships as one of the priorities for deterring and competing with countries such as China. The Strategic Guidance further states that through alliances, the United States and its global partners can present a common front, leverage strengths, and pool resources to advance shared interests and deter common threats. In addition to strengthening its relationship with China, Russia has expanded its influence and activity in areas such as the Arctic and Europe. These actions require the DoD to strengthen its relationships and alliances across the globe to check these strategic competitors. The DoD must also identify capability gaps and work with partners and allies to develop the capabilities necessary to combat aggression from China and Russia in key regions. The challenge for the DoD is building these alliances when China and Russia have greater economic influence over some of these countries.

THE INDO–PACIFIC

Strong alliances with regional and non-regional partners will be crucial in countering Chinese and Russian activities in the Indo–Pacific region. Some Indo–Pacific countries may value economic development over security, so China's ability to leverage its economic strength to influence U.S. allies and partners could undermine regional partners' willingness to work with the United States. China also continues to take more direct actions to assert its dominance in the region, such as staking an exclusive claim to the South China Sea, to weaken U.S. military influence. In addition to China's influence, Russia provides weapons to U.S. allies and partners in the region, which may make Russia a partner of choice for defense.

The U.S. relationship with Vietnam has become an important part of U.S. defense planning for the region, and the U.S.–Vietnamese security relationship has been on a positive trajectory. However, a January 2020 RAND Corporation study shows that China has more ability to incentivize Vietnam through economic measures than the United States does.[2] Furthermore, Vietnam prefers to procure and use Russian-made weapons. The high cost of U.S. weapons and difficulty of integrating U.S. weapon systems into existing Vietnamese defense systems continues to make Russian-made weapons more attractive to Vietnam. This dynamic makes it less likely that the DoD will develop deep, long-lasting relationships across the Vietnamese military through weapons sales and integration. Additionally, the August 2017 Countering America's Adversaries Through Sanctions Act targets those entities that procure Russian military equipment, which could apply to Vietnam, further cooling the overall U.S.–Vietnamese relationship and hindering the DoD's ability to strengthen the military-to-military ties between the two countries.[3]

The DoD also continues to revitalize its relationship with the North Atlantic Treaty Organization (NATO) and its alliances with Australia, New Zealand, Japan, and the Republic of Korea, all of which have strong economic ties with China. For example, the United States and Australia continue to deepen the military-to-military relationship

[2] RAND Corporation, "Regional Response to U.S.-China Competition in the Indo–Pacific, Study Overview and Conclusions," January 2020.

[3] Center for Strategic and International Studies, "The Unlikely, Indispensable U.S.–Vietnam Partnership," July 6, 2021.

and interoperability through the biannual Talisman Sabre joint military exercises. In addition, in September 2021 the United States, United Kingdom, and Australia announced the AUKUS security pact, a trilateral partnership that will involve the United States and United Kingdom providing Australia with the ability to deploy nuclear-powered submarines. However, China is Australia's largest trading partner, and China may use the trade relationship to pressure Australia to support China's regional goals.

Another challenge is the U.S. relationship with the Philippines, which has been strained since 2016 when political leadership changed in the Philippines. The new Philippine government moved closer to China and threatened to revoke the 1998 Visiting Forces Agreement and the 2014 Enhanced Defense Cooperation Agreement.[4] Revocation of these two agreements would be a significant setback in the U.S.–Philippine relationship and make it more difficult for the DoD to develop a meaningful partnership with its counterparts from that country.

China and Russia will continue to challenge the DoD's efforts to develop deeper partnerships across the Indo–Pacific region. The DoD must continue to broaden its collaboration with Indo–Pacific regional partners to ensure adequate power projection in the region to deter aggression and influence from China and Russia.

THE ARCTIC

The DoD must continue to work with allies in the Arctic. The Arctic, which is warming twice as fast as the rest of the world, is emerging as a region where U.S. alliances and partnerships are increasingly critical for maintaining a strategic advantage. As the ice melts in the Arctic, expanded shipping lanes and increased access to natural resources during the summer months has prompted increased Russian military activity in the region. Russia has also given China access to the region through a 2015 agreement to further develop the Northern Sea Route and a 2017 agreement to work together on an Arctic Silk Road Initiative to improve Arctic shipping routes. In 2019, Russia and China also agreed to jointly develop an Arctic research center. The evolving partnership between Russia and China, coupled with China's increasing assertiveness, is adding urgency for the United States to increase its presence in the Arctic.

In the Arctic, China plans to build infrastructure and conduct commercial trial voyages as part of the Arctic Silk Road Initiative. These actions will complement China's Belt and Road Initiative, which is a series of infrastructure projects that connect Russia and Eurasia, Africa, Southeast Asia, and parts of South Asia. This infrastructure network will enable China to achieve its economic ambitions and demonstrate its great power status across the globe, directly challenging U.S. economic and security interests.

While China is inserting itself in the Arctic region through its cooperation with Russia, Russia continues to expand its economic and military presence inside its own borders. About 25 percent of Russia's land mass is in the Arctic, and Russia has made significant investments there. Russia's commercial investments have been matched by its continued defense investments and activities that strengthen both its territorial defense and its ability to control the Northern Sea Route. Russia has gradually strengthened its Arctic military presence by creating new units, refurbishing old airfields and infrastructure, and establishing new military bases along its Arctic coastline.

[4] Center for Strategic and International Studies, "The U.S. Alliance with the Philippines," December 3, 2020.

Survival, evasion, resistance, and escape (SERE) specialists dig a snow cave at Utqiaġvik (Barrow), Alaska, on January 12, 2021. The snow caves served as shelter for the SERE specialists during their second night of upgrade training.

Source: The Air Force, 354th Fighter Wing Public Affairs.

For example, according to a May 2021 *BBC News* article, Russia has upgraded its military airfield at Alexandra Island, Franz Josef Land—less than 600 miles from the North Pole—to allow planes to land year-round, and stationed anti-ship missile launchers there.[5] In FY 2022, the DoD OIG plans to perform an evaluation of the North Warning System that detects potential airborne threats in the Arctic region.

Because of the strategic importance of the Arctic, the Military Services revised their Arctic plans. The Services are also increasing their presence and extreme cold weather training in Alaska and conducting more frequent training with partners and NATO allies in Northern Europe. For example, Norway will lead Cold Response 2022, a biennial exercise designed to train participating NATO allies and partners in cold weather operations. In FY 2022, the DoD OIG plans to audit the readiness of Soldiers and Marines to conduct training, exercises, and operations in extreme cold weather.

The DoD must continue to work with NATO allies and Nordic countries that are increasing their military presence and operations in the Arctic. The DoD's ability to increase its Arctic presence, work with allies and partners, and project power is critical to deterring Russian and Chinese aggression in the region.

EUROPE

In Europe, NATO remains the strategic center of gravity and foundation of deterrence and assurance in the region. Russia continues to challenge NATO partners with provocative actions such as air space violations, jamming global positioning system (GPS) signals, hacking soldiers' personal electronic devices, increasing military presence and aggression on the eastern Ukrainian border, and artificially pushing up gas prices in an effort to weaponize Russian energy supplies to the European Union. Russia's actions require the DoD to continue to revitalize NATO relationships and promote coordination and interoperability.

[5] *BBC News*, "Russia Flexes Muscles in Challenge for Arctic Control," May 20, 2021.

One way the DoD works with its NATO allies in Europe is through the European Deterrence Initiative, which aims to enhance the U.S. deterrence posture in Europe and support the collective defense and security of NATO allies. The DoD invested nearly $6 billion in the initiative in FY 2020. The DoD also continues to work with non-NATO partners in the region to maintain and build defense relationships as Russia and its proxies work to disrupt the international order and weaken governments and institutions. For example, U.S. alliances and partnerships support Ukraine's defense efforts against Russian aggression and Russia's heightened military presence along their shared border.

The DoD will also need to monitor China's increasing military cooperation with Russia and its aggressive expansion of economic activities in Europe. For example, China was an official observer in the 2021 Russian Zapad exercise—one of Russia's largest military exercises on its western border—which raised concerns within the NATO community. Additionally, along with its military cooperation with Russia, China has been aggressively pursuing investments in key infrastructure projects from the Baltics to the Mediterranean. For example, in the past decade, Chinese companies have acquired stakes in 13 ports in Europe, including in Greece, Spain, and Belgium. These ports control approximately 10 percent of Europe's shipping container capacity. With such significant economic control over Europe's most important ports in the European Union, China could exploit its access to these ports to increase naval power and influence in Europe.

The DoD must effectively collaborate with European allies and partners to identify and address threats from Russia and China and to collectively prepare for future challenges. The DoD should continue to invest in the European Deterrence Initiative to enhance the DoD's posture in the European theater, improve the ability of allies to respond and deter aggression in the region, and help preserve peace in Europe.

THE MIDDLE EAST

The United States has maintained a presence in the Middle East for decades. This presence in the region sends a clear signal to competitors, such as to Iran, that the United States has the capability to defend its partners and national interests. With the U.S. departure from Afghanistan and drawdown across the Middle East, the DoD will need to continue demonstrating the U.S. capability to counter Iran's support for terrorist organizations and other malign activities. The challenge to the DoD is in how to demonstrate power in ways that do not rely on U.S. forces being located in the region. In addition, the DoD must demonstrate a responsive force posture along with strong partnerships with regional and Coalition forces.

China and Russia have taken advantage of a decline in the U.S. presence in the Middle East to deepen defense and trade cooperation across the region.[6] China and Russia continue to exploit the withdrawal of U.S. and allied forces in the region, along with reduced U.S. partner engagement resulting from the coronavirus disease–2019 pandemic, to strengthen their foothold in the area. Russia continues to sell arms in the Middle East without end-use restrictions, resulting in the destabilization of arms sales in the region. Russia also continues to establish permanent bases in Syria and Sudan. Russia's growing presence in the region has led to increased unauthorized and unsafe Russian interactions with Coalition forces.

[6] DoD, "Great Power Competition Adds to Challenges in Middle East," February 9, 2021.

These interactions have complicated the DoD's operations to counter violent extremists in the region. China also continues to strengthen defense cooperation throughout the region with arms sales, exercises, and active involvement in multilateral organizations such as the League of Arab States, the Gulf Cooperation Council, and the Union of the Arab Maghreb. Based on China's actions, a March 2020 article from the University of Nottingham, Asia Research Institute concluded that China aims to establish and strengthen trade, diplomatic, and defense relationships across the Middle East.[7]

Finally, the easing of tensions between Israel and other Arab countries through the September 2020 Abraham Accords enables the DoD to transfer the responsibility for DoD coordination with Israel from the U.S. European Command to the U.S. Central Command. The move may offer the DoD a strategic opportunity to align additional partners against shared threats in the Middle East, but the transfer of responsibilities from one combatant command to another will be a complex challenge for the DoD.

AFRICA

In Africa, the United States faces challenges competing with China and Russia for influence. Africa has a vast geographic area three times the size of the continental United States, comprising 52 countries. However, the United States maintains only a small footprint in Africa, and the DoD relies on focused, sustained engagement with partners to achieve shared security objectives. The DoD implements this approach through exercises, counter-violent extremist operations, and security cooperation and assistance programs. Despite these partnerships and programs, as the DoD prioritizes and allocates resources, it may need to scale back activities in Africa, which could create opportunities for other nations, such as China or Russia, to fill the void. In testimony to the Senate Armed Services Committee on April 22, 2021, the Commander of the U.S. Africa Command stated that China and Russia have "long recognized the political, military, and economic importance of Africa and each continues to seize opportunities to expand their influence across the continent."

China's increasing influence in Africa has resulted in some African countries choosing China as their preferred security partner, rather than the United States. China has engaged in intelligence sharing, technology transfers, and joint military and police training with several African countries. China also loans or donates in ways that help it gain access in countries that otherwise do not have strong ties to the Chinese government.[8] For example, China now exerts economic and military influence over the strategic port in Djibouti, which was previously used almost exclusively by the United States and its allies. In his testimony on April 22, 2021, the Commander of the U.S. Africa Command stated that China had expanded its naval pier in Djibouti and said, "This pier has the capability to dock their largest ships, to include the Chinese aircraft carriers as well as nuclear submarines." Furthermore, in a May 2021 interview with the Associated Press, the Commander of the U.S. Africa Command stated that China is looking to establish a large navy port capable of hosting submarines or aircraft carriers on Africa's western coast.[9]

According to U.S. Africa Command officials, developing strong relationships with African states and becoming their "partner of choice" is one of the primary ways to counter adversaries in the

[7] University of Nottingham, Asia Research Institute, "China's Partnership Diplomacy in the Middle East," March 24, 2020.

[8] *The Washington Post*, "China's Belt and Road Initiative Invests in African Infrastructure – and African Military and Police Forces," April 30, 2021.

[9] The Associated Press, "General: China's Africa Outreach Poses Threat From Atlantic," May 6, 2021.

region.[10] As the DoD applies its finite resources throughout the world, it will continue to face challenges in building and maintaining effective partnerships with countries in Africa without leaving room for other strategic competitors to do the same.

COUNTERING VIOLENT EXTREMISM

As the DoD continues to focus on strategic competition, it must maintain its ability to counter violent extremist organizations (VEOs) around the world. In regions where the DoD chooses to maintain a counterterrorism presence, the shift toward strategic competition may require the DoD to accept more risk in the counterterrorism mission than it has in the last two decades.

The 2021 Interim National Security Strategic Guidance states that terrorism and violent extremism remain "significant threats."[11] For example, in the Middle East, the Islamic State of Iraq and Syria (ISIS) continues to launch attacks on U.S. personnel and interests in the region. In Afghanistan, with the collapse of the Government of the Islamic Republic of Afghanistan and the Afghan National Security and Defense Forces, the Taliban have taken control. As a result, the United States will not have access to previously accessible intelligence and will be challenged to respond to threats to U.S. interests by terrorists and VEOs that originate from Afghanistan. In addition, in Africa, ISIS and al-Qaeda affiliates are expanding across the continent and, according to April 20, 2021 testimony from the Commander of the U.S. Africa Command before the House Armed Services Committee, these affiliates are "becoming increasingly more capable, violent, and difficult for our African partners to defeat without international support."

As the DoD reprioritizes its counterterrorism objectives with respect to strategic competition, it must identify new ways to achieve the objectives in a manner that complements the shift in priorities. U.S. forces may increasingly provide advisory support to partner forces from a distance, rather than conducting unilateral or accompanied missions. The DoD may need to increase its reliance on international partners and allies for counterterrorism operations. However, this support from partners and allies is not guaranteed. In June 2021, France announced its intent to end a counterterrorism mission in West Africa that it has led since 2013. It is unclear whether local African partners will be able to continue their fight against ISIS and al-Qaeda without international support.

Combating global terrorism continues to consume a large portion of DoD high-demand, low-density resources, such as special operations forces and intelligence, surveillance, and reconnaissance platforms. While U.S. military units that fight VEOs often operate in small groups, they work in austere environments that require several resource-intensive functions, including intelligence, surveillance, and reconnaissance; logistics; and medical and evacuation services. Because of the high demand for these limited resources, the DoD must be strategic in how it uses them in the future as priorities evolve. Furthermore, the DoD must continue to develop new capabilities to address evolving VEO tactics. For example, the DoD must maintain language and technical capabilities to monitor and counter VEO messaging campaigns. While most VEOs often rely on small arms and homemade explosives, some groups are increasingly able to launch attacks using sophisticated weapons, such as the drone attacks that targeted U.S. interests at Ain al-Asad Airbase in Iraq in July 2021. To prevent or interdict these more sophisticated attacks, the DoD will need to

[10] *Military Times*, "How AFRICOM Plans to Counter Russian, Chinese Influence in Africa," January 20, 2020.

[11] The White House, "Interim National Security Strategic Guidance," March 2021.

maintain visibility of VEO and terrorist networks, which may be a challenge in countries where there is no U.S. presence, such as Afghanistan.

In many parts of the world, the United States pursues a partner-centric approach to counterterrorism whereby participating countries assume the responsibility of counterterrorism missions within their borders. The United States provides dozens of countries with training and equipment to build their security forces' capacity to counter violent extremism. One of the benefits of this approach is that as a country's ability to counter VEOs improves, there can be a reduction of the amount of U.S. special operations support for these counterterrorism missions, making these forces available for other missions. However, these capacity-building missions often require years of commitment and take place in nations with limited resources and weak governmental institutions. And, as seen in Afghanistan with the rapid collapse of the Afghan National Defense and Security Forces, there are no guarantees that this approach will be successful in each country. Therefore, as the DoD continues to reprioritize counterterrorism capabilities, it must review the underlying assumptions regarding building partner capacity programs to understand the likelihood of success and the potential increased risk to U.S. interests in the affected countries.

SUSTAINING TECHNOLOGICAL DOMINANCE

The rapid evolution and international proliferation of advanced technology—largely because of advances in the commercial sector—sets a pace of development that threatens to erode traditional sources of U.S. military advantage, such as air, space, and information dominance. Research and development is key to ensuring that the United States maintains a competitive advantage in technologies and defense. According to a June 2021 *New York Times* article, the U.S. Government used to spend significant funds on research and development to ensure that the country led in innovation and technology.[12] Every year from the 1950s through the 1970s, Federal spending on research and development equaled at least 1 percent of gross domestic product. Part of the reason for the U.S. Government investing in research and development is that the private sector does not do this on its own unless the return on the investment is profitable, regardless of the potential benefit to society or national security.

Federally funded research and development from the 1950s through 2000 resulted in the development of jets, satellites, semiconductors, and more. The U.S. Government did not continue to invest heavily in research and development after 2000, and in 2017, investments had dropped to less than 0.7 percent of gross domestic product. The lack of spending on research and development places the United States at a disadvantage against competitors such as China, which spent an estimated 1.3 percent of gross domestic product on research and development in 2017. On June 8, 2021, the Senate passed legislation to spend about $250 billion over the next 5 years on scientific research and development to bolster competitiveness against China. The bill also included investments in emerging technologies. However, as of October 5, 2021, the House had not yet considered the bill. According to a May 28, 2021 statement by the Secretary of Defense, the President's FY 2022 budget request to Congress included $14.7 billion for science and technology and $112 billion for research, development, test, and evaluation for the DoD.[13] In FY 2022, the DoD OIG plans to perform an evaluation of research and development for new

[12] *The New York Times*, "The Morning Newsletter," June 8, 2021.

[13] DoD, "The Department of Defense Releases the President's Fiscal Year 2022 Defense Budget," May 28, 2021.

technologies to ensure that the DoD monitored and mitigated risks when developing new technologies with partners in industry and academia.

Artificial intelligence (AI) is an example of an emerging technology for which the United States faces strong competition from China. Within the DoD, the Joint Artificial Intelligence Center continues to enable the development of AI capabilities and the Defense Advanced Research Projects Agency continues to engage in AI research and produce AI tools. However, according to the 2021 Annual Threat Assessment of the U.S. Intelligence Community, China seeks to lead in emerging technology fields, including AI, by 2030, and has a well-resourced and comprehensive strategy to acquire and use technology, including state-sanctioned technology transfers and intelligence gathering.

In addition to increasing its investment in research and development, the United States needs to place more emphasis on science and engineering education to be a global leader in these areas. According to a March 2021 *Forbes* article, China is graduating eight times as many science and engineering students as the United States.[14] The population of China is four times the population of the United States, so this is a sharp disparity even on a per capita basis. The United States needs scientists and engineers to research, develop, and innovate for not just the betterment of our defense, but for the economy as a whole. For more information on the DoD's need for personnel in the science and engineering fields, see Management Challenge 9, "Recruiting and Retaining a Modern Workforce."

Finally, the DoD may be challenged in developing the corresponding policies, doctrine, and organizational structures at the speed needed to effectively integrate and employ emerging technologies. Effectively integrating new technology into DoD activities and operations will need to be underpinned by sound, and potentially novel, operational concepts to ensure that they are complementary to those that currently exist. Leaders at all levels will need to embrace and understand the value of emerging technologies, such as AI, along with where and how the technologies best fit within the DoD so the benefits can be maximized. Additionally, the speed at which new technology is being introduced will necessitate continually adapting and training the force on its use.

To be a global leader in the technologies, including the kind of advanced and emerging technologies that will be key to defense now and in the future, the United States must find ways to increase the number of Americans who enter the science and engineering career fields and must fund research and development at a Federal level. The DoD will also need to consider the corresponding policy impacts of new technology and how to best integrate it into DoD operations. The DoD must lead in development and implementation of new technologies to cultivate advantages against, and stay ahead of, strategic competitors and promote overall technological dominance.

CONCLUSION

China and Russia continue to assert their presence and influence in the Indo–Pacific, Arctic, Europe, Middle East, and Africa. The DoD must enhance, improve, and revitalize its alliances in those regions to counter strategic competitors, project power, and continue to effectively conduct counterterrorism operations. Finally, the DoD must invest in new technologies to maintain a competitive advantage and effectively implement those technologies. Strengthening alliances and developing, adopting, and integrating new technologies into DoD operations will be key in protecting U.S. national security interests.

[14] *Forbes*, "Biden's Supply Chain Worries Signal A Looming Crisis In U.S. Security," March 9, 2021.

A Delta IV rocket launches from Cape Canaveral Space Force Station, Florida, on December 10, 2020. (photo by Jeff Spotts)

Challenge 2. Assuring Space Dominance, Nuclear Deterrence, and Missile Defense

INTRODUCTION AND OVERVIEW

Space is an increasingly contested environment. Missile defense and nuclear deterrence rely on the freedom of the U.S. military to operate in space, requiring an interconnected set of capabilities in this new warfighting domain. However, the DoD faces new and emerging threats in space as strategic competitors field and develop space capabilities and counter-space capabilities.

The U.S. Space Force (USSF) will play a key role in any future space conflict, and it must be positioned to protect and defend U.S. interests in space. At the same time, the U.S. nuclear arsenal is aging, with many of its delivery systems and warheads reaching obsolescence over the next decade. It is vital that the United States modernize its space-based, nuclear deterrence, and missile defense capabilities to meet present-day and future challenges. While modernization efforts are occurring, the DoD must continue to sustain operational capabilities of legacy systems and ensure that operators and support personnel, including maintainers, are proficient in both legacy and new platforms.

BALANCING THE SUSTAINMENT OF LEGACY SYSTEMS WITH MODERNIZATION

To maintain the advantage against strategic competitors and ensure U.S. dominance in the space domain, the DoD must sustain its space-based, nuclear deterrence, and missile defense systems and equipment, and also modernize. As the Secretary of Defense stated in his March 4, 2021 Message to the Force, the DoD must prioritize China as the "number one pacing challenge" and "bolster deterrence" to maintain the U.S. competitive advantage; "innovate at a speed and scale that matches a dynamic threat landscape"; and "divest of legacy systems and programs that no longer meet our security needs, while investing smartly for the future." Therefore, the DoD must balance which space-based, nuclear, and missile defense systems and equipment to sustain and which to divest, while also ensuring that it modernizes these systems rapidly enough to maintain vital capabilities and not jeopardize the competitive advantage.

SPACE-BASED SYSTEMS SUSTAINMENT AND MODERNIZATION

In the June 2020 Defense Space Strategy Summary, the DoD defined space as vital to U.S. national security and economic prosperity and a "source of and conduit for national power, prosperity, and prestige."[15] The public and the DoD rely on space-based systems for communication, weather, intelligence, navigation, and a variety of other critical functions. These space-based systems are part of U.S. infrastructure and allow the military to conduct operations across the world in support of national security objectives. According to the Government Accountability Office (GAO), the DoD is in the beginning phases of acquiring 13 new major programs for spaced-based operations. These programs range from new satellites and ground processing capabilities—including missile warning, protected communications, and space-based environmental monitoring—to space command and control.

Space continues to become more contested as strategic competitors expand their presence in space by fielding systems that directly challenge U.S. space dominance. Russia and China have tested and deployed advanced counter-space systems over the past decades. These systems are a threat to U.S. space systems and U.S. space superiority. Rogue states such as Iran and North Korea cannot seriously challenge the U.S. in space, but do possess cyber and jamming systems that could disrupt U.S. space systems. To ensure space superiority, the DoD must replace older space systems with new ones while making current systems more survivable against advanced threats. In February 2021, the DoD OIG announced an audit to review the extent to which the DoD maintained the equipment and infrastructure needed to support space launches.

In its goal to develop and acquire new space capabilities for the DoD, the USSF is overseeing several major acquisition programs. One of these programs is the national security launch program to develop commercial launch vehicles for national security missions. The DoD uses three launch vehicles for national security payloads—United Launch Alliance's (ULA) Atlas V and Delta IV, and Space Exploration Technologies Corporation's (Space X) Falcon 9. The USSF plans to continue to use Space X's Falcon 9, but will phase out the ULA's Atlas V and Delta IV. The National Defense Authorization Act for FY 2017 prohibits the use of the Russian-made engines that power the Atlas V for national security missions after December 31, 2022, and the Delta IV is no longer in production.

To replace the Atlas V and Delta IV, the USSF chose another ULA launch vehicle named Vulcan. Vulcan is still under development and must successfully complete two flights before it can be certified to carry national security payloads. However, Vulcan's certification flights have been delayed due to issues with its engine development and scheduling complications caused by the coronavirus disease–2019 (COVID-19) pandemic. With the Delta IV out of production, the restrictions on using the Atlas V for DoD missions past 2022, and the delays to the certification of new launch systems, the DoD risks having only one launch platform.

In addition to replacing the legacy launch vehicles, the USSF is also replacing Global Positioning System (GPS) satellites and overhead infrared systems. The USSF has launched only half of the replacement GPS satellites and future launches face possible delays caused by the acquisition timeline of a new ground control

[15] Defense Space Strategy Summary, June 2020.

system for the GPS constellation (a networked collection of satellites on orbit). Ground control systems monitor and control satellites on orbit. The USSF scheduled operational testing for the new ground control system for 2023, after the USSF accepts delivery of the remaining replacement GPS satellites. By testing the ground control system after the contractor delivers the satellites, there is a risk that testers might discover deficiencies to already-produced or launched satellites. Testing the ground control system after the satellite deliveries also constrains the USSF's options for corrective action and potentially increases risk to the program's cost, schedule, and performance.

NUCLEAR ENTERPRISE SUSTAINMENT AND MODERNIZATION

The United States is at a critical point in modernizing its nuclear arsenal and sustaining legacy systems. The DoD has little margin to bring new nuclear systems online before the current systems reach the end of their service lives. The strategic nuclear triad consists of:

1. land-based intercontinental ballistic missiles (ICBMs),
2. submarines armed with ballistic missiles, and
3. strategic bombers carrying gravity bombs and air-launched cruise missiles.

The DoD is planning to spend half a trillion dollars through 2030 to modernize all three legs of the triad.

The land-based portion of the nuclear triad consists of Minuteman III ICBMs that entered service in 1970 and originally had a 10-year service life. The DoD has extended the life of the Minuteman III through 2030—over four times longer than originally intended. Sustaining the ICBMs is difficult and expensive. According to a January 2021 *Air Force Magazine*

341st Missile Maintenance Squadron personnel securely place a cover on the front of the stage-one booster of the Minuteman III ICBM at the missile handling facility on Malmstrom Air Force Base, Montana, on April 20, 2021.

Source: The Air Force, 354th Fighter Wing Public Affairs.

article, the Commander of the U.S. Strategic Command stated, "You cannot life-extend Minuteman III. It is getting past the point of 'it's not cost effective.' ... That thing is so old, in some cases, the drawings don't exist anymore, or where we have drawings, they're like six generations behind the industry standard."[16] The replacement ICBMs, the Ground Based Strategic Deterrent (GBSD), will bring DoD missile technology into the 21st century. The Air Force plans to test launch the first GBSD in 2023, and start deploying it in 2029. Failure to field the GBSD will negatively impact the DoD's nuclear operational capabilities. Specifically, according to the 2018 Nuclear Posture Review, delays in the deterrent program, accompanied by a rapid age-out of the Minutemen III ICBMs, puts the United States at risk. The risk is that strategic competitors would need fewer resources for an attack to threaten U.S. deterrence capabilities.

The sea-based portion of the nuclear triad consists of *Ohio*-class submarines that entered service in the 1980s with a planned 30-year service life. The DoD has extended the class's service life through 2040, for a total service life of 60 years. Similar to the modernization challenges for the land-based portion of the nuclear triad, there is no margin for risk or error in fielding the replacement for the sea-based portion of the nuclear triad. The Navy will replace the *Ohio*-class submarine with the *Columbia*-class submarine, with the first of the replacements procured in FY 2020. Based on the Navy's planned replacement schedule, the number of submarines in the nuclear triad will eventually fall from 14 to 10 and will remain at that level until 2041.

As reported in a May 2021 GAO report on the nuclear triad, according to Navy and U.S. Strategic Command officials, the Navy will struggle to meet its operational requirements starting in FY 2030 and continuing through 2040 because the Navy will have four fewer submarines than the current fleet.[17] The Navy faces several risks to an on-time delivery of the *Columbia*-class submarine, including new technologies, design challenges, issues with production quality, and an aggressive production schedule. Lack of shipbuilding infrastructure is another factor that could delay the deployment of the *Columbia*-class submarine and jeopardize the DoD's ability to provide sufficient nuclear deterrence from the sea-based portion of the nuclear triad. For more information on the shipbuilding industry, see Management Challenge 4, "Reinforcing the Supply Chain While Reducing Reliance on Strategic Competitors."

Similar to the other two legs of the nuclear triad, the air-based leg of the triad also faces sustainment and modernization issues. The air-based leg of the triad consists of bomber aircraft, including the B-2 Spirit and B-52 Stratofortress, both of which the Air Force plans to modernize or replace. However, according to the May 2021 GAO report on the nuclear triad, the Air Force will be challenged to balance mission requirements with modernization and maintenance.

With respect to modernization, the GAO identified in the May 2021 report on the nuclear triad that the replacement for the B-2, the B-21 Raider, faces the prospect of delays due to supply chain risks and an insufficient DoD nuclear certification workforce. Specifically, the GAO reported that the supply chain risks stem from the DoD not following best practices

[16] *Air Force Magazine*, "STRATCOM Welcomes Nuke Review, but Says Minuteman III Life Extension Should Not be Considered," January 5, 2021.

[17] Report No. GAO-21-210, "Nuclear Triad: DoD and DOE Face Challenges Mitigating Risks to U.S. Deterrence Efforts," May 6, 2021.

for the acquisition, which include matching resources to customer needs; ensuring that the design is stable and performs as expected; and ensuring that production meets cost, schedule, and quality standards. In addition, the GAO determined that the insufficient nuclear certification workforce was due to a limited number of qualified workers. If these risks are realized, they would delay modernization, forcing continued sustainment of the legacy bombers and jeopardizing the DoD's ability to provide sufficient nuclear deterrence from the air-based leg of the nuclear triad.

As part of the overall nuclear modernization efforts, the DoD is developing a new generation of components to support the Nuclear Command, Control, and Communications (NC3) system. The NC3 system is the combination of capabilities to use or terminate the use of nuclear weapons and ensure that the use of those weapons is authorized. Today's NC3 system is a legacy of the Cold War, the last comprehensive update was almost 3 decades ago. While once state-of-the-art, the NC3 system is now subject to challenges from aging system components and new, growing 21st century threats, such as sophisticated cyber attacks. According to a January 2021 *National Defense Magazine* article, the Director of the NC3 Enterprise Center at the U.S. Strategic Command stated that the threat environment is evolving and there is a need to ensure that there are no critical gaps or mismatches between the various components of the NC3 enterprise.[18]

The DoD has acknowledged the risk factors and challenges to maintaining legacy systems and modernizing the nuclear triad and the components of the NC3 system. The DoD must continue its efforts to strategize and mitigate these risk factors and challenges to ensure that the nuclear triad acquisition program does not fall behind schedule, thereby avoiding nuclear deterrent shortfalls in the next decade.

MISSILE DEFENSE SUSTAINMENT AND MODERNIZATION

Strategic competitors may use missiles to attack the United States, making missile defense a key capability for national defense. Contractors have struggled to deliver new interceptor missiles to the Missile Defense Agency (MDA) that would counter these types of attacks. The contractors' delays in providing the missiles to the MDA, caused by the temporary unavailability of electronic parts, resulted in corresponding testing delays. Specifically, the MDA has not been able to test Aegis Standard Missile-3 Block IIA, Terminal High Altitude Area Defense, and Homeland Defense Ground-Based interceptors as robustly as it had planned. The MDA conducted only three of nine scheduled tests for the interceptors, and two of those tests were failures. The remaining six MDA flight tests for interceptors have been delayed because of the ongoing COVID-19 pandemic. The COVID-19 pandemic will continue to adversely affect the MDA's ability to test its interceptors into FY 2022. Modernizing missile defense is vital to a capable and persistent homeland defense and is necessary to ensure sustainable U.S. power projection.

MAINTAINING OPERATIONAL CAPABILITIES FOR LEGACY SYSTEMS WHILE TRAINING ON REPLACEMENT SYSTEMS

As the DoD continues to decommission outdated and legacy systems and replace them with more modern systems, training will be vital. Operators and support personnel, including maintainers, will need to remain proficient in

[18] *National Defense Magazine*, "Just In: STRATCOM Revitalizing Nuclear Command, Control Systems," January 5, 2021.

the legacy system, while simultaneously learning the skills needed for the replacement system. This will pose a challenge to the DoD to devote sufficient time and funding necessary to ensure operators and support personnel are fully proficient in the system. Ensuring that operators receive the right training on the right equipment at the right time is imperative, and failure to adequately train personnel can be catastrophic. For example, the Navy experienced a catastrophic loss on August 21, 2017, when the USS *John S. McCain* and a commercial tanker collided near Singapore, resulting in the death of 10 Sailors and the injury of 48 more. According to the Navy's investigation, one contributor to the accident was the crew's lack of knowledge of the steering control. As evidenced by this event, the right training on the right equipment is critical, regardless of whether that equipment operates a ship, space systems, or nuclear systems.

SPACE ENTERPRISE

The USSF must restructure its training to allow Guardians to operate in a new space environment. The Chief of Space Operations has stated that this shift in training is a "different way of doing business," than how the Air Force Space Command trained personnel. On August 23, 2021, the USSF activated the Space Training and Readiness Command (STARCOM) to oversee training and readiness of USSF Guardians. Before activating STARCOM, the Space Force Space Training and Readiness (STAR) Delta (Provisional) oversaw the training and education of Guardians.

The Air Force started improving its space training and education even before the USSF established STAR Delta (Provisional), and the training and education will continue to evolve as the USSF raises awareness of the threats facing assets on orbit and on the ground, and offers a more holistic view of how those tools fit into the larger warfighting picture. The primary difference between the training and education that STARCOM is developing and past practices is that STARCOM's training and education is focused on space as a domain of warfare. Previous training and education focused on day-to-day operations in a peacetime environment, while the current training and education is preparing the USSF to prevail in a contested, degraded, and operationally limited environment. Training and education now entail developing space warfighting doctrine and tactics, techniques, and procedures, as well as testing and evaluating USSF capabilities. This is a complex task because there is little precedent for space warfighting doctrine, unlike those of air, land, and sea, from which to build space-mission training and education. According to a November 2020 *Breaking Defense* article, the Commander of STAR Delta (Provisional) said, "The essential nature of war hasn't changed," and the USSF will continue to look to legacy doctrine, such as Joint Publication 3-14 Space Operations, as well as warfighting doctrine from other domains, because there are still lessons to be learned from them.[19] In addition to training the operators of space systems, the USSF will need to ensure that its support personnel and the maintainers of those systems also receive appropriate training to ensure proficiency.

The USSF also requires training simulators to prepare to fight in a contested space domain. In a December 2020 interview with *Air Force Magazine*, the Commander of STAR Delta (Provisional) stated, "It's often hard to practice orbital offense and defense without

[19] *Breaking Defense*, "STARCOM: Training Troops to Fight Space Wars, Boldly," November 30, 2020.

actually being there."[20] The Commander added that the USSF needs more advanced simulators to help show how events might play out in an electronic or physical war. Simulators offer Guardians valuable opportunities to learn in a safe environment. During simulated training Guardians can problem solve in real-time, rehearse tactics, develop muscle memory for operating equipment, and identify deficiencies in equipment, policy, or resources. According to a December 2020 *National Defense Magazine* article, the Deputy Commander of the U.S. Space Command acknowledged the importance of having quality simulators, and stated that the DoD did not have enough simulators to train Guardians. The Deputy Commander further stated that the USSF needs to develop simulators able to model a potential conflict and fight, conduct war games, and do these at a scale and scope that have not been done before.[21]

Training for operations in the space domain is essential to successfully accomplishing USSF missions. The challenge for the USSF is developing appropriate doctrine; training and education; and tactics, techniques, and procedures, while ensuring that it has the resources and equipment to effectively train Guardians to prevail in this increasingly competitive warfighting domain.

NUCLEAR ENTERPRISE

The GBSD will be the first ICBM fielded by the Air Force since 1985, and the *Columbia*-class submarine will be the first ballistic missile-class submarine fielded by the Navy since 1981.

Both the GBSD and *Columbia*-class submarine will use far more advanced technology than the platforms they will replace. This means that operators will have to be retrained for these more advanced platforms. In addition to training the operators on these advanced systems, the Air Force and Navy will need to ensure that their support personnel and the maintainers of those systems also receive appropriate training to ensure proficiency. However, it will not be possible to start familiarizing personnel with the GBSD and *Columbia*-class submarine until both platforms enter the production stage, meaning that the Air Force and Navy are at least several years away from starting this process.

There are tight schedules and minimal overlap between fielding the GBSD and *Columbia*-class submarines, and the retirement of Minuteman III ICBMs and the *Ohio*-class submarines. The combination of coordinating the fielding of new systems with current operations, maintenance, and sustainment activities reduces the time and manpower available to train personnel on the new systems. The Air Force and the Navy will be challenged to concurrently operate and maintain the legacy systems while fielding the new systems.

CONCLUSION

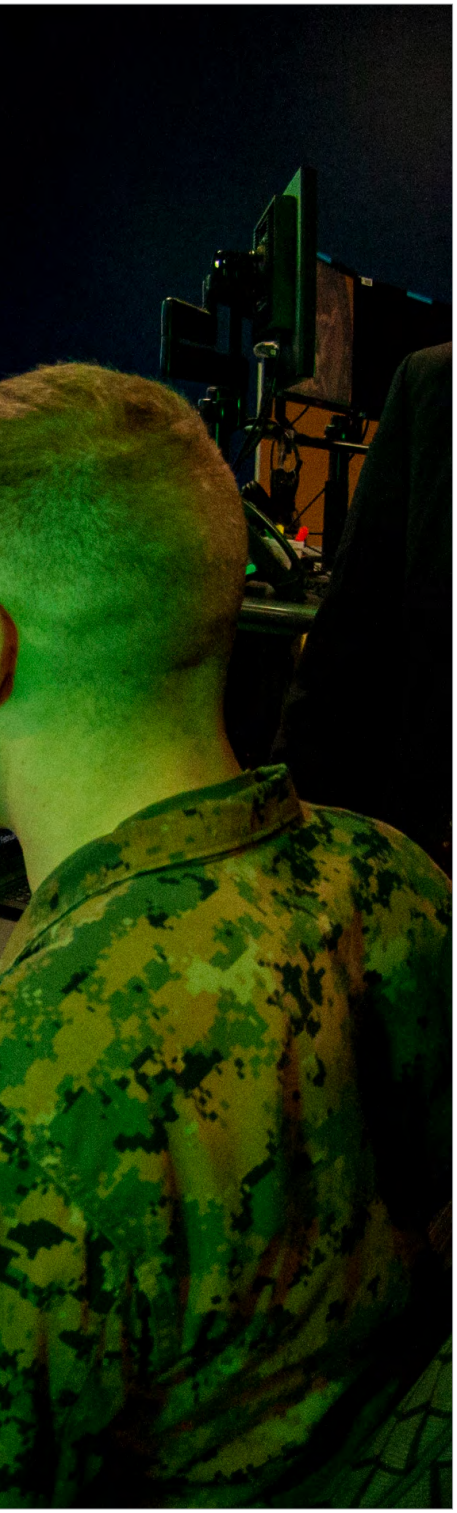
Space is an increasingly contested environment with strategic competitors fielding systems that threaten U.S. space superiority. The DoD is challenged with balancing the sustainment of legacy systems with the modernization and fielding of new systems, including training the operators and support personnel for proficiency. The potency and effectiveness of the U.S. strategic defense architecture depends on how effectively the DoD balances sustainment and modernization.

---

[20] Orbital offense and defense refer to operations in the different layers of the earth's orbit—high earth orbit, medium earth orbit, and low earth orbit. According to the National Aeronautics and Space Administration, weather and communication satellites tend to operate in high earth orbit, farthest away from the surface, while navigation and specialty satellites operate in medium earth orbit, and scientific satellites tend to operate in low earth orbit. *Air Force Magazine*, "Space Force Training Takes Shape," December 1, 2020.

[21] *National Defense Magazine*, "Pentagon, Industry Investing in Space Force Simulations," December 7, 2020.

A Marine with Marine Corps Forces Cyberspace Command works in the cyber operations center at Lasswell Hall, Fort Meade, Maryland, on Febuary 5, 2020. (U.S. Marine Corps photo)



Challenge 3. Strengthening DoD Cyberspace Operations and Securing Systems, Networks, and Data

INTRODUCTION AND OVERVIEW

The DoD continues to face sophisticated and evolving cyber attacks from malicious actors such as nation-states, terrorist groups, and hacktivists. These adversaries constantly try to exploit DoD cybersecurity vulnerabilities. The DoD depends on cyber capabilities to conduct and support operations across all domains and enhance U.S. military advantages.

The DoD Information Network (DODIN)—the globally interconnected set of information capabilities and communication and computing systems and services—must be protected. The DoD must also be prepared to defend the networks and systems operated by non-DoD entities, such as the Defense Industrial Base (DIB). Recent cyber attacks on Federal agencies—such as the compromise from the SolarWinds Orion platform and the on-premises Microsoft Exchange servers—highlight the DoD's ongoing need to improve its cybersecurity, modernize its systems and networks, and protect its data. The 2019 DoD Digital Modernization Strategy focuses on increasing DoD-wide technological capabilities and adopting enterprise systems to further its competitive advantages.

Deterring and defeating cyber threats requires the DoD to develop and acquire innovative cyber tools and capabilities that continuously improve cyberspace operations. To protect and defend the DODIN, the DoD must modernize its aging legacy systems, networks, and devices, including software, and integrate cutting-edge technology. The DoD's challenges with its cyber workforce are discussed in Management Challenge 9, "Recruiting and Retaining a Modern Workforce."

COORDINATING AND CONDUCTING EFFECTIVE CYBERSPACE OPERATIONS

The DoD faces challenges in having the capabilities, interoperable systems, defined roles and responsibilities, and inter- and intragovernmental information sharing to coordinate and conduct effective cyber operations. Specifically, the DoD continues to face challenges in developing and implementing two cyber operations capabilities—the Joint Cyber

Marines with Marine Corps Forces Cyberspace Command in the cyber operations room at Lasswell Hall on Fort Meade, Maryland, February 5, 2020.

Source: The Marine Corps.

Warfighter Architecture (JCWA) and the Joint All Domain Command and Control (JADC2) concept. These capabilities are intended to improve coordination and information sharing in the U.S. Cyber Command and among other DoD Components. Without developing and deploying these capabilities, the DoD may not be able to efficiently conduct its operations and identify, disrupt, or halt adversaries and suspicious cyber activities at their source.

The JCWA enables the U.S. Cyber Command and its subordinate commands to conduct coordinated, integrated, joint cyberspace operations worldwide, regardless of service and physical location. The JCWA requires a variety of data, and the Air Force operates the Unified Platform that consolidates and standardizes this data. The Unified Platform is intended to guide the development and prioritization of cyberspace capabilities across the DoD. However, the Government Accountability Office (GAO) identified problems in the DoD's implementation of the JCWA and the Unified Platform. In a June 2020 report, the GAO found that the Unified Platform's cost estimate was more than five times its initial estimate at program initiation due to evolving the U.S. Cyber Command requirements, and limitations of the prototyping program that requires fielding new features every 3 months, instead of on a continuous basis using the industry's agile practices.[22] In a November 2020 report, the GAO found that the U.S. Cyber Command had not defined the JCWA interoperability requirements for integrated systems or developed the roles and responsibilities for the integration and management offices.[23]

The JADC2 concept strives to connect sensors from all Military Services into one network for better DoD-wide visibility and to replace existing, stove-piped command and control architectures. However, the DoD has

[22] Report No. GAO-20-439, "Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight," June 3, 2020.

[23] Report No. GAO-21-68, "Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance," November 19, 2020.

encountered several delays in implementing the JADC2, some of which were caused by funding issues and the legal challenges associated with the canceled Joint Enterprise Defense Infrastructure (known as JEDI) cloud contract. In June 2021, the Acting DoD Chief Information Officer (CIO) testified before the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems that the DoD still has an unmet need for an enterprise cloud capability for unclassified and classified networks that extend from the DoD's headquarters to forward deployed units (the tactical edge). To address this unmet need, the DoD intends to acquire the Joint Warfighter Cloud Capability, which the DoD believes will enable it to achieve several initiatives, such as the JADC2. During a technology conference in August 2021, the Defense Information Systems Agency Director (also the Joint Force Headquarters-DODIN Commander) and the Joint Staff CIO stated that the DoD needs to produce a minimal viable product for the JADC2 platform within 6 months, not 5 years, by leveraging existing DoD technology and rapidly developed commercial software.[24]

Without developing and modernizing its command and control infrastructure to coordinate and conduct operations, the DoD will not be able to maintain a competitive advantage over adversaries in cyberspace. In FY 2022, the DoD OIG plans to perform an audit to determine the extent to which the DoD has modernized its command, control, communications, and computer infrastructure and systems to support enterprise-wide missions and priorities.

IMPROVING CYBER HYGIENE TO PROTECT THE DODIN

The DoD has worked to improve cyber hygiene (the set of practices and steps intended to manage common cybersecurity risks) by identifying and remediating cyber vulnerabilities. However, the oversight community continues to identify challenges in this area. In an April 2020 report, the GAO stated that cybersecurity experts estimate that 90 percent of cyber attacks could be prevented by implementing basic cyber hygiene controls and sharing best practices. To protect the DODIN and its data, the DoD needs to improve its cyber hygiene by reducing risk and mitigating or remediating identified vulnerabilities.

Operating during the coronavirus disease–2019 (COVID-19) pandemic required the DoD to provide significant remote access and telecommunication capabilities to support maximum teleworking and facilitate remote network connections to the DODIN for nearly 3 million Military Service members, civilians, and contractors. These connections from an individual's home network (via secure connection), in addition to other personal and smart devices sharing the same home network, significantly increased the number of potential vulnerabilities and risk of cyber attacks. These home network connections also highlighted the continued need for effective cyber hygiene. In a March 2021 report, the DoD OIG found that several DoD Components did not consistently implement required cybersecurity controls to protect DoD networks during maximum telework. The DoD OIG plans to perform audits in FY 2022 on the DoD's use of information technology (IT) collaborative software, used extensively during the pandemic, and the DoD's cybersecurity over remote and telework access.

[24] *Signal*, "DoD to Deliver Initial JADC2 in Coming Months," August 19, 2021.

One way the DoD is protecting its systems, networks, devices, and data is through the use of zero trust architecture. This architecture assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for unusual or malicious activity. In a February 2021 article from *C4ISRNET*, the Acting DoD CIO stated that one of his top priorities was to strengthen the DoD's cybersecurity by staying focused on cyber hygiene and adopting the zero trust architecture.[25] The transition to zero trust was accelerated due to the cybersecurity concerns brought on by the increased remote connections from the COVID-19 pandemic and the recent Federal breach through vendor software. In April 2021, the DoD released its Zero Trust Reference Architecture, which outlines how the DoD will implement zero trust across the DODIN to improve overall cybersecurity.[26] Zero trust architecture would embed cybersecurity through the DODIN and would assume that no user, system, network, or service operating outside or within the security perimeter is trusted by continuously verifying all activity.

Another way to protect the DODIN is through cybersecurity vulnerability management, but the DoD struggles to identify and mitigate known vulnerabilities. Test and evaluation (such as penetration testing) conducted early in a program or system's life cycle is intended to identify and mitigate vulnerabilities and improve system survivability and operational resilience. However, according to the FY 2020 Annual Report from the Director of Operational Test and Evaluation, the current DoD test and evaluation process is inadequate to keep pace with the volume of complex systems and aggressiveness of cyber attacks. Because the DoD cannot keep pace, it cannot identify all cyber-related vulnerabilities through test and evaluation processes.[27] Additionally, recent DoD OIG and GAO reports found that DoD Components did not take the necessary corrective actions in response to previously identified cyber vulnerabilities and continue to face challenges implementing cybersecurity practices, such as risk and vulnerability management.

The DoD cannot protect the DODIN from all cyber threats, and must prioritize and protect the most critical systems, networks, and data. To prioritize threats, the DoD developed a Risk Management Framework to integrate activities for selecting, implementing, and monitoring system security controls based on the designated system risk level. The Framework requires mission and system owners to identify and mitigate risks and vulnerabilities on their systems, networks, and devices in a timely manner. The DoD also has the Vulnerability Disclosure Program for a single focal point for receiving vulnerability reports and leveraging private sector cybersecurity experts. The DoD Vulnerability Disclosure Program processed 11,984 vulnerability reports for 2020, which was a 299-percent increase over the previous year. In January 2021, the program was expanded from all DoD public-facing websites to also include all public-facing information systems (accessible via the internet). Although the DoD is focused on identifying vulnerabilities, it is essential that it remains equally focused on reducing risks across the DODIN by mitigating and remediating vulnerabilities. To continue assessing the DoD's progress with vulnerability management, the DoD OIG has an ongoing audit

[25] *C4ISRNET*, "Pentagon Acting CIO Pushes on With Cybersecurity, Software Development," February 16, 2021.

[26] "DoD Zero Trust Reference Architecture," Version 1.0, dated February 2021, publicly released on April 28, 2021.

[27] Director, Operational Test and Evaluation, "FY 2020 Annual Report," January 13, 2021.

of the DoD's efforts to oversee its vulnerability identification and mitigation programs related to DODIN threats.

Improving DoD cyber hygiene and vulnerability assessment and detection programs are essential to combat the threats from adversaries seeking to exploit vulnerabilities in and gain access to DoD systems, networks, devices, and data.

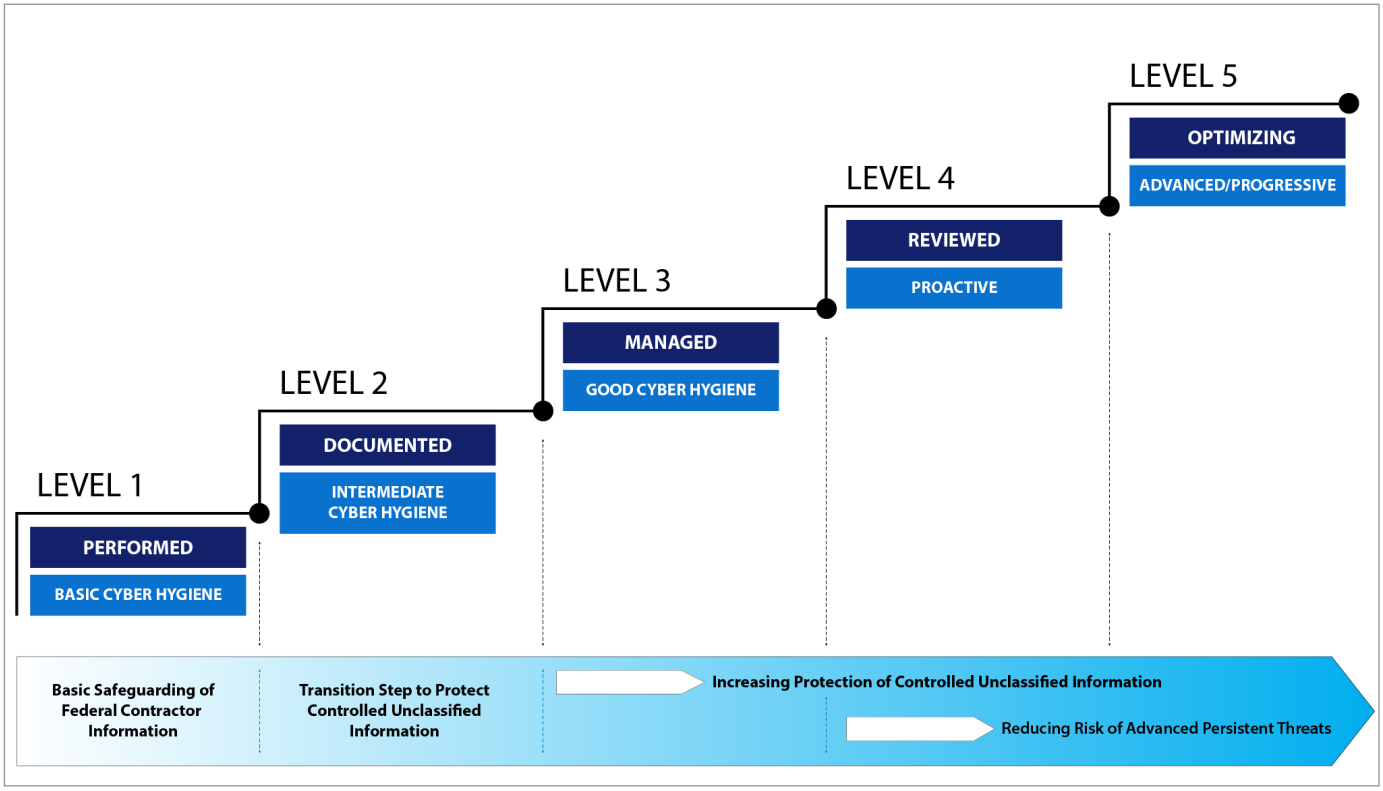
IMPROVING CYBERSECURITY IN THE SUPPLY CHAIN AND DIB

The DoD continues to face evolving threats to its supply chain and DIB, requiring the DoD to continually improve cyber hygiene and protect DIB systems, networks, devices, and data. In July 2021, a Russian-linked cybergang, REvil, claimed that it stole 23 gigabytes of data belonging to a Florida-based defense contractor that works on aerospace and weapon launch technology for the DoD and other Federal agencies.[28] To improve the cyber hygiene of the DIB, the Office of the Under Secretary of Defense for Acquisition and Sustainment implemented the Cybersecurity Maturity Model Certification (CMMC) process in 2021. Another way the DoD is seeking to improve cyber hygiene in the supply chain and DIB is through Cybersecurity Supply Chain Risk Management (C-SCRM).

The CMMC process is intended to verify that DIB contractors are implementing appropriate cybersecurity practices and processes to

[28] *Washington Times*, "Cybergang REvil Hits Defense Contractor," July 9, 2021.

CMMC Levels and Descriptions



Each CMMC level includes the processes and practices of the previous level. Level 1 is the most basic cyber hygiene to safeguard federal contractor information. Each level progresses in cybersecurity protections culminating in Level 5 where the cybersecurity is designed to protect controlled unclassified information and to reduce risk from advanced persistent threats. Advanced persistent threats are sophisticated and sustained cyber attacks where an intruder is undetected over a prolonged period.

Source: The Office of the Under Secretary of Defense for Acquisition and Sustainment.

protect DoD information stored within their unclassified networks. The private sector and the DIB have generally been receptive of the CMMC as an essential measure to secure sensitive information, but in 2021, small business owners testified to Congress that the costs associated with CMMC compliance will generally prevent them from competing for future defense contracts. DoD officials stated that the DoD is trying to reduce the cost of CMMC accreditation for small businesses. As discussed in Management Challenge 5, "Increasing Agility in the DoD's Acquisition and Contract Management," the DoD has struggled in getting nontraditional defense contractors to participate in the DoD's traditional acquisition process, which is slow and regimented. The DoD has attempted to increase agility in acquisition by reforming the acquisition process to increase the number of nontraditional contractors engaged with the DoD by using unique authorities that are less regulated, such as other transaction authorities. The DoD should implement the CMMC in a way that is responsive to concerns about the process and in a way that encourages small business and nontraditional defense contractors to participate in the DoD acquisition process. The DoD OIG planned to audit the CMMC process in FY 2022, but decided to postpone the audit after coordinating with the GAO, which was tasked by Congress to review the CMMC implementation.

C-SCRM is intended to identify, assess, and mitigate the risks and vulnerabilities associated with the distributed and interconnected nature of IT product supply chains for the entire life cycle of a system. The DoD currently has multiple pilot programs focused on enhancing DoD C-SCRM capabilities at the enterprise and programmatic levels. The DoD C-SCRM capabilities should help reduce supply chain risks within the DoD and assist with the development of enhanced techniques and procedures. For example, the DoD created a SCRM dashboard in collaboration with the General Services Administration, which provides a basic SCRM profile and continuous monitoring of a variety of products, including cybersecurity or IT-related products. To assess the DoD's progress with C-SCRM, the DoD OIG is conducting an audit to determine whether DoD Components and DIB contractors identified, responded to, and mitigated any compromise to their networks and systems, when using software that was recently targeted in a cyber attack. In FY 2022, the DoD OIG plans to conduct an audit that will determine whether the Defense Logistics Agency implemented Federal and DoD C-SCRM practices for products with IT hardware and software.

Improving the DIB and supply chain's cybersecurity is vital to combat the threat from adversaries seeking to exploit vulnerabilities in and gain access to relevant systems, networks, devices, and data.

USING AGILE SOFTWARE DEVELOPMENT TO CREATE CYBER RESILIENT SYSTEMS

According to the FY 2020 Annual Report from the Director of Operational Test and Evaluation, the DoD's ability to assess and protect its software is not keeping pace with our adversaries' ability to compromise it. Cybersecurity experts believe that more than 80 percent of breaches exploit known vulnerabilities in a software application. To build cyber-resilient systems capable of keeping pace with adversary abilities to exploit those systems, the 2019 DoD Digital Modernization Strategy states that the DoD plans to use agile software development approaches.

An Airman with the 60th Communications Squadron configures a switch at Travis Air Force Base, California, on September 23, 2021. Source: The Air Force.

In 2021, the Acting DoD CIO and the Under Secretary of Defense for Acquisition and Sustainment recognized "the urgent need to rethink [DoD] software development practices and culture by leveraging the commercial sector for new approaches and best practices."[29] To address this need, they issued the DoD Enterprise DevSecOps Strategy. DevSecOps—development (Dev), cybersecurity (Sec), and operations (Ops)—is an agile approach that ensures that cybersecurity is integrated in software development. Previously, developers would test for cybersecurity after the code for the software was completed. With DevSecOps, developers use automated cybersecurity test and evaluation while they write the software code, which allows the developers to build, test, and securely release software faster by reducing the manual assessments needed. Enabling security and functional capabilities to be tested and built simultaneously could lower development costs and allow for the deployment of secure software at a more rapid pace.

In a May 2020 memorandum, the DoD CIO designated Platform One, operated by the Air Force, as one of the DoD enterprise service providers for DevSecOps.[30] However, recent problems have impeded the DoD's use of the DevSecOps providers. According to a September 2021 *Federal Computer Week* article, the Air Force Chief Software Officer abruptly announced his resignation, citing a lack of support for his office, which oversees various software development projects, including Platform One.[31] A September 2021 *FedScoop* article stated that efforts to expand the use of software development capabilities, such as Platform One, have stalled after senior leaders raised cybersecurity concerns about these

[29] DoD, "DoD Enterprise DevSecOps Strategy Guide," March 2021.

[30] DoD Chief Information Officer Memorandum, "Designation of Enterprise Service Provider for DevSecOps," May 22, 2020.

[31] *Federal Computer Week*, "Air Force Chief Software Officer to Resign," September 2, 2021.

platforms.[32] To assess the DoD's progress in implementing DevSecOps, the DoD OIG plans to perform two audits in FY 2022 related to developing secure software using this method.

USING INNOVATIVE AND EMERGING TECHNOLOGIES TO IMPROVE CYBERSECURITY

Through recent innovations such as cloud computing, artificial intelligence (AI), and fifth-generation (5G) wireless technology, the DoD is focusing on the secure interconnectivity of its systems, networks, devices, and data. The DoD is challenged to implement these innovative and emerging technologies to stay ahead of adversaries and their increasingly sophisticated cybersecurity attacks. In his June 29, 2021 testimony to the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems, the Acting DoD CIO testified that it is urgent for the DoD to develop an enterprise-wide cloud capability that unlocks the power of AI capabilities and assists with organizing massive data sets.

Cloud computing is a fundamental component of the DoD's strategy to provide the warfighter with data and information critical to maintaining the U.S. military's technological advantage. The DoD is leveraging commercial cloud computing to increase its bandwidth, store and process large volumes of data, and implement technologies such as AI and a type of AI, machine learning. For example, the JADC2 concept previously discussed will leverage the Joint Warfighter Cloud Capability to connect all weapons systems and sensors extending out to the tactical edge. To assess the DoD's progress on implementing secure cloud computing, the DoD OIG has an ongoing audit to determine whether the DoD Components used approved cloud service offerings and ensured that cloud service providers maintained the necessary Federal and DoD cybersecurity requirements.

To improve network monitoring, the DoD plans to incorporate the use of AI to stay ahead of malicious actors and thwart cyber attacks. The Secretary of Defense stated at a 2021 summit on AI that the DoD must focus on incorporating AI into all aspects of warfare and intends to invest nearly $1.5 billion over the next 5 years.[33] The DoD plans to develop a machine learning tool that can more quickly detect cyber intrusions and enable a more rapid response. According to the Defense Information Systems Agency Director (also the Joint Force Headquarters-DODIN Commander), the DoD started a pilot project using machine learning and AI designed for early detection of cyberattacks on the DODIN. The early detection would help enable the defense of the DODIN proactively instead of reactively and provide an opportunity to more quickly identify the sources of attack and to make informed decisions.[34] Based on the results of the AI pilot project, the DoD plans to determine whether this capability could be leveraged DoD-wide.

In addition, the DoD plans to implement 5G technologies to accelerate the secure connectivity of mobile devices, while ensuring that those devices and systems are protected, resilient, and reliable. 5G wireless communication systems are the new global wireless standard designed to transport voluminous data, including sensitive information military operations at the tactical edge. In 2020,

[32] *FedScoop*, "Air Force Software Platform Expansion Stalled by Cybersecurity Concerns," September 14, 2021.

[33] DoD, "Secretary of Defense Austin Remarks at the Global Emerging Technology Summit of the National Security Commission on Artificial Intelligence (As Delivered)," July 13, 2021.

[34] *Signal*, "DISA, JAIC Developing AI-Enabled Cybersecurity Tool," December 1, 2020.

the DoD issued two strategic plans that outline the DoD's overall approach to implementing secure 5G communications and to define the lines of effort to achieve the DoD's goals with respect to implementing and using 5G technology, thereby accelerating the DoD's secure digital transformation efforts.[35] The lines of effort include assessing vulnerabilities, a key part of implementing any technology. If the DoD's 5G network was compromised, the malicious actor would gain unauthorized access that could potentially compromise operations; violate the privacy of military personnel, civilians, and contractors; or disrupt critical infrastructure. To assess the DoD's progress with 5G communications, in FY 2022, the DoD OIG plans to audit the DoD's implementation of secure 5G wireless communications technologies, including the mitigation of associated cybersecurity risks.

Successfully integrating new technologies and capabilities into existing DoD systems and networks is essential to maintaining security and improving cyberspace operations.

CONCLUSION

DoD innovation is key to protecting the systems, networks, devices, and data of the DoD, supply chain, and DIB. Increasing the DoD's capability to share information and integrate systems and processes is vital. The DoD must develop and deliver new cyber capabilities that can meet the evolving threat from strategic competitors and other malicious actors seeking to exploit vulnerabilities in the DODIN. The DoD must also remain focused on improving cyber hygiene across the DODIN and the DIB to combat threats from adversaries seeking to exploit vulnerabilities and gain access to systems, networks, devices, and data. Using new technologies to monitor and adjust to emerging threats will be imperative to cyber operations and cybersecurity. By continuously identifying, addressing, and adapting to evolving challenges, the DoD can improve its cyberspace operations and defend the DODIN.

[35] DoD, "5G Strategy," May 2, 2020. DoD, "5G Strategy Implementation Plan," December 15, 2020.

USS Pasadena (SSN 752) arrives at Norfolk Naval Shipyard on September 28, 2020, for drydocking to replace, repair, and overhaul boat components. (U.S. Navy photo)

Challenge 4. Reinforcing the Supply Chain While Reducing Reliance on Strategic Competitors

INTRODUCTION AND OVERVIEW

Globalization and the decline in American manufacturing have negatively impacted the Defense Industrial Base (DIB) and resulted in limited sources of supply, reliance on foreign sources of supply, and other challenges related to maintaining major weapon systems and military equipment. As stated in the FY 2020 Industrial Capabilities Report to Congress, "the DIB is the key to preserving and extending U.S. competitive military dominance in the coming century and, with it, deterrence that will keep Americans safe and keep the peace."[36] The DIB designs, produces, and maintains the platforms and systems on which our military depends. With an extensive, multi-tiered global supply chain, the DIB plays a role in every aspect of a system's life cycle from extraction of raw materials to sustainment.

The DoD must focus resources on critical industries, such as shipbuilding and semiconductors, and increase capabilities by partnering with industry and allies. Increased collaboration with allies will reinforce the supply chain and reduce reliance on strategic competitors. As the DoD fields new equipment and technologies, it must also allocate resources for sustainment, a significant portion of an item's life-cycle management. Finally, the DoD must use all available means to support small and midsize businesses in the DIB, which are integral to the supply chain, but economically vulnerable due to their reliance on DoD contracts. Addressing the U.S. manufacturing decline and reliance on foreign sources requires continued focus and will challenge the DoD for years to come.

[36] Office of the Deputy Assistant Secretary of Defense for Industrial Policy, "FY 2020 Industrial Capabilities Report to Congress," January 2021.

IMPROVING THE DIB AND SUPPLY CHAINS IN KEY INDUSTRIES TO MAINTAIN COMPETITIVE ADVANTAGE

According to the FY 2020 Industrial Capabilities Report to Congress, the continued deindustrialization of the United States has led to a reduction in U.S.-based manufacturing, which has shrunk as a percent of gross domestic product from 40 percent in the 1960s to 12 percent in 2021. This decline in manufacturing had a corresponding impact on the number of workers in manufacturing positions. According to *The Economist*, in 1970, the manufacturing industry employed about 25 percent of all workers.[37] Today, manufacturing employs fewer than 11 percent of all workers. Causes for this reduction in the manufacturing workforce included the jobs becoming more highly skilled, workers being less willing to move for a job, and U.S. competition with China.[38]

Similar to the declines in manufacturing and the workforce, the number of defense contractors has reduced from 15 large defense contractors at the end of the Cold War to just 5 large defense contractors today. Fewer sources of supply leads to challenges related to over-reliance on foreign sources, limited competition, and increased risk of product or maintenance delays. Limited sources of supply can also increase prices because of the scarcity of needed supplies and lack of competition among vendors. For more information on limited and sole sources of supply and the impacts from a lack of competition, see Management Challenge 5, "Increasing Agility in the DoD's Acquisition and Contract Management."

Past and current administrations recognized the adverse impact that the shrinking manufacturing base and DIB could have on national security, and issued executive orders for the DoD to assess and develop methods to build resiliency, agility, and strength back into the DIB.[39] In response to a February 2021 Executive Order on U.S. supply chains, the Administration issued a report containing 100-day reviews performed by the Departments of Defense, Commerce, Energy, and Health and Human Services on four industries—(1) semiconductor manufacturing and advanced packaging, (2) large capacity batteries, (3) critical minerals and materials (also known as rare earth elements), and (4) pharmaceuticals and their ingredients. The June 2021 report on U.S. supply chains included recommendations for Congress to:

- enact a program to identify and mitigate supply chain vulnerabilities; and
- provide $50 billion in funding to give Federal agencies the tools necessary to make transformative investments to strengthen the U.S. supply chain across a range of critical products.[40]

To ensure an advantage against strategic competitors and reduce reliance on foreign suppliers, the DoD must invest in two key industries—shipbuilding and microelectronics. Furthermore, as the DoD develops new technologies such as artificial intelligence, fifth generation (5G) wireless technology, and hypersonics, it must invest in the corresponding

[37] *The Economist*, "Industrial Metamorphosis," October 1, 2005.

[38] Bureau of Labor Statistics, Monthly Labor Review, "The Fall of Employment in the Manufacturing Sector," August 2018.

[39] Executive Order 14017, "Executive Order on America's Supply Chains," February 24, 2021, and Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," July 21, 2017.

[40] "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017," June 2021, by the White House, including reviews by the Departments of Commerce, Energy, Defense, and Health and Human Services.

supply chain and DIB to ensure that the new technology can be sustained effectively and securely.

INVESTING IN SHIPBUILDING

To project power and sustain its competitive advantage, the United States must invest in capabilities to produce and maintain ships. China continues to outpace the United States in shipbuilding, taking advantage of China's rapidly expanding commercial shipbuilding industry. As a result, China has the largest naval fleet in the world, estimated at more than 350 ships and submarines. By contrast, according to the FY 2020 Industrial Capabilities Report to Congress, shipbuilding has become a key vulnerability for the DoD. The National Defense Authorization Act (NDAA) for FY 2018 required a Navy battle force of 355 ships. However, as of July 2021, the U.S. fleet stood at 296 ships.

Currently, the Navy primarily contracts with seven shipyards owned by four U.S. companies. For nuclear-powered submarines, the Navy relies on just two U.S. companies. The limited number of facilities and suppliers creates a reliance on sole source and single source procurements that reduces competition, and puts the DoD at risk for paying higher prices and suffering potential delays in ship and submarine construction and maintenance.

The capacity, condition, and configuration of the Navy's four public shipyards are insufficient and must be addressed to prevent maintenance delays at the shipyards. In August 2020, the Government Accountability Office (GAO) reported that from FYs 2015 through 2019 the Navy's shipyards completed 75 percent of aircraft carrier and submarine maintenance late. According to the GAO report, the average maintenance delay was 113 days for carriers and 225 days for submarines.[41] In response to these concerns, the Navy developed the Shipyard Infrastructure Optimization Plan, which outlines $21 billion in investments to the public shipyards. The Navy's plan calls for significant improvements including dry dock repairs, restoring and moving shipyard facilities, and replacing aging equipment. However, the Shipyard Infrastructure Optimization Plan is based on the size of the current fleet and does not account for growth. In addition, the plan assumes timely completion of projects and accurate cost estimates. Lastly, the Navy must consider the impact of extreme weather and rising sea levels to ensure shipyard resilience. For more information on the effect of climate change on DoD installations, see Management Challenge 7, "Building Resiliency to Environmental Stresses."

The Navy's Report to Congress on the Long-Range Plan for Maintenance and Modernization of Naval Vessels for FY 2020 highlighted the need for infrastructure improvements and an increase in certified dry docks at private shipyards to support the current inventory and the newer classes of ships.[42] The high ratio of ships to dry docks presents a unique challenge, especially as the Navy fleet grows in size. As laid out in the Navy's report to congress, there are only 21 certified dry docks used for scheduled ship maintenance. Although the Navy continues to adjust maintenance schedules, workload forecasting has historically been difficult due to unplanned work not included in final maintenance requirements. Inadequate and aging shipyard infrastructure hinders the Navy's ability to timely return ships to sea to project

[41] Report No. GAO-20-588, "Actions Needed to Address the Main Factors Causing Maintenance Delays for Aircraft Carriers and Submarines," August 20, 2020.

[42] U.S. Navy, "Report to Congress on the Annual Long-Range Plan for Naval Vessels for Fiscal Year 2020," March 2019.

naval power. The Navy, in coordination with the private shipyards, must make adequate investments so that private shipyards can support timely ship maintenance.

The DoD can mitigate the effects of these challenges by providing a stable demand signal to the shipbuilding industrial base. The DoD has struggled to provide predictable requirements to shipbuilders to ensure a healthy industrial base. The DoD has publicly stated that requirements for its fleet have varied from as low as 321 ships to as high as 446 ships. This variance makes the true need unclear, and the industry cannot adequately prepare to support shipbuilding contracts. Additionally, the Navy plans to decommission legacy platforms and systems, which often incur higher maintenance costs, and reinvest those resources to develop new capabilities. This strategy assumes that the Navy can build enough ships at a rate fast enough to replenish the decommissioned ships. Government and independent studies have highlighted the need for a larger, more capable Navy to maintain critical sea advantages against strategic competitors. The DoD must carefully balance industry capacity, current fleet readiness, and future capabilities within fiscal constraints to ensure that its forces can deter and win conflict against a strategic competitor.

The Navy must improve antiquated infrastructure at shipyards and expand its maintenance capacities to sustain its fleet. To meet this challenge, the DoD must invest in public and private shipyards that perform maintenance by ensuring a planned and steady workload for these shipyards.

INVESTING IN MICROELECTRONICS AND RESHORING SEMICONDUCTOR PRODUCTION CAPABILITIES

Semiconductors (also known as microchips), used in microelectronics, are essential to national security. According to the June 2021 report on U.S. supply chains:

> [s]emiconductors enable the development and fielding of advanced weapons systems and control the operation of the nation's critical infrastructure. They are fundamental to the operation of virtually every military system, including communications and navigations systems and complex weapons systems such as those found in the F-35 Joint Strike Fighter.

The DoD is at risk of having shortfalls in semiconductors due to reliance on foreign sources of supply and the need for larger quantities of semiconductors as emergent and new technologies, such as artificial intelligence, become more pronounced. The risk has increased because the pandemic reduced available supply and delayed shipments. Also, the lack of U.S.-based investment and innovation in semiconductor technology, and the DoD's history of purchasing safely produced semiconductors that are less advanced than those produced for the commercial market, contribute to this risk. Furthermore, there are security and transportation risks related to the most advanced semiconductors, which are produced by countries located close to China, a key strategic competitor. The DoD must bolster American innovation and consider reshoring (bringing manufacturing services back to the United States from overseas) production of technologically advanced semiconductors to ensure U.S. dominance in this vital industry. Another benefit of reshoring semiconductor production is creating manufacturing jobs.

Taiwan and South Korea control a large percentage of semiconductor manufacturing. In addition, China has begun to develop and produce high-end microchips as a domestic industry.[43] The U.S. share of global manufacturing capacity for semiconductors has eroded from 37 percent in 1990 to 12 percent in 2021. One reason for the erosion in U.S. capacity is that the governments of other countries invested ambitiously in chip manufacturing incentives and the U.S. Government did not. The U.S. Government recognized this trend and increased investments in the American semiconductor industry through funding provided in the FY 2021 NDAA and by using the Defense Production Act (DPA). The FY 2021 NDAA established a financial assistance program to incentivize the DoD to invest in facilities and equipment in the United States for semiconductor fabrication, assembly, testing, advanced packaging, and research and development.

In addition, the DoD has used the DPA and funding from the Coronavirus Aid, Relief, and Economic Security (CARES) Act to bolster the semiconductor industry in the United States. For example, in September 2020, the DoD announced that it used $1.9 million in CARES Act funding to establish a DPA agreement with a small business to sustain and advance domestic capabilities for aerospace grade optical sensors, a type of microelectronic. These sensor capabilities are essential for national defense, and the funding helped retain the highly skilled staff at risk during the pandemic that would be difficult to backfill if lost. In another example, in March 2021, the DoD used a combination of the DPA and a contract from the DoD Industrial Base Analysis and Sustainment office to provide a combined $14 million to an American company for volume production of advanced packaging solutions for computer chips embedded within defense systems. Access to secure, state-of-the-art microelectronics used by military systems such as DoD aircraft, ground vehicles, and complex weapon systems is critical to ensuring our Nation's technological advantage.

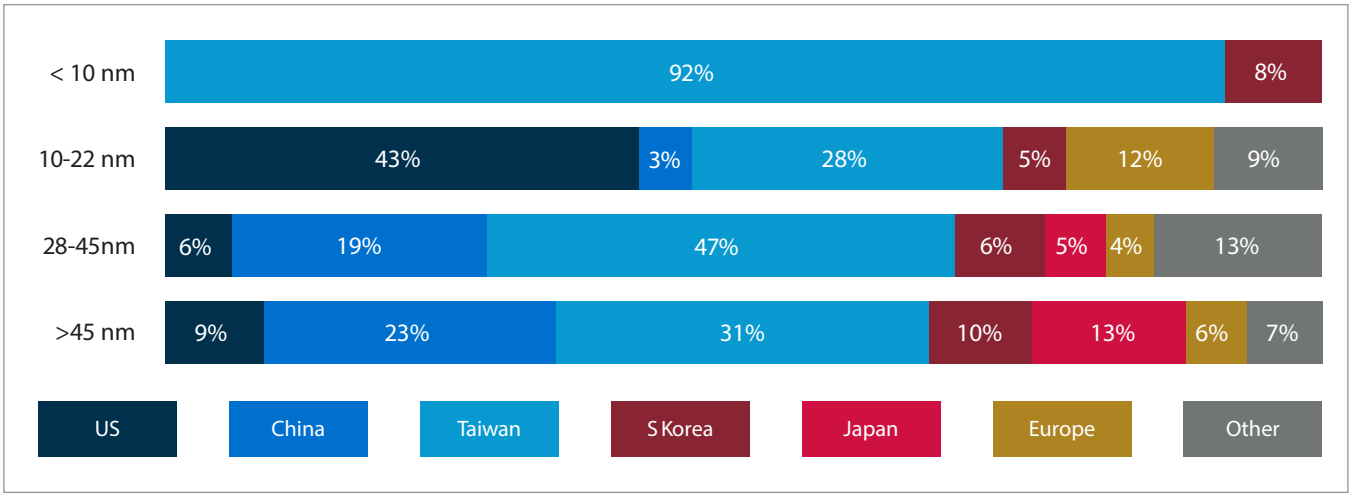
As previously mentioned, Asia produces most of the world's semiconductors. More specifically, Taiwan produces the most technologically advanced and the largest quantity of microchips that the world uses. Intel, the only U.S.-based company that produces microchips, plans to devote $20 billion to building two fabrication facilities in the United States. Intel broke ground on the facilities in September 2021 and plans to be fully operational by 2024. However, Intel still does not have the ability to produce the kind of advanced microchips needed for DoD weapon systems and does not have the kind of commercial clients that can provide needed resources to further advance microchip technology. Alternatively, according to a May 2, 2021 *60 Minutes* report, the Taiwan Semiconductor Manufacturing Company, which has more than half of the market share for the semiconductor industry:

- produces microchips 30 percent faster and more powerful than Intel's;
- plans to spend $100 billion on research and development and building a fabrication facility in the same state as Intel; and
- has major commercial clients, such as Apple, whose demand for microchips can fund research and development and innovation in advanced microchips.[44]

[43] *Developing Telecoms*, "China Gets Serious About Microchips," July 27, 2021.

[44] CBS News, *60 Minutes*, "Chip Shortage Highlights U.S. Dependence on Fragile Supply Chain," May 2, 2021.

Global Manufacturing of Semiconductors by Size in 2019



Nm Nanometer

The power of semiconductors is generally measured in nanometers. According to the Semiconductor Industry Association, the most advanced semiconductors are less than 10 nanometers and in 2019 were all produced outside of the United States.

Source: The Office of the Under Secretary of Defense for Acquisition and Sustainment.

There are two main security concerns with semiconductors. The first is the proximity of Taiwan to China. Protecting Taiwan from aggression from China is important for ensuring access to semiconductors, not just for the United States, but also for U.S. allies and partners. Protecting the supply chains in the semiconductor industry is imperative to national security. According to a May 28, 2021 statement by the Secretary of Defense, the President's FY 2022 budget request to Congress included $2.3 billion for investments in microelectronics specific to the DoD.

The second security concern is with the supply chain of semiconductors and microelectronics. According to the June 2021 report on U.S. supply chains, the semiconductor supply chain "is extremely complex and geographically diverse" with the typical production process including multiple countries and crossing international borders up to 70 times. To protect itself, beginning in the 1990s, the DoD began using the "trusted foundry" model for purchasing microelectronics. This model ensured that the DoD had control over the foundries that manufactured its microelectronics, but the model left the DoD at risk to insider threats and did not give the DoD access to the most modern microelectronic technology available commercially.

In March 2020, the DoD announced that it was switching to a "zero trust" model for buying microelectronics—assuming that the microelectronics are not safe and secure and instead validating and verifying the security of the products before use. The use of the zero trust model is intended to allow the DoD access to the most current microelectronics. In October 2020, the DoD OIG began an evaluation of the DoD's transition from the trusted foundry model to the zero trust model for procuring microelectronics.

The DoD must continue to invest in U.S-based production and innovation of semiconductors and microelectronics and enhance the security of microchip production outside the United States to protect the U.S. technological advantage.

BUILDING THE DIB AND SUPPLY CHAINS TO SUSTAIN NEW TECHNOLOGY

Once the DoD acquires the systems it needs, it must sustain those systems. Sustainment is a vital aspect of life-cycle management, with an estimated 70 percent of life-cycle costs for a system going toward sustainment. However, sustainment costs are often discarded or used as a trade-off during the requirements process. Planning, funding, and ensuring a strong DIB and supply chain for sustainment is critical. As contractors consolidated over the past half-century, this consolidation reduced the available sources of supply. As microeconomic principles dictate, when there are fewer sources of supply, costs increase, and costs continue to increase along with demand. The DoD is committed to developing new technologies, but it must also commit to appropriately sustaining those technologies for as long as they are relevant. Often the DoD extends the life of weapon systems far beyond what was ever intended, which is why sustainment is so vital. For example, the DoD has used the B-52 Bomber for more than 60 years, with the newest B-52 Bomber reaching 50 years of service in October 2012. The DoD must ensure that sustainment is not sacrificed as a way to reduce costs, but considered an essential part of acquiring new systems.

REDUCING RELIANCE ON COMPETITORS AND INCREASING COLLABORATION WITH ALLIES

The decrease in U.S.-based manufacturing created the current reliance on competitors for critical supplies such as medical supplies and rare earth elements. The United States cannot work alone to build a more robust and agile DIB and supply chain, it must work with its allies. The DoD has several avenues to building up U.S. and ally-based manufacturing and supply chains and to ensure that it increases partnerships with industry to encourage innovation. These avenues include the previously mentioned DPA, which allows the DoD to fund increased or new production in support of national security objectives; but also the National Technology Industrial Base, bilateral supply arrangements, and reciprocal defense agreements. These arrangements and agreements allow the United States to work with allies for mutually beneficial supply and production of goods and services to ensure national security and technological superiority.

According to a December 2020 Congressional Research Service report on China medical supply chains, reduced exports from China during the pandemic resulted in shortages of personal protective equipment, medical devices, antibiotics, and active pharmaceutical ingredients.[45] The Congressional Research Service also notes that early in the pandemic, China nationalized control of medical supply production and distribution and directed that all produced supplies be used domestically. The lack of supply caused the United States to access its stockpiles and increase domestic manufacturing of medical items such as personal protective equipment by using the DPA and

[45] Congressional Research Service, "COVID-19: China Medical Supply Chains and Broader Trade Issues," updated December 23, 2020.

CARES Act funding. The U.S. Government will need to consider how it can work with allies and partners to reduce reliance on a strategic competitor for medical supplies, especially in case of another pandemic.

As discussed in last year's challenge, China produces significant amounts of rare earth elements, which the DoD uses in major weapon systems and are also used in medical devices. The DoD continued to make strong investments in the industry through the use of the DPA. On September 10, 2020, the Defense Logistics Agency increased the scope of its Rare Earth Salts Rapid Innovation Fund project to expand production of a rare earth element at a Nebraska facility. The company made its first deliveries of the element to an industry partner in 2020. Also, on November 17, 2020, the DoD announced three contracts, valued at $12.8 million, to establish domestic processing capabilities for light rare earth elements (used in both defense and commercial applications), add processing and separation capabilities to a refining site, and study rare earth magnet supply chains.[46] Last year the DoD used DPA funding to create rare earth element separation facilities with an Australian company. Working with allied nations is important, but must be tempered with the knowledge that relationships may change over time. The F-35 Program serves as a cautionary tale, where the DoD relied on parts produced in Turkey, but when the diplomatic relationship with Turkey changed, the United States had to seek an alternative means to produce those parts.

The DoD must also ensure that national interests are protected from foreign influence, including the materials and businesses used to build up the domestic and ally DIB. The Committee on Foreign Investment in the United States received expanded authorities from the Foreign Investment Risk Review Modernization Act of 2018, to protect American companies that work in the national security arena. With the increase in authorities and foreign investment, officials from the office responsible for evaluating DoD cases that go to the Committee stated that the cases increased from about 350 to 700 (100 percent) in a year.

Finally, the DoD has the Trusted Capital program, which helps open the market for better competition, provides stable funding from vetted sources, and ultimately offers the DoD access to cutting-edge technology. The program has a marketplace where trusted sources of private capital can meet with innovative domestic companies to work on emerging technologies and strengthen domestic manufacturing while limiting foreign access to critical technology. Building a stronger and more robust DIB and supply chain, secure from foreign influence, is critical to national defense.

MITIGATING DOMESTIC SUPPLY CHAIN AND DIB VULNERABILITIES HIGHLIGHTED BY THE PANDEMIC

The coronavirus disease–2019 (COVID-19) pandemic highlighted the need for increased U.S. and allied nation production of critical supplies and led to temporary shutdowns or slowdowns of DIB operations. According to the Defense Contract Management Agency, between June 2020 and February 2021, 94 DoD programs experienced a delay related to the pandemic. As of March 15, 2021, 40 programs still had delays of about 2 months. Of particular concern are small and midsize businesses that rely on steady payments from DoD contracts or rely on their subcontracting or supplier relationship with larger businesses in the DIB. The small and

[46] DoD, "DoD Announces Rare Earth Element Awards to Strengthen Domestic Industrial Base," November 17, 2020.

midsize businesses are more at risk because of their limited resources. The DoD used COVID-19 stimulus funds and the DPA to increase the production of needed supplies in the United States and provide some stability to the DIB.

From May 2020 through June 2021, the DoD announced a total of about $696 million in DPA actions to help sustain defense-critical workforce capabilities, directly offset financial distress to the most adversely impacted organizations in the DIB, and produce needed medical supplies and equipment. Specifically, DPA actions used CARES Act funding streams, in the medical, aviation, shipbuilding, space technology, electronics, clothing and textiles, satellite solar array panels, rare earth materials, and body armor industries. Keeping the DIB ready and working is an important aspect of power projection, ensuring that the United States does not appear economically weak to competitors such as China, which according to a March 2021 *Bloomberg* article experienced a faster economic recovery than the United States.[47]

While increased use of the DPA and the funding provided by the CARES Act helped to support the DIB during the pandemic, the CARES Act funding was limited by amount, purpose for which the funds could be used, and timeframe in which the funds could be used. The DoD must find ways to innovate and change the way it does business, including increasing collaboration with allies, to ensure that the supply chain and DIB are resilient.

CONCLUSION

A healthy DIB is critical to preserving and extending U.S. competitive military dominance. The decline in the domestic DIB has resulted in limited sources of supply and reliance on foreign sources. The COVID-19 pandemic further exacerbated these vulnerabilities within the DIB and supply chain. The DoD must continue to focus on supply chain resilience and target investments in critical industries such as domestic shipbuilding and microelectronics to maintain strategic advantages and reduce reliance on foreign sources of supply. The U.S. Government used the DPA and other initiatives to protect the DIB. However, collaboration with allies and strategic investments are critical components to combat limited sources of supply and dependency on countries like China. Strengthening the DIB will take time and continued attention, but is essential for the DoD to ensure that its national defense objectives are met now and in the future.

[47] *Bloomberg*, "China's Covid Rebound Edges it Closer to Overtaking U.S. Economy," March 30, 2021.

Airmen from the 40th Flight Test Squadron, and 85th Test & Evaluation Squadron, deliver the first F-15EX to its new home station, Eglin Air Force Base, Florida, on March 11, 2021. (U.S. Air Force photo)

Challenge 5. Increasing Agility in the DoD's Acquisition and Contract Management

INTRODUCTION AND OVERVIEW

Acquisition and contracting are how the DoD develops and buys the products and services needed to effectively perform its mission. DoD spending on contracts is significant, with $422 billion obligated on contracts for goods and services in FY 2020. Those obligations were more than 59 percent of the DoD's $714 billion budget in FY 2020. Through the third quarter of FY 2021, the DoD had obligated $272 billion toward contracts. Acquisition and contract management are enduring challenges, regularly appearing in the DoD OIG's Top Management Challenges and remaining on the Government Accountability Office's (GAO) High-Risk List since the mid-1990s.

Strategic competitors, such as China, aim to outpace the United States in developing and fielding technology, including military weapon systems and other defense capabilities. Efficient and rapid acquisition and astute contract management are vital to building and maintaining the DoD's military and national security advantage and to developing and deploying cutting-edge technologies.

The DoD has attempted to address some of the longstanding challenges by implementing acquisition reforms designed to streamline the acquisition process and other transactions (OTs) to gain access to commercial technologies and nontraditional defense contractors. However, the results of acquisition reforms and using OTs are mixed. Furthermore, using the traditional acquisition process for weapon systems has led to DoD weapon systems having cost overruns, schedule delays, and performance shortfalls. Lastly, the DoD struggles to obtain the data necessary to determine whether it is paying a fair and reasonable price because the DoD has been limited by law and regulation in its ability to obtain that data for commercial and sole-source items.

EXECUTION OF ACQUISITION REFORM AND RAPID ACQUISITION

The March 2021 Interim National Security Strategic Guidance states that the DoD will streamline the processes for developing, testing, acquiring, and deploying cutting-edge technologies and capabilities. The Secretary of Defense acknowledged that fielding new capabilities continues to proceed at a slower pace than is required to address the challenges the DoD faces from strategic competitors.[48] In March 2021, the Defense Innovation Unit Director stated that China already leads in some technologies and that the United States is in a superpower marathon with China for technological dominance.[49] To improve its ability to field new technology faster, the DoD has implemented acquisition reforms that provide greater flexibility and unique pathways for acquiring goods and services. While the DoD has not always developed capabilities that meet its needs in a timely manner, the DoD has seen recent success using the middle-tier pathway and the software acquisition pathway.

One of the unique pathways for acquiring new capabilities rapidly is the middle-tier acquisition pathway. The middle-tier pathway is used to develop new capabilities quickly, within 5 years. In September 2018, the Army used the middle-tier acquisition pathway to rapidly prototype the Integrated Visual Augmentation System. This future capability will allow Service members operating in certain environments

[48] Senate Armed Services Committee, Advance Policy Questions for Lloyd J. Austin, Nominee for Appointment to be Secretary of Defense.

[49] DoD, "Defense Innovation Leader Stresses Importance of U.S., China Technology Race," March 25, 2021.

Soldiers don the Integrated Visual Augmentation System Capability Set 3 hardware while mounted in a Stryker at Joint Base Lewis-McCord, Washington, on February 19, 2021.

Source: The Army.

to wear goggles that offer a variety of sensor capabilities, such as night vision and thermal imaging, and augmented reality, to enhance combat effectiveness. The DoD has invested an estimated $964.3 million in research, development, test, and evaluation, and the total estimated procurement costs are $2.4 billion. However, the system prototypes have had low user acceptance during testing. In March 2021, the Director of Operational Test and Evaluation issued a report stating that 84 percent of Soldiers and 61 percent of Marines indicated that they did not believe that the Integrated Visual Augmentation System contributed to their ability to accomplish their mission.[50] The DoD OIG plans to perform an audit of the Integrated Visual Augmentation System in FY 2022. While the DoD is making progress in rapidly developing systems through new acquisition pathways, the DoD must ensure that these systems meet the DoD's needs.

In addition to the middle-tier acquisition pathway, 16 DoD Components have used the new software acquisition pathway that became effective in October 2020. The software acquisition pathway facilitates timely acquisition of custom software capabilities and better enables the DoD to continuously develop and deploy new technologies to maintain the competitive edge. For example, the Algorithmic Warfare Cross Functional Team used the software acquisition pathway for Project Maven. The project, with a budget of $502 million in FYs 2021 and 2022, uses artificial intelligence to fuse operations and intelligence to help mission commanders, operators, and intelligence analysts in every domain of warfare. Though the software acquisition pathway became effective just one year ago, according to a May 2021 *FedScoop* article, the Acting Under Secretary of Defense for Acquisition and Sustainment said that initial results were positive.[51]

With competitors, such as China, developing and fielding new capabilities at accelerated rates, the DoD must continue to use the flexible acquisition pathways and implement lessons-learned to ensure that it is getting the right capability to the right user at the right time.

OTHER TRANSACTIONS

OTs are another way that the DoD can improve agility and reduce barriers in acquisition and contracting. OTs make it easier for the DoD to adopt commercial industry standards and best practices and access state-of-the-art technology from nontraditional defense contractors. According to an August 2021 *Defense News* article, from 2018 to 2019 there was a 75 percent increase in the DoD's use of OTs; however, the DoD lacks data on OTs or metrics to measure success.[52] Without data or metrics for OTs, the DoD cannot be sure that OTs are resulting in:

- commercial capabilities being fielded faster,
- more nontraditional contractors working with the DoD, or
- taxpayer funds being put to their best use.

OTs are generally not subject to as much regulation as traditional contracts and are exempt from having to follow the Federal Acquisition Regulation (FAR). With the decreased regulations that govern OTs comes the increased need for DoD officials to provide effective oversight to protect Government interests and ensure the proper use of taxpayer

[50] Director, Operational Test and Evaluation, "Integrated Visual Augmentation System (IVAS) Capability Set 3 Operational Assessment," March 2021.

[51] *FedScoop*, "DoD Procurement Lead Says Software Acquisition Changes Are Yielding Results," May 21, 2021.

[52] *Defense News*, "The Goldilocks Principle: Getting Rapid Contracting 'Just Right'," August 31, 2021.

funds. In February 2020, the Army Audit Agency reported that OTs need safeguards so that contracting officials can assess and mitigate risks; ensure that contractors can meet technical, schedule, and cost expectations; and ensure that invoices are supported and properly approved before payment.[53]

Additionally, in April 2021, the DoD OIG reported that DoD contracting personnel did not properly track, have an accurate count of, or know the associated dollar values of OTs awarded to consortiums (when two or more individuals, companies, or organizations act as one).[54] The DoD OIG also found that DoD contracting personnel did not consistently award OTs or have a consistent approach for negotiating the fees associated with managing a consortium. As a result, DoD officials did not have access to important data associated with OTs awarded through consortiums, such as which contractor received the OT award and the specific costs associated with funded OT projects.

With the DoD spending approximately $15.8 billion on OTs in FY 2020, the need for complete and accurate data and metrics on the use of OTs is imperative. With accurate data and metrics, the DoD can make well-informed decisions about OTs and determine whether they are effective.

THE ACQUISITION PROCESS

The DoD continues to have challenges with managing major defense acquisition programs. The GAO reported in 2020 that the DoD plans to invest more than $1.8 trillion in 93 current and future programs, to acquire weapon systems such as aircraft, ships, and satellites.[55] Although the Military Services are working toward fielding capabilities faster, the DoD's ability to acquire weapon systems to meet operational requirements and maintain an advantage against strategic competitors is slowed by continuous requirement changes, schedule delays, and cost overruns.

For example, the USS *Gerald R. Ford* nuclear aircraft carrier is the costliest single weapon system that the DoD owns, with a cost of $13.2 billion, and it has taken 2 decades to complete. With China aggressively building ships, the DoD must produce more ships and produce them faster to remain competitive. In 2001, the Navy started spending for the USS *Gerald R. Ford* nuclear aircraft carrier. The aircraft carrier is 27 percent over budget, in part, because the Navy started this acquisition program with technologies that did not exist and had to be developed as the ship was designed and built. In July 2021, the Chief of Naval Operations acknowledged that the decision to introduce 23 new technologies at once was a mistake. The DoD must be mindful of introducing too many in-development or emerging technologies at one time because it can introduce unnecessary risks and delays to the program.

The Military Services must also carefully balance their weapon systems portfolios and consider which programs to continue, which programs to divest, and which programs to develop as the DoD works to maintain a competitive advantage in times when the Congressional Budget Office

[53] Report No. A-2020-0038-BOZ, "Other Transaction Authority Control Environment," February 27, 2020.

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

[55] Report No. GAO-20-439, "Defense Acquisitions Annual Assessment: Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight," June 3, 2020.

projects the DoD budget to have nominal, if any, growth. For example, the Air Force is simultaneously:

- operating legacy F-15 Eagle and F-16 Fighting Falcon fighter jets and modern F-22 Raptor and F-35 Lightning II fighter jets;
- planning to divest more than 200 aircraft in FY 2022, including 48 F-15C and F-15D models;
- developing and purchasing F-35 Lighting IIs;
- developing and purchasing newer versions of the F-15, the F-15EX Eagle II; and
- developing new fighter aircraft for its Next Generation Air Dominance Program.

Although this is an Air Force example, as the Secretary of Defense testified in June 2021, all of the Military Services are "making tough choices in terms of what to prioritize."[56] Making strategic decisions to allocate funding between maintaining legacy systems, modernizing systems, and developing future systems is a continuing challenge for the DoD.

PRICING FOR COMMERCIAL ITEMS

In recent years, the DoD has found it more difficult to determine whether it is paying a fair and reasonable price for the items it buys. Previous National Defense Authorization Acts (NDAAs) broadened the definition of a commercial item and required the DoD to use commercial buying practices. Corresponding changes to the commercial section of the FAR require the DoD to continue to purchase an item commercially if it has previously purchased the item that way. The consequence of these commercial buying practices is that contractors can deny the DoD access to cost and pricing data related to that item, which contracting officers need to determine whether the contractor is charging the DoD a fair and reasonable price.

The commercial item initiative within the Federal acquisition system was intended to streamline the contracting process, result in lower prices, and reduce the amount of time it took to acquire items. However, purchasing items commercially often results in the DoD paying excessive prices because it does not have access to the cost data to determine how much of the price charged is profit and how much is the actual cost to produce the item. For example, the DoD OIG found that a commercial part cost the contractor $199 to produce. However, the contractor charged the DoD $746 for that part, earning $547 in profit for each part it sold to the DoD. Often the DoD purchases parts in large volumes, sometimes by the thousands. Because this was a commercial item, the contractor could refuse to provide cost and pricing data to the DoD. In addition, the DoD does not capture or track data that it can analyze to determine whether the commercial item initiatives have resulted in the intended outcomes.

At least nine DoD OIG reports over the past 22 years have identified instances where contractors did not provide cost or pricing data when requested by contracting officers, or contracting officers stated that they did not request the data because they knew the contractor would not provide it. In FY 2022, the DoD OIG is planning an audit on costs associated with commercial spare parts for DoD weapon systems.

[56] *Stars and Stripes Online*, "Lawmakers Fume Over Acting Navy Secretary's Call to Cancel Nuclear Sea-Launched Cruise Missile," June 10, 2021.

PRICING FOR ITEMS FROM LIMITED OR SOLE SOURCES

When goods or services are provided by limited or sole sources of supply, the lack of competition and lack of alternative sources could result in the DoD paying more than fair and reasonable prices. Between 2008 and 2018 the average cost of a DoD weapon system increased by 13 percent, and according to a 2019 GAO report, a lack of competition among contracts for major weapon systems was cited as a reason for this cost increase.[57]

In FY 2020, the DoD spent about $211 billion for contracts that were not competed among multiple vendors. In a fair and open market, competition drives down costs and increases innovation. Alternatively, a lack of competition increases prices and stalls innovation. Sole-source suppliers often charge the DoD inflated prices because there are no alternate vendors to encourage suppliers to price their goods or services competitively. In addition, the FAR enables sole-source providers and manufacturers to avoid providing cost data, even when requested, for contracts less than $2 million. The sole-source items are often commercial, which may further constrain contracting officers from obtaining cost data.

The DoD OIG has an ongoing audit to determine whether the Military Services and Defense agencies negotiated fair and reasonable prices for sole-source depot maintenance contracts, including seven commercial contracts, performed at contractor facilities. The intent of the audit is to evaluate whether sole-source depot maintenance contracts encounter the same enduring challenges as other sole-source contracts, which lead to cost escalation beyond industry inflation.

Lack of data from contractors to inform fair and reasonable pricing will endure because the DoD has been limited by law and regulation in its ability to obtain that data for commercial and sole-source items. Obtaining fair and reasonable prices is one way in which the DoD is a good steward of taxpayer money and builds trust with the public.

CONCLUSION

The DoD must continue to address the challenges with its acquisition and contracting practices. Using new and more agile acquisition pathways and OTs can help the DoD develop and field new capabilities faster with the help of nontraditional contractors. Quickly developing and fielding new capabilities and technologies is important for maintaining the U.S. advantage in strategic competition. The DoD must continue to improve its traditional acquisition process for cost, schedule, and performance while also supporting the warfighter with the right capability. Finally, the DoD must find alternative solutions to maximize competition and increase innovation while also obtaining fair and reasonable prices for commercial and sole-source items.

[57] Report No. GAO-19-336SP, "Weapon Systems Annual Assessment; Limited Use of Knowledge-Based Practices Continues to Undercut DoD's Investments," May 7, 2019.

U.S. and Thai personnel work to offload a Joint Light Tactical Vehicle from the MV Cape Henry in support of Exercise Cobra Gold 21, at Toong Pronge Port in Chon Buri Province, Thailand, July 31, 2021.

Source: The Marine Corps.

Soldiers with the Golden Eagles from the 230th Finance Management Support Unit, 4th Special Troops Battalion, conducted a field training exercise in August 2021. (U.S. Army photo)

Challenge 6. Improving DoD Financial Management and Budgeting

INTRODUCTION AND OVERVIEW

Longstanding financial management challenges continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information needed for accurate budget forecasting and decision making. With the DoD's budget making up about half of the U.S. Government's discretionary spending and the DoD owning approximately 78 percent ($3.1 trillion) of the U.S. Government's total assets, the DoD must demonstrate that it is a good steward of taxpayer money. One way the DoD can demonstrate its stewardship is through preparing reliable financial statements.

The DoD FY 2020 Annual Performance Report identified the strategic goal of improving the quality of budgetary and financial data. The annual financial statement audits help achieve this goal by determining the reliability of the DoD financial statements and providing transparency on where the DoD spends its resources. The Under Secretary of Defense (Comptroller)/Chief Financial Officer stated in the June 2021 DoD Financial Improvement and Audit Remediation report:

> The annual financial statement audits and the benefits derived from remediating findings are our best tool for fostering lasting cultural changes needed to achieve our business reform goals and modernize the Department. We are committed to integrating audit remediation and sustainment into our daily business operations, corporate culture, and policies in support of the warfighter.

The DoD will continue to face significant challenges related to financial management and budgeting due to the size and complexity of the DoD and shortcomings in its current business processes and systems. To improve its financial management and budgeting, the DoD must continue to implement corrective actions, including addressing notices of findings and recommendations (NFRs) from auditors, to improve financial and business processes across the DoD and its Components. Ultimately, these improvements will aid the DoD in producing more timely and reliable financial statements and result in an unmodified audit opinion (sometimes referred to as a clean opinion) on the DoD financial statements.

THE DOD SEES IMPROVEMENTS IN FINANCIAL STATEMENT AUDITS, BUT STILL LAGS BEHIND THE REST OF THE FEDERAL GOVERNMENT

The DoD's inability to produce reliable financial statements is a major factor in the Consolidated Financial Statements of the U.S. Government receiving a disclaimer of opinion each year. A disclaimer of opinion means that auditors are unable to obtain sufficient evidence on which to base an audit opinion. The DoD has made some progress, but many DoD Components continue to produce financial statements that auditors cannot conclude are reliable.

In FY 2020, the DoD OIG issued a disclaimer of opinion on the DoD Agency-Wide Basic Financial Statements. The DoD OIG contracted with five independent accounting firms and oversaw the completion of 24 DoD Component financial statement audits. Of these 24 audits, only 9 DoD Component financial statements received unmodified opinions, meaning that the auditors concluded that management presented the financial statements fairly and in accordance with Generally Accepted Accounting Principles. Of the remaining 15 DoD Component financial statements, 1 received a qualified opinion, meaning that the auditors concluded that there were misstatements in the financial statements that are material, but not significant to the overall presentation of the financial statements, and 14 received disclaimers of opinion.

Auditors identified 26 agency-wide material weaknesses, which are weaknesses in internal controls that result in a reasonable possibility that management will not prevent, or detect and correct, a material misstatement in the financial statements in a timely manner. The DoD's material weaknesses included findings related to the agency's inability to provide a complete universe of transactions that reconciled to its accounting records; ineffective processes and controls for reconciling the Fund Balance With Treasury; inability to accurately value its General Property, Plant, and Equipment assets; and the omission of the Joint Strike Fighter Program from the DoD financial statements. The Joint Strike Fighter Program is material to the audit because the value of the program exceeds $1 trillion, with each F-35 aircraft costing more than $70 million.

The results of the FY 2020 financial statement audits for the 24 DoD Components are a slight improvement over previous years, but the overall audit opinion for the DoD, and most of the 24 DoD Components, did not change from FY 2019 to FY 2020. The Defense Information Systems Agency did receive a clean audit opinion on its working capital fund financial statements, which was an improvement from the disclaimers of opinion it received in FYs 2018 and 2019. In addition, the DoD and Components implemented recommendations or took alternative actions that resulted in auditors closing 857 prior-year NFRs in FY 2020. The DoD must continue to focus on improving the accuracy and reliability of its financial statements to ensure the financial statements can pass audit scrutiny and to provide transparency to the public on how the DoD spends taxpayer money.

MAINTAINING THE PUBLIC TRUST THROUGH ACCOUNTABILITY

The Chief Financial Officers Act of 1990, as amended, requires that 24 Federal agencies, including the DoD, prepare financial statements and have those financial statements audited. More than 30 years later, the DoD remains the only agency that has never been able to accurately account for and report on its spending or physical assets during a financial statement audit. The DoD financial statement audit

An F-35A Lightning II of the 62nd Fighter Squadron prepares to takeoff from Luke Air Force Base, Arizona, on December 15, 2020.
Source: The Air Force, 56th Fighter Wing Public Affairs.

provides Congress and the public an assessment of where the DoD spends its resources and the reliability of the DoD's financial information. During an April 2021 House Armed Services Committee hearing on DoD financial improvement, the DoD's Deputy Chief Financial Officer stated, "The audit is giving taxpayers improved accountability for the assets entrusted to us, transparency in our use of those assets, and is pushing DoD and the U.S. Government closer to a clean opinion." He also acknowledged that the DoD's inability to obtain a clean audit opinion has led to the public not trusting what the DoD is financially reporting. For more information on preserving trust in the DoD and with the public, see Management Challenge 10, "Preserving Trust and Confidence in the DoD."

DoD and Component leadership at all levels must endorse the benefits of the audit and create a performance-based culture focused on continuous improvement. In a March 2021 memorandum, the Secretary of Defense communicated his expectation that personnel will ensure that the DoD's financial and operational processes, reporting, systems, and data are accurate, reliable, and secure.[58] The Under Secretary of Defense (Comptroller)/Chief Financial Officer echoed this theme during his May 2021 confirmation hearing by stating that he would ensure the DoD gives full effort and attention to the

[58] Secretary of Defense Memorandum, "Reaffirming Our Values and Ethical Conduct," March 1, 2021.

financial statement audit in order to build on and accelerate the progress toward the goal of a clean opinion. The statements from the Secretary of Defense and the Under Secretary of Defense (Comptroller)/Chief Financial Officer demonstrate a "tone at the top" that reflects the importance of strong financial processes and accurate financial statements.

The tone at the top is a fundamental component of an effective internal control environment and an important aspect of maintaining public trust. According to Federal Internal Control Standards, the tone at the top describes management's commitment to openness, honesty, integrity, and ethical behavior. Over the last few years, the Office of the Secretary has experienced senior civilian vacancies or turnover. For example, the Under Secretary of Defense (Comptroller)/ Chief Financial Officer position had a 2-year gap between Senate-confirmed officials. Additionally, the Director of Cost Assessment and Program Evaluation position was vacant for long periods of time between Senate-confirmed officials. Furthermore, the National Defense Authorization Act for FY 2021 eliminated the position of the Chief Management Officer of the DoD, effective on January 1, 2021. The DoD realigned the Chief Management Officer functions and responsibilities to other DoD officials on September 1, 2021. When there are gaps in leadership positions within the DoD, especially in positions that relate to financial management and budgeting or business process improvements, the tone at the top may be inconsistent or absent.

On June 21, 2021, a bipartisan group of senators wrote the Under Secretary of Defense (Comptroller)/Chief Financial Officer to express their concerns about the DoD's continued failure to obtain a clean financial statement audit opinion. The senators stated that, although the audits have led to some positive impacts, there has been little improvement to the crucial infrastructure of financial management systems and information technology. The senators further indicated that the DoD has spent billions of dollars over the last decade to implement modern enterprise resource planning systems, but remains reliant on more than 250 information systems that are incapable of producing trustworthy, reliable data. This shows the importance Congress is placing on the DoD's ability to obtain a clean financial statement opinion.

ACCURATE DATA AND SUSTAINABLE BUSINESS PRACTICES FOR TIMELY AND RELIABLE FINANCIAL STATEMENTS

To produce timely and reliable financial statements, the DoD must have accurate data and well-defined and sustainable business processes. The DoD stated that it uses over 250 information systems to support the financial statements. The DoD needs more accurate, complete, and real-time data from these systems and business processes over these systems that have appropriate internal controls and automated procedures rather than manual procedures. The DoD gains important information about needed improvements to the financial statements and the associated systems and processes by undergoing the audit. Throughout the process, auditors issue NFRs to communicate to management identified weaknesses and inefficiencies in financial processes.

To support the management of the NFRs from the financial statement audits and to start building a universe of transactions to support the financial statements, the Office of the Under Secretary of Defense (Comptroller)/ Chief Financial Officer developed the Advanced Analytics (Advana) platform. The DoD developed

Advana as the "single authoritative source for audit and business data analytics" and has expanded its use to provide easy and timely access to large volumes of data. As of June 2021, Advana had combined billions of transactions from across the DoD and was standardizing the data using a common data model. Advana captures data once and centrally manages the data so the DoD can analyze it and make well-informed decisions about processes and programs across the Department. The Under Secretary of Defense (Comptroller)/Chief Financial Officer stated in the June 2021 DoD Financial Improvement and Audit Remediation report, "One of the biggest DoD-wide benefits of audits is the improvement of our data, which collectively is one of our most valuable, strategic assets." While Advana is a promising step toward useful data for producing the DoD financial statements, it is only as good as the data in the systems feeding into it. In 2021, auditors found that the DoD had not yet fully implemented Advana, and as a result the DoD could not produce a complete or accurate universe of transactions.[59]

Although the DoD has made progress implementing auditor recommendations or taking alternative actions to address auditor findings, DoD senior leaders must sustain efforts to address longstanding information technology system deficiencies and implement consistent and sustainable enterprise business processes. During the FY 2020 audit, auditors reissued 2,641 prior-year NFRs and issued 918 new NFRs. These numbers include 1,093 reissued NFRs and 393 newly issued NFRs related to information technology systems. With over 250 information systems used to support the financial statements, unique, manual, and poorly integrated processes hinder the DoD's ability to produce timely and reliable financial statements.

As a result of the DoD and its Components addressing the deficiencies identified in the NFRs and improving business processes through initiatives such as the Business Enterprise Architecture, auditors have reduced or downgraded material weaknesses, seen enhanced business processes, and had access to improved supporting documentation for transactions selected for testing. For example, in FY 2019 auditors identified a material weakness because the Navy's Contract Authority processes, policies, procedures, internal controls, and supporting documentation were not effective to identify, detect, and correct inaccurate balances recorded in the general ledger. During FY 2020, the Navy developed new controls that the auditors tested. The auditors were able to downgrade that material weakness to a significant deficiency.

The DoD has also focused on improving the efficiency of business processes by implementing interoperable defense business solutions that align to a robust Business Enterprise Architecture. The Architecture defines the DoD business transformation priorities, the business capabilities required to support those priorities, and the combinations of enterprise systems and initiatives that enable those capabilities. This Architecture assists system owners and program managers by identifying potential solutions for their requirements in other areas of the DoD, standardizing the investment review process, and capitalizing on enterprise best practices.

Although there have been improvements to its financial statements, the DoD struggles to meet the November 15 deadline established by the Office of Management and Budget for

[59] Report No. DODIG-2021-095, "Audit of Accounting Corrections on the SF 1081," June 25, 2021.

issuing the agency-wide financial statements. To enable the DoD to meet this deadline, each Component must provide audited financial statements to the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer by November 8, for compilation. However, many Components continue to struggle to meet the November 8 deadline and some do not meet the deadline. For example, while the Defense Information Systems Agency's working capital fund was able to obtain a clean opinion in FY 2020, the effort required an extension to the mandatory reporting deadline and extensive additional work from the Defense Finance and Accounting Service. This opinion was issued on December 17, 2020, after the DoD issued its agency-wide financial statements.

Until all Components can produce audited financial statements by November 8 for compilation, the DoD will continue to face challenges in producing timely DoD agency-wide financial statements. As the DoD continues to implement recommendations from NFRs, improve the interoperability and accuracy of the data in its information systems, and develop and implement sustainable business processes, the DoD will likely be able to produce a more timely and reliable financial statement.

CONCLUSION

During the Secretary of Defense's confirmation hearing, his written statement asserted, "The value of audit is in the audit recommendations that bring insight into how the Department can improve its operations, and should lead to strengthened internal controls, streamlined business processes, improved visibility of assets and financial resources, and increased transparency and accountability. All of this makes the Department more effective." While the road to a clean financial statement audit opinion is a long-term effort, the DoD could realize more immediate improvements by implementing the recommendations contained in the auditor-issued NFRs, prioritized by the seriousness of the deficiency. Ineffective information technology system controls and business practices, identified in the NFRs, leave the DoD at risk of continuing to produce financial statements that are unreliable. The tone at the top must reflect the seriousness and importance of continued focus on producing reliable financial statements that help ensure the public's trust in the DoD's stewardship of taxpayer funds.

A Soldier tests the Squad Area Network capability during a network modernization experiment taking place at Joint Base McGuire-Dix-Lakehurst, New Jersey, on September 10, 2020.

Source: The Army.

An Air Force Staff Sergeant, with the 821st Contingency Response Squadron at Travis Air Force Base, California, prepares to unload over 57,000 bottles of water, at Joint Base San Antonio-Kelly Field, Texas, to support the emergency response to Winter Storm Uri on February 21, 2021. (U.S. Air Force photo)

Challenge 7. Building Resiliency to Environmental Stresses

INTRODUCTION AND OVERVIEW

Environmental stresses, such as climate change, extreme weather events, and other environmental hazards, have a direct impact on the DoD's operational plans, readiness, infrastructure, and budget. In January 2021, the Secretary of Defense concluded, "There is little about what the Department does to defend the American people that is not affected by climate change. It is a national security issue, and we must treat it as such."[60] Specifically, in the last 4 years, climate change and extreme weather events have caused billions of dollars in damage to DoD infrastructure, including the loss of critical energy supplies needed to sustain essential missions at DoD installations.

The DoD must incorporate climate hazards, environmental stresses, and energy considerations into its infrastructure and operational planning to reduce the risk to DoD installations, missions, and operations worldwide. Furthermore, the DoD has a responsibility to protect the land, air, and water resources that it owns and in which it operates. While environmental hazards, contaminants, and pollutants may not pose an immediate threat, the DoD must balance the challenge of identifying, evaluating, and, where appropriate, mitigating these hazards, while conducting operations and maintaining readiness.

IMPACT OF CLIMATE CHANGE AND EXTREME WEATHER ON THE DOD

Environmental stresses, such as climate change and extreme weather events, are increasing in frequency and strength, causing adverse effects to the DoD's operations and resources. Environmental stresses include heat, drought, coastal flooding, inland flooding, energy demand, land degradation, wildfires, and extreme weather events. Many of these stresses are difficult to forecast, which presents unique risks and challenges to the DoD. Climate change has, and will continue to impact infrastructure, military readiness, and resources, which is why the DoD has identified climate change as a critical national security threat and a threat multiplier.

[60] DoD, "Secretary of Defense Statement on Tackling the Climate Crisis at Home and Abroad," January 27, 2021.

IMPACT ON INFRASTRUCTURE

In recent years, the effects of climate change, such as extreme weather events, have devastated DoD installations, resulting in billions of dollars in damages, repairs, and new construction projects. For example, 484 facilities at Tyndall Air Force Base (AFB), Florida, were destroyed or damaged beyond repair after Hurricane Michael made landfall in October 2018. As a result, the DoD invested $5 billion to fund more than 300 projects to demolish, renovate, or rebuild new facilities that are more resilient against future extreme weather events.[61] Tyndall AFB is only 1 of 10 DoD installations that were negatively affected by extreme weather events from 2017 through 2021. In total, the damages at those 10 DoD installations is costing taxpayers $13 billion to correct.[62] Protecting DoD infrastructure from future extreme weather events requires strategic plans, risk assessments, and continual investments to adapt existing infrastructure, relocate installations, or build resilient infrastructure.

The DoD began several enterprise-level initiatives to prioritize and incorporate climate change considerations into DoD infrastructure planning and risk analyses. Specifically, in March 2021, the Secretary of Defense established the DoD Climate Working Group to track the implementation of DoD actions to address climate change, including efforts to increase the resilience of DoD installations to extreme weather events. In April 2021, the DoD also announced a plan to complete climate exposure assessments on all major U.S. installations by April 2022 and all major overseas installations by April 2023 using the DoD Climate Assessment Tool.[63] The DoD Climate Assessment Tool is designed to identify an installation's vulnerabilities to climate-related hazards and enable DoD senior officials to make informed policy and investment decisions for the adaptation and resiliency of DoD infrastructure.[64]

However, climate-related policy and investment decisions for DoD infrastructure rely on the sustained support of DoD leadership and congressional funding. According to a June 2019 Government Accountability Office (GAO) report on climate resilience, the absence or insufficiency of DoD leadership support and funding may result in greater future financial burdens to repair or rebuild infrastructure that was unprepared to withstand extreme weather events and climate changes.[65] In FY 2022, the DoD OIG plans to conduct an audit to determine whether Navy officials planned for current and future environmental threats to naval shipyards in accordance with Federal and DoD policies.

In addition to damages to the physical plant, extreme weather events have the potential to significantly hamper access to services, such as electricity and water, on DoD installations. For example, in February 2021, Winter Storm Uri highlighted risks related to the DoD's infrastructure. The storm damaged 694 facilities and 1,366 privatized homes across four Army installations stretched throughout the Midwest and South. DoD personnel assigned to Fort Riley, Kansas; Fort Sill, Oklahoma; Fort Hood, Texas; and Fort Polk, Louisiana, experienced prolonged power outages and compromised supplies of potable water.

---

61 325th Fighter Wing Public Affairs, "Tyndall Updates Community on State of Base Rebuild," April 26, 2021. Air Force Installation and Mission Support Center, "Tyndall Program Management Office," updated 2021.

62 DoD, "Tackling the Climate Crisis," updated September 2021.

63 DoD, "DoD Announces Installation Climate Exposure Assessments Plan Through the Defense Climate Assessment Tool," April 22, 2021.

64 DoD, "DoD Climate Assessment Tool," April 5, 2021.

65 Report No. GAO-19-453, "Climate Resilience: DoD Needs to Assess Risk and Provide Guidance on Use of Climate Projections in Installation Master Plans and Facilities Designs," June 12, 2019.

In 2018, Hurricane Michael caused significant structural damage to the majority of Tyndall Air Force Base, Florida, and surrounding areas after going ashore as a Category 4 storm.

Source: The Air Force.

Compromised electrical and water systems negatively affect the health and safety of DoD Service members and their families, and make it difficult for DoD installations to execute their critical missions and sustain readiness. Enhanced resiliency measures are necessary to address the effects of climate change and extreme weather events on DoD electrical and water system operations.

The DoD first identified energy resiliency as a problem in 2012 when it established the Electric Power Resilience Working Group.[66] Despite the attention, the DoD continues to struggle to integrate energy resiliency into its policies, plans, and actions for electrical and water systems at DoD installations. During a March 2021 hearing before the House Armed Services Subcommittee on Readiness, senior leaders at each of the Military Service installation commands described their Military Service-specific plans for energy resiliency. For example, the Commander of the Air Force Materiel Command stated that as of March 2021, the Air Force completed energy plans for 24 installations and planned to complete energy plans for 20 other installations by the end of FY 2021.[67] The Commander of the Marine Corps Installations Command also discussed investments in smart grids and micro-grid technologies and the integration of climate considerations into all installation master plans. Even with the development of plans to integrate energy resiliency at DoD installations and infrastructure, the

[66] Office of the Assistant Secretary of Defense for Sustainment, "Energy Resilience Timeline."

[67] DoD, "Leaders Testify About DoD Installation Resiliency Efforts," March 29, 2021.

implementation of the plans will require time, funds, expertise, training, and advanced technology.

One example of successful planning for energy resiliency is at Barksdale AFB, Louisiana. Prior to Winter Storm Uri in 2021, Barksdale AFB officials installed redundant connections to a neighboring city's water supply as a secondary water source in case the installation's primary water source was compromised. This contingency planning enabled Barksdale AFB to quickly recover from the disruption to the installation's potable water supply caused by the storm. As shown in the example of Barksdale AFB, building resilient energy systems through alternative and redundant energy supplies can enable DoD installations to continually execute critical missions while protecting the health and safety of DoD Service members and surrounding communities. However, building resilient electrical and water systems requires comprehensive plans that take time to develop, key investments in adaptable power systems, and partnerships with local communities through long-term agreements.

IMPACT ON READINESS

In January 2021, the Administration issued an Executive Order directing the Secretary of Defense to evaluate the vulnerabilities of DoD facilities and operations to climate change. The Order also required the DoD to consider climate change when planning war games and to incorporate climate change into the future National Defense Strategy, risk analyses, strategy development, and planning.[68] The April 2021 "DoD Installation Exposure to Climate Change at Home and Abroad" report, issued in response to this Executive Order, identified the climate hazards to which DoD installations are most exposed.[69]

For all DoD installations, rising temperatures will increase exposure to a wide range of hazards that can directly impact military readiness, including heat-related health problems and adverse effects on military training and testing. For example, increases in temperature are anticipated to have significant effects on military training and testing, including increases in the number of "black flag" (suspended outdoor activities) or fire hazard days (limited live-fire activities). Higher temperatures may also reduce pilot readiness by limiting cockpit time both on the ground and during takeoff and landing. In addition, climate change has resulted in fire seasons lasting longer and burning twice as many acres annually, especially in areas not historically affected by wildfire. Installations with dry conditions and range activities in areas with dense wildland vegetation will have increased potential to initiate a wildfire. Wildfires pose a significant risk to operations, decreasing the type and potential timing of training activities at a given location. Infrastructure may also be vulnerable to damage from wildfires that originate off an installation.

Finally, climate change has and will continue to impact local and regional energy supplies by altering peak and cumulative energy demand, and by disrupting power generation and transmission. Climate change can also affect water availability for power generation, such as hydropower and thermoelectric cooling. According to the 2021 DoD Installation Climate Exposure at Home and Abroad report, climate hazards that affect energy demand at military installations will be greatest in Alaska and

[68] Executive Order 14008, "Tackling the Climate Crisis at Home and Abroad," January 27, 2021.

[69] DoD, "DoD Installation Exposure to Climate Change at Home and Abroad, April 2021.

the Northern Plains because of the rapidly warming temperatures in all seasons. To assess the DoD's progress in building the resilience of DoD infrastructure against the effects of climate change, the DoD OIG has an ongoing evaluation to determine the extent to which the DoD addressed climate resilience of U.S. military installations in the Arctic and sub-Arctic.

Climate change exposure and impacts do not stop at the installation boundary. The surrounding communities may provide essential energy, water, transportation, communication, emergency, and other services to the installation. Military and civilian personnel may live in the surrounding communities; therefore, the energy resilience of the surrounding communities is an essential component of military installation resilience. To help improve this resilience, the DoD provides grants to local communities to undertake investments in public services and infrastructure to support the readiness and resilience of the military installation.

Identifying the climate hazards to which DoD installations are most exposed is the first step in addressing the potential physical harm, security impacts, degradation in readiness, and increased humanitarian deployment needs resulting from global climate change. Fortunately, the DoD has undertaken several site-specific climate-related studies through its Strategic Environmental Research and Development Program and the Environmental Security Technology Certification Program.[70] The 2021 DoD Installation Climate Exposure at Home and Abroad report states, "Exposure to climate change hazards is not a new problem for DoD installations, but the nature and severity of this problem is changing. The costs and consequences for failing to adapt are increasing, as are the benefits of improved resilience."

THE DOD'S RESPONSIBILITY TO PRESERVE AND RESTORE THE ENVIRONMENT

The DoD is responsible for more than 26.9 million acres of land, air, and water resources that it uses for training, testing, and operations. The challenge for the DoD is ensuring that Service members can perform needed training and operations while still being good stewards of environmental resources and native plant and animal species. In some cases, the protection of the environment can result in the Military Services developing workarounds, such as altering operations, performing training in a simulated environment, or relocating training to other installations. The potential problem with such workarounds is that they may lack realism and can lead to the practice of tactics, techniques, and procedures that are contrary to those used in combat.

Additionally, restricted or inadequate training may lead to insufficient skills or unnecessarily risky practices on the battlefield. For example, at Camp Pendleton, California, the U.S. Fish and Wildlife Service designated 10 percent of the installation as critical habitat for endangered species, which limits the use of off-road vehicles and the digging of defensive positions. A Marine Corps commander commented that the restrictions at Camp Pendleton affected his Marines. According to the commander, the Marines were not fully ready for conditions in Afghanistan because they "rarely practiced digging in … due to environmental restrictions

[70] DoD, "DoD Installation Exposure to Climate Change at Home and Abroad, April 2021.

and the base's limits on off-road maneuvering left Marine drivers unprepared for Afghanistan's rugged terrain."[71]

The presence of threatened and endangered species and critical habitats can result in training, testing, and operating activity restrictions. For example, the Pōhakuloa Training Area in Hawaii is home to 26 threatened and endangered species and 1,200 archeological sites. The protection of these species and sites has resulted in the DoD being able to use just one third (70 square miles) of the 210 square miles of range land.[72] Similarly, the U.S. Fish and Wildlife Service designated part of Camp Pendleton as a critical habitat, which reduced the amount of beach available for amphibious assault, preventing training to doctrinal standards.[73] Certain maritime testing and training operations at Camp Pendleton must stop when rare marine mammals, such as the endangered right whale, are present in the training area.

The DoD has had some success in striking a balance to protect the environment and conduct training. For example, at Camp Lejeune, North Carolina, the Marine Corps collaborated with environmentalists to restore the longleaf pine habitat on 521 acres, enhancing and expanding the endangered red-cockaded woodpecker's natural habitat, resulting in fewer restrictions on military training in those areas.[74] The Marines were able to expand into the woodpecker's territory to enlarge training areas and continue simulated battles without greatly disturbing the birds, as well as allow artillery, small-arms, and armored vehicle training.[75]

IMPACT OF DOD ACTIVITIES ON THE ENVIRONMENT

While environmental hazards, contaminants, and pollutants may not pose an immediate threat to DoD operations, they become important drivers for DoD missions, programs, resources, and liability in the future. The DoD must respond to known environmental hazards, but also be forward thinking when considering and using new substances or chemicals that may prove harmful in the future. The health and safety of DoD personnel and the public, along with the financial and reputation cost of identifying, mitigating, and responding to environmental hazards, will continue to challenge the DoD and can have long-lasting impacts.

Under the Defense Environmental Restoration Program, DoD officials are required to respond to and remediate DoD releases of hazardous substances or contaminants at active and closed DoD properties. According to a January 2018 DoD report, as of the end of FY 2016, the DoD had a total of 34,065 sites to restore and had completed restoration at 29,409 (86 percent) of the sites.[76] The January 2018 report estimated that the DoD would complete restoration at 95 percent of the sites by the end of FY 2021, leaving more than 1,850 sites for restoration into FY 2022 and beyond. The DoD does not anticipate completing restoration at all of the remaining sites until FY 2046 and at

[71] RAND Corporation, "The Thin Green Line: An Assessment of DoD's Readiness and Environmental Protection Initiative to Buffer Installation Encroachment," 2007.

[72] Report No. DODIG-2019-081, "Audit of Training Ranges Supporting Aviation Units in the U.S. Indo–Pacific Command," April 17, 2019.

[73] RAND Corporation, "The Thin Green Line: An Assessment of DoD's Readiness and Environmental Protection Initiative to Buffer Installation Encroachment," 2007.

[74] RAND Corporation, "Building Resilience Together: Military and Local Government Collaboration for Climate Adaptation," 2020.

[75] U.S. Fish and Wildlife Services, "Marines and woodpeckers share the high ground," March 22, 2018.

[76] Under Secretary of Defense for Acquisition and Sustainment, "Department of Defense Achieving Response Complete at Installation Restoration Program Sites," January 2018.

The Threatened and Endangered Species Program team at Camp Lejeune, North Carolina, actively manages and protects the red-cockaded woodpecker population and on-base habitat. On June 7, 2021, the team added tags to the chicks to track their movements and nest activity.

Source: The Air Force, 56th Fighter Wing Public Affairs.

an estimated cost of $11.8 billion because of the complexity and difficulty of the required clean up.

The DoD is not always aware when contamination or pollution occurs. For example, in the 1980s, contaminants were found in several wells that provided drinking water at Camp Lejeune. According to the Department of Veterans Affairs, the contaminants were in the water supply from the mid-1950s until February 1985, when the Marine Corps shut down the wells and provided an alternative water source. It took more than 30 years for the Marine Corps to learn of the contamination and shut down the wells. There are also emerging hazards, contaminants, and pollutants that the Environmental Protection Agency either does not regulate or only loosely regulates, which makes elimination and cleanup more complicated for the DoD. In 2006, to help evaluate and manage risks from the chemicals and materials the DoD uses, DoD officials established the Chemical and Material Risk Management Program. Since the beginning of the Program, the DoD has evaluated how to protect its readiness, its personnel, and the environment from emerging chemicals such as lead, and most recently, perfluoroalkyl and polyfluoroalkyl substances (PFAS).

PFAS are fire-resistant, synthetic chemicals that repel oil, grease, and water and can be found in almost every U.S. home and business. However, some products containing PFAS are

largely limited to the DoD. For example, in the 1970s, the DoD began using a foam that contains PFAS to extinguish dangerous petroleum-based fires. When the DoD uses the foam, PFAS can make its way into the ground and groundwater, and may eventually reach sources of drinking water. As of September 30, 2020, DoD officials identified 687 sites, including active and National Guard installations, former military installations, and Defense Logistics Agency sites, where the DoD used or released the foam. The DoD has a responsibility to protect human health and the environment and must identify, plan, program, and budget for any actions to mitigate contamination from the chemicals that it uses.

Although there are times when the environmental hazards, contaminants, and pollutants are known, the actions taken by the DoD are not sufficient to avoid future liability and ensure safe operations. In July 2021, the DoD OIG found that DoD officials had taken steps to identify, mitigate, and remediate contaminant effects from PFAS-containing fire-fighting foam at DoD installations, including restricting nonessential use of the foam and initiating cleanup response actions.[77] However, DoD officials had not proactively identified, mitigated, and remediated contaminant effects from PFAS-containing materials other than fire-fighting foam at DoD installations. Furthermore, in a June 2021 report, the GAO recommended that the DoD include cost estimates for future PFAS investigation and cleanup in the DoD's annual environmental report to Congress.[78]

The DoD has been working for decades to identify, evaluate, and, where appropriate, respond to the effects of environmental hazards, contaminants, and pollutants, but the changing nature of science and regulation surrounding emerging substances and chemicals creates challenges for the DoD as officials work to mitigate potential risks. Failure to identify and mitigate the effects of hazardous substances, contaminants, or pollutants not only costs the DoD billions in remediation and cleanup, but also affects the reputation of the DoD and most importantly the health and well-being of DoD personnel and their families, surrounding communities, and foreign partners.

CONCLUSION

From hurricanes and extreme heat waves to contaminants and pollutants, environmental stresses continue to challenge the DoD at its sites across the world. As the Secretary of Defense wrote in the Message to the Force in March 2021, the "growing climate crisis ... must be met by ambitious immediate action." Although the DoD has long recognized the need to protect the environment and the potential impacts of climate change on its operations and installations, specific actions to fortify DoD structures and improve energy resiliency remain unaccomplished. The DoD must effectively integrate climate considerations into its operational plans, programs, policies, and tools to build resilience against the effects of the climate crisis.

---

[77] Report No. DODIG-2021-105, "Evaluation of the Department of Defense's Actions to Control Contamination from Perflouroalkyl and Polyflouroalkyl Substances (PFAS) at DoD Installations," July 22, 2021.

[78] Report No. GAO-21-421, "Firefighting Foam Chemicals: DOD Is Investigating PFAS and Responding to Contamination, but Should Report More Cost Information," June 22, 2021.

Soldiers from the 10th Special Forces Group look out over the National Training Center at Fort Irwin, California, on August 17, 2021. The terrain and environment at the National Training Center closely matches the hot, dry conditions Soldiers experience while on some deployments.

Source: The Army.

A member of team Homestead receives the COVID-19 vaccine at a vaccination event during the August Unit Training Assembly at Homestead Air Reserve Base, Florida, on August 7, 2021. (U.S. Air Force photo)

Challenge 8. Protecting the Health and Wellness of Service Members and Their Families

INTRODUCTION AND OVERVIEW

Protecting the health and wellness of Service members and their families is critical for the DoD to maintain a ready force that can meet the demands of its assigned missions. In the Secretary of Defense's written statement ahead of his January 2021 confirmation hearing, he stated, "Nothing is more important than the health and well-being of our people and their families." Despite recognizing the importance of the health and wellness of Service members and their families, the DoD faces key challenges in this area.

The Military Health System (MHS) is entering its sixth year of transitioning the responsibility for operating DoD medical treatment facilities (MTFs) from the Military Departments to the Defense Health Agency (DHA). The military medical departments continue to face challenges maintaining a medically ready operational force. Additionally, the medical force faces unique challenges related to maintaining sufficient manning levels and ensuring medical personnel receive sufficient training and experience to meet DoD requirements. The DoD continues to experience higher rates of suicide, substance use disorders, and sexual assaults despite intense focus on awareness and prevention. With the coronavirus disease–2019 (COVID-19) pandemic in its second year, a resurgence in cases could strain the ability of the MHS to provide medical services. Finally, military housing conditions continue to present serious concerns for the health and safety of DoD personnel and their families.

Although this year's challenge focuses on the areas previously described, some management challenges identified in prior years persist, such as the DoD's deployment of an interoperable electronic health record system with the Department of Veterans Affairs and increasing health care costs.

MEDICAL READINESS OF THE FORCE

Both the Active and Reserve Components have reported an increase in deployment-limiting medical conditions. The Military Departments are required to assess the medical readiness of Service members during each clinical encounter and determine whether the individual is able to deploy. Each Service member's assessment affects the unit's readiness and, depending on how many personnel are non-deployable, could compromise the unit's operational capabilities.

As of March 2021, 6 percent of Active Component and 8 percent of Reserve Component Service members had a deployment-limiting medical condition, up from 5 percent and 7 percent, respectively, in March 2020. Musculoskeletal conditions are the most common type of deployment-limiting condition. To maintain the physical readiness of uninjured Service members, reduce vulnerability to injury, and aggressively treat injured Service members and return them to duty, the Military Departments have embedded physical therapists within operational units. In a similar effort, the Military Departments have embedded mental health providers within operational units to raise awareness of mental health conditions, increase access to care, and reduce the stigma of seeking mental health care.

However, the Military Departments have implemented these programs differently and lack key performance indicators to help measure the programs' impact. Without knowing whether programs are effective, the Military Departments cannot make well-informed decisions on program changes or develop alternative solutions related to medical readiness. In FY 2022, the DoD OIG plans to audit the accuracy of individual medical readiness reporting.

READINESS OF THE SERVICE MEMBERS IN THE MEDICAL FIELD

The DoD also faces challenges maintaining the readiness of its medical force. The military medical departments are required to staff, train, and equip a medical force capable of providing medical services in an operational setting. As a combat support agency, the DHA enables and sustains medical force readiness. The Military Services rely on the DHA-managed MTFs to maintain the knowledge, skills, and abilities of MTF medical providers, including preparing the military providers for deployment. However, MTF medical providers are not maintaining these required skills.

Reforms contained in the National Defense Authorization Act (NDAA) for FY 2017 and DoD Instruction 6000.19, issued in February 2020, were designed to address this challenge by ensuring that medical providers have the opportunities and the ability to meet critical wartime medical readiness skills and core competencies for health care providers. In 2016, the DoD began identifying the knowledge, skills, and abilities (KSAs) required for providers in combat-related medical specialties while in a deployed setting. DoD Instruction 6000.19 requires the DHA to coordinate with the Military Departments to meet medical force readiness requirements, through placement of personnel at DHA-administered MTFs or at the facilities of civilian partners during peacetime.[79] The DoD has begun to define KSA targets for Active Duty providers, based on the volume and complexity of medical procedures performed during peacetime. However, for some medical specialties, only a small percentage of military providers meet the KSA target. For example,

[79] DoD Instruction 6000.19, "Military Medical Treatment Facility Support of Medical Readiness Skills of Health Care Providers," February 7, 2020.

Alaska Army National Guard flight medics from the 2nd Battalion, 211th General Support Aviation Battalion and Air Force C-130J Super Hercules crew chiefs secure a simulated patient during casualty evacuation training at Joint Base Elmendorf-Richardson, Alaska, on August 23, 2021.

Source: The Air Force, Joint Base Elmendorf-Richardson Public Affairs.

only 22 of 355 (6.2 percent) General Surgeons, a key component of a combat casualty team, met the General Surgery KSA threshold, as of April 2021.

The Navy and Air Force Surgeons General testified before the Senate Committee on Appropriations in April 2021 that their Services continue to face challenges maintaining the readiness of medical personnel. Specifically, the Air Force Surgeon General stated that the MTFs do not have the patient volume that medical personnel require to maintain the skills required during combat deployments. A 2020 DoD OIG audit of the training of mobile medical teams in the U.S. Indo–Pacific Command and U.S. Africa Command areas of responsibility found that surgical and tactical training were not always provided to mobile medical team members before deployment, and when provided, were often reported as ineffective.[80]

The FY 2021 NDAA requires the DoD to assess the ability of its existing methods for maintaining skills required during deployment, such as allowing providers to work in civilian trauma centers to address readiness shortfalls. It further requires the DoD to evaluate the cost and effectiveness of alternative models to improve the medical readiness of the Armed Forces to provide combat care. A medical force capable of performing emergency and lifesaving skills required during combat and

[80] Report No. DODIG-2020-087, "Audit of Training of Mobile Medical Teams in the U.S. Indo–Pacific Command and U.S. Africa Command Areas of Responsibility," June 8, 2020.

training deployments is imperative for the health and safety of the total force. In FY 2022, the DoD OIG plans to evaluate the DoD's efforts to maintain the readiness of the medical force through the use of civilian and Department of Veterans Affairs partnerships.

PROVIDING CARE TO VICTIMS OF SEXUAL ASSAULT

Treating victims of sexual assault remains a persistent and serious challenge as the DoD continues to combat the rise in sexual assaults. From 2004 to 2019, Congress passed 249 statutory requirements to address sexual assault in the military, with more than a third of the requirements relating to victim advocacy and assistance, including medical care.[81] The DoD still faces challenges in providing appropriate care and support to victims of sexual assault while maintaining the patients' privacy. Continued focus on preventing sexual assault is paramount, and when victims come forward, they must receive the best physical and mental health care that the DoD can provide.

On February 26, 2021, the Secretary of Defense established an Independent Review Commission (IRC) to assess the military's treatment of sexual assault, which included a review of the clinical and non-clinical services provided to victims. On July 2, 2021, the IRC released its report, finding that installation programs designed to coordinate the response and care for sexual assault victims are often staffed by personnel without proper training, experience, or sufficient time to devote to the victim.[82] Specifically, most victim advocacy is conducted by Service members as a collateral duty to their primary job, such as aircraft maintenance or logistics, rather than by experienced, full-time professional advocates. The report's findings also noted that victim advocate programs are often not co-located with the medical facilities, reducing the continuity of care and leaving the victim unsure of where to go for help. The IRC strongly recommended that the DoD establish a solution that ensures adequate resources for full time and professional victim care personnel.

The IRC also found that sexual assault victims suffer stigmatization and a loss of privacy when seeking care and support services on the installation where they are assigned, leading victims to forgo seeking care after an assault. The IRC recommended that the DoD expand access to sexual assault services provided by civilian programs and allow Service members to confidentially access Department of Veterans Affairs services for sexual assault without a referral. The IRC's report also noted that the lack of access to immediate medical forensic health care on some Navy ships and isolated installations resulted in additional trauma for the victim and increased risk of loss or damage of critical evidence. The IRC recommended that the Navy remedy this by assigning a trained Sexual Assault Medical Forensic Examiner to vessels and at isolated installations.

The Acting Assistant Secretary of Defense for Health Affairs requested that the DoD OIG review MTFs to ensure they are adequately prepared to treat sexual assault victims. The Acting Assistant Secretary said that from a medical standpoint, it is important that all military hospitals have the resources they need to help people who have been victims of sexual assault. In FY 2022, the DoD OIG plans to perform an audit to determine whether

[81] Report No. GAO-21-463T, "Sexual Assault in the Military: Continued Congressional Oversight and Additional DoD Focus on Prevention Could Aid DoD's Efforts," March 24, 2021.

[82] Independent Review Commission on Sexual Assault in the Military, "Hard Truths and the Duty to Change: Recommendations from the Independent Review Commission on Sexual Assault," July 2, 2021.

An Airman with the 138th Security Forces Squadron places teal-colored ribbons near high-traffic areas to bring awareness of the campaign to eliminate sexual assault within the military.

Source: The Air Force.

the DoD MTFs have the required personnel, resources, and training needed to treat victims of sexual assault.

The DoD must continue to combat sexual assault through training and holding personnel accountable for their actions, while also continually improving the care and support it provides to victims of sexual assault. For more information on sexual assault and sexual harassment in the DoD, see Management Challenge 10, "Preserving Trust and Confidence in the DoD."

BEHAVIORAL HEALTH

Behavioral health conditions, such as substance use disorders and suicide-related behaviors, and access to inpatient and outpatient health care to treat those conditions, remain key health and safety issues for Service members and their families. Unaddressed behavioral health conditions can limit the ability of a Service member to meet the demands of military life and reduce Total Force readiness.

According to the 2019 DoD Health of the Force Report, 8.4 percent of active duty Service members were diagnosed with a behavioral health disorder and accounted for 1.9 million (16.2 percent) outpatient encounters in 2019.[83] When left undiagnosed and untreated, behavioral health conditions can lead to medical readiness concerns, alcohol and opioid abuse, suicidal behavior, and early discharge.

Substance use disorders can develop in individuals who use alcohol or other addicting drugs in harmful quantities, and substance use is linked to suicides and suicide attempts. In the October 2017 DoD Report to Congress on "Prescription Opioid Abuse and Effects on Readiness," the Office of the Under Secretary of Defense for Personnel and Readiness reported

[83] DoD, "2019 Health of the DoD Force," 2020.

that prescription opioid misuse in Service members remained an issue of concern for the DoD. Previous DoD OIG reports have found that MTFs potentially overprescribed opioids from 2015 through 2017 because of a lack of policies and processes in place to identify and monitor daily prescribed amounts. The reports also found that the DoD did not implement standard outcome and process measures specific to opioid use disorder beneficiaries who were prescribed over the recommended opioid amount per day.[84]

In addition, the 2019 DoD Health of the Force Report found that 13.3 percent of active duty Service members screened positive for hazardous drinking, based on the Service member's responses to questions on the frequency and quantity of their alcohol consumption. According to the Uniformed Services University and the Center for the Study of Traumatic Stress, the DoD spends more than $600 million annually in medical care and lost work time for alcohol abuse alone. The Army's 2020 Health of the Force Report found that drug and alcohol overdose was the leading method of suicide attempt for Soldiers in 2020.[85]

The DoD has increased efforts to recognize and treat behavioral health problems and prevent suicides. The DoD and the Military Services continue to identify high-risk populations, such as Service members transitioning out of the military, and provide them with access to suicide prevention resources, such as suicide awareness campaigns, suicide intervention training, and suicide crisis hotline marketing. The DoD also offered training to military chaplains and family members on suicide prevention and identifying suicide risk factors. Furthermore, the Defense Suicide Prevention Office continues to promote training initiatives to reduce stigma and promote the use of available support services. In response to an Executive Order, in March 2018, the Secretaries of Defense, Veterans Affairs, and Homeland Security issued a Joint Action Plan, which described actions to provide seamless access to mental health care and suicide prevention resources for transitioning Service members.[86] The Joint Action Plan sought to eliminate barriers to care and gaps in access to mental health care and suicide prevention services.

Despite these efforts, the DoD continues to face significant challenges related to identifying, diagnosing, and treating behavioral health issues and risk factors for military personnel and other health care beneficiaries.

IMPACT OF COVID-19 AND PREPAREDNESS FOR FUTURE PANDEMICS

The DoD continues to face challenges protecting its personnel and beneficiaries from the COVID-19 virus, providing health care during the COVID-19 pandemic, and incorporating lessons learned into preparing for future pandemics. In 2021, the COVID-19 virus evolved and continued to threaten DoD personnel and their families, and adversely impact medical readiness. As of September 29, 2021, the DoD reported 372,146 COVID-19 cases, 5,274 hospitalizations, and 515 deaths among its Service members, civilians, dependents, and contractors. As COVID-19 variants continue to spread, a resurgence in cases could strain the ability

[84] Report No. DODIG-2020-048, "Audit of Controls Over Opioid Prescriptions at Selected DoD Military Treatment Facilities," January 10, 2020. Report No. DODIG-2019-091, "Evaluation of the DoD's Management of Opioid Use Disorder for Military Health System Beneficiaries," June 10, 2019.

[85] Army, "2020 Health of the Force Report," 2021.

[86] Secretaries of Defense, Veterans Affairs, and Homeland Security, "Joint Action Plan for Supporting Veterans During Their Transition From Uniformed Service to Civilian Life," March 9, 2018 (revised April 2018).

of the MHS to deliver mission-essential health care services, including providing COVID-19 services to Service members and beneficiaries.

Although vaccine mandates for Service members and DoD personnel are ongoing and the DoD has taken actions to mitigate the virus's effects on patients and providers, the DoD must continue to mitigate the risk of exposure to COVID-19 variants, monitor breakthrough cases of COVID-19, and ensure it plans for future infectious disease pandemics. In FY 2021, the DoD OIG reported that controls and measures designed to mitigate the spread and reduce the risk of infectious diseases, such as COVID-19, at the DoD's basic training centers, onboard Navy ships, and at the Armed Forces Retirement Homes were not adequately implemented. Poor implementation of these controls and measures increased the risk to the health of Service members, health care professionals, and retired Service members.[87]

To sustain access to health care throughout the pandemic, the DoD has prioritized the allocation of personal protective equipment and encouraged the use of telemedicine, particularly for follow-up appointments and ongoing care of isolated patients with COVID-19. Medical and emergency management professionals must have the medical supplies to serve the Force and maintain their own safety. The pandemic also identified challenges related to critical medical supply stockpiles and highlighted the importance of a safe, secure, and reliable supply chain. The DoD must remediate these supply chain risks in the event of another pandemic or other disaster.

The DoD deployed thousands of military medical personnel to supplement state and local health care capabilities during the COVID-19 response. However, the medical specialties that the civilian sector needed most from the DoD, such as critical care nursing and physician staff, are those where the DoD has chronic shortages, which in some cases limited what the DoD could provide. The DoD must assess its medical capabilities to ensure it can continue to support combat missions and provide care to beneficiaries if also called on to provide support to state and local authorities in future pandemics.

Evaluating the DoD's response to the COVID-19 pandemic, such as its ability to mitigate the virus's spread and properly protect its employees and beneficiaries, is critical to inform future policies, best practices, and resourcing decisions. The DoD established a COVID-19 after action review working group to identify lessons learned. Additionally, the FY 2021 NDAA directed numerous studies and policies to address the impacts of the COVID-19 pandemic on the DoD, including the delivery of mental health services during the COVID-19 pandemic, a strategy to leverage telehealth services, and protocols and mitigation strategies aboard ships and Navy vessels.

Since May of 2020, the DoD OIG has published a quarterly COVID-19 update that includes current information on oversight projects and other pandemic-related information. In August 2021, the DoD OIG announced an evaluation to provide DoD leadership with a snapshot of the challenges, concerns, and needs encountered by medical personnel working at DoD MTFs during the COVID-19 pandemic.

[87] Report No. DODIG-2021-069, "Audit of the Impact of Coronavirus Disease-2019 on Basic Training," March 31, 2021. Report No. DODIG-2021-049, Evaluation of the Navy's Plans and Response to the Coronavirus Disease-2019 Onboard Navy Warships and Submarines, February 8, 2021. Report No. DODIG-2021-055, "Evaluation of the Armed Forces Retirement Home Response to the Coronavirus-2019 Pandemic," February 12, 2021.

Airmen construct the first home in the Cherokee Veterans Housing Initiative in Tahlequah, Oklahoma, on May 18, 2021.
Source: The Air Force.

HEALTH AND SAFETY MANAGEMENT OF MILITARY HOUSING

From 2013 through 2020, the DoD OIG and GAO issued numerous oversight reports with recommendations to the DoD related to the quality, management, and health concerns associated with military housing. The DoD needs to improve its management of military family housing, especially as it relates to privatized military family housing. For example, a March 2020 GAO report determined that the DoD conducted some oversight of the physical condition of privatized housing, but the scope of the DoD's oversight efforts was limited.[88] In April 2020, the DoD OIG reported on systemic deficiencies in the management of three hazards present in DoD family housing—lead-based paint, asbestos-containing material, and radon. The DoD OIG also reported that DoD housing policies failed to define minimum standards for health and safety hazard management and failed to require the Military Services to assess health and safety hazards in Government-owned, Government-controlled military family housing.[89] While these oversight reports have repeatedly identified similar issues, the DoD has been slow to act in some cases, and in other cases the DoD has significant work remaining to implement changes.

The 2020 DoD OIG and GAO reports, as well as media reporting and congressional testimony about health and safety hazards in military family housing, align with the extensive requirements for military housing reform in the NDAAs for FYs 2020 and 2021. The FY 2020 NDAA listed several reforms for privatized military

[88] Report No. GAO-20-281, "Military Housing: DoD Needs to Strengthen Oversight and Clarify Its Role in the Management of Privatized Housing," March 26, 2020.

[89] Report No. DODIG-2020-082, "Evaluation of the DoD's Management of Health and Safety Hazards in Government-Owned and Government-Controlled Military Family Housing," April 20, 2020.

housing, including reforms to clarify contract management and create a dedicated process for addressing health and safety hazards in the home. The FY 2020 NDAA also called for the DoD to establish a tenant bill of rights. The bill of rights lists all the rights that military families are entitled to as tenants of privatized military housing, including the right to:

- reside in a well-maintained house that meets health and environmental standards;
- access the house's maintenance history; and
- receive a written lease with clearly defined rental terms.

The bill of rights also provides tenants with multiple avenues for promptly resolving housing problems. With a few exceptions, the FY 2020 NDAA required the DoD to start or report on efforts related to military housing reform during FY 2021. Additionally, the FY 2021 NDAA clarified language from the FY 2020 NDAA and expanded coverage to include Government-owned, Government-controlled housing. To monitor progress and ensure that the DoD appropriately implements required reforms, the DoD OIG started evaluations in March 2020 and March 2021, with a third evaluation planned for FY 2022.

The DoD has prioritized implementing the tenant rights over other housing reforms. On June 2, 2021, the Acting DoD Chief Housing Officer reported that the DoD issued policy guidance to implement the tenant bill of rights and that nearly all privatized housing partners agreed to implement the rights.[90] However, the DoD has received pushback from private partners and has been unable to negotiate some changes to privatized housing business agreements.

Furthermore, because the DoD prioritized the reforms, as of July 2021, it had not yet tackled a large portion of NDAA requirements related to health and safety hazard management and identification. In addition, the DoD did not meet a February 2021 deadline in the FY 2020 NDAA to establish and implement a uniform code of basic housing standards for safety, comfort, and habitability for privatized military housing aligned with a nationally recognized, consensus-based, model property maintenance code.

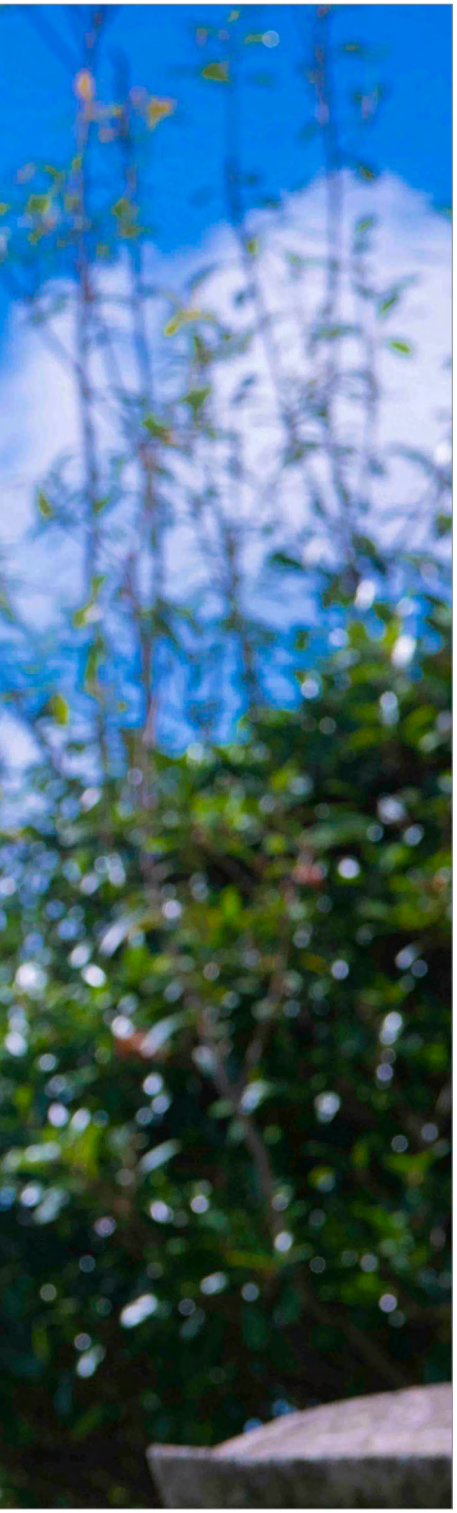
While the DoD has made progress toward ensuring safe and fully functional military housing, additional efforts are needed to complete required reforms and continue to evaluate whether these reforms have met the needs of Service members and their families. In addition to the evaluation planned in FY 2022, the DoD OIG is conducting an audit to determine the percentage of privatized military housing units determined to be unsafe, unhealthy, or both. These oversight projects will help clarify problems with military housing reform and make recommendations that help ensure the safety of military personnel and their families.

CONCLUSION

Providing adequate health care and support to military personnel and their families is a critical challenge for the DoD. How the DoD responds to the challenges of maintaining a healthy force, maintaining the skills of its medical providers, treating victims of sexual assault, providing behavioral health care, responding to a pandemic, and maintaining safe housing will have direct impacts on the health and well-being of its 9 million beneficiaries and the readiness of the Total Force.

[90] DoD, "DoD Gives Update on Tenant Bill of Rights for Privatized Housing, June 4, 2021.

An Airman 1st Class, an engineering technician with 718th Civil Engineer Squadron, Execution Support, levels a Trimble S6 at Kadena Air Base, Japan, on June 9, 2021. (U.S. Air Force photo)



Challenge 9. Recruiting and Retaining a Modern Workforce

INTRODUCTION AND OVERVIEW

When the Secretary of Defense announced his top priorities in his March 2021 Message to the Force, he stated, "Our most critical asset as a Department is our people. We remain the preeminent fighting force in the world because of our personnel in and out of uniform." The Secretary of Defense also stated that to maintain the advantage over the Nation's enemies and competitors, the DoD "will build opportunities for growth and development in the Department, invest in training and education, and create new opportunities for advancement that drive promotion and retention for our total workforce—civilian and military." Furthermore, the Secretary of Defense acknowledged that "efforts on building out a range of skills and capabilities among the workforce and removing barriers that limit our people from realizing their full potential as partners in the work of the DoD" are important steps in growing and developing the DoD's workforce.

The DoD is the Nation's largest employer, with more than 1.3 million active duty Service members, approximately 800,000 Reserve and National Guard Service members, and more than 700,000 civilian employees. As threats change and technology evolves, the DoD must have an agile, modern workforce with the skills and abilities to effectively operate in a knowledge-based environment, take advantage of emerging technologies, and continue to support traditional mission requirements.

The DoD faces workforce challenges, including identifying new skill requirements and career fields; recruiting, training, and retaining people with the right mix of skills and abilities for the wide range of DoD missions; and building a diverse and inclusive workforce that reflects the American public. A dedicated, highly skilled, and diverse workforce is essential to the readiness of the DoD.

STRENGTHENING OUR WORKFORCE PLANNING TO MEET EMERGING REQUIREMENTS

The evolving global security environment, emerging technologies, and expanding cyberspace and space domains illustrate the dynamic threats facing the United States. The Administration's Interim National Security Strategic Guidance states, "For our national security strategy to be effective, it is essential to invest in our national security workforce, institutions, and partnerships, inspire a new generation to public service, ensure our workforce represents the diversity of our country, and modernize our decision-making processes."

The dynamic threats and the significant investments in research and development require more personnel with science, technology, engineering, and math (STEM) skills. In addition, with strategic competition evolving and fewer on-site counterterrorism operations, the DoD must consider how it should transform training and education for the intelligence workforce to ensure it has appropriate subject matter experts with foreign language capabilities. The DoD must have the right manpower and human capital resources in the right places at the right time to provide for the Nation's defense.

An example of a skill gap in the STEM workforce is in the Military Service laboratories. In a December 2019 report to Congress, the Office of the Under Secretary of Defense for Research and Engineering identified the need for 7,500 more personnel in priority technology areas including hypersonics, directed energy, space, cybersecurity, and artificial intelligence (AI), among others.[91] The report stated that the Military Services lack "a phased, coordinated plan to promote priority emerging technology areas over time. In the absence of a strategy that would be defensible in long-range budget planning negotiations, DoD laboratories struggle to acquire sufficient resources." To maintain an advantage over strategic competitors and ensure that the DoD leads in various technology fields, the DoD must continue to identify the need for STEM skills and determine the best way to use its funding to recruit and retain the required workforce.

A 2021 RAND Corporation report on talent management for DoD knowledge workers, such as those in STEM fields, found problems in DoD's ability to build and organize, train and develop, motivate and manage performance, and promote and retain the right talent.[92] The RAND report found that the DoD struggled to define the required capabilities and job classification for personnel with responsibilities related to cyber, data science, and security cooperation. RAND research found that the DoD could improve its training and development by identifying specific competencies and measuring whether training and development improved those competencies in knowledge workers. In addition, the research showed that nonfinancial incentives, such as meaningful work and the opportunity for lifelong learning, were powerful incentives for knowledge workers and were potentially more influential than financial incentives. The DoD could consider increasing and expanding its use of nonfinancial incentives to motivate and retain skilled knowledge workers, including those in the cyber workforce.

[91] Office of the Under Secretary of Defense for Research and Engineering, "Report to Congress on Workforce and Infrastructure Needs for National Defense Strategy Priority Technologies," December 2019.

[92] RAND Corporation, "Talent Management for U.S. Department of Defense Knowledge Workers: What Does RAND Corporation Research Tell Us?," January 2021.

COMPETING FOR INTERESTED SKILLED, AND QUALIFIED INDIVIDUALS IN THE CYBER WORKFORCE

The DoD's ability to recruit and retain talented individuals is important in many career fields, but perhaps most critical in highly skilled fields, such as STEM. As discussed earlier, the DoD has a gap in the STEM workforce needed to work on emerging technologies and conduct research and development. These skillsets are in high demand, and often bring higher pay in the private sector than at the DoD. To further explain the DoD's challenges with attracting and retaining a workforce with STEM skills, we focus on the cybersecurity profession, which includes civilians, Service members, and contractors that work in system administration, cybersecurity management, software development, network services, and 28 other specialty areas.

COMPETING DEMAND FOR THE CYBER WORKFORCE

The DoD continues to struggle to recruit and retain a highly skilled cyber workforce. The 2021 National Security Commission on AI report states that the U.S. Government will not be able to recruit its way out of its technology workforce deficit.[93] According to the report, in 2020 alone, there were more than 430,000 open computer science jobs in the United States; however, there are only 71,000 new computer science graduates from American universities each year. In addition to the limited pool of graduates, the DoD has to compete with big tech firms and others within the private sector who can offer more workplace flexibilities and higher pay.

According to an April 2021 *FedScoop* article, the Acting Deputy Assistant Secretary of Defense for Civilian Personnel Policy stated that the DoD is one of the three largest markets for cybersecurity talents and is in competition with the private sector for top personnel out of college.[94] In an attempt to be more competitive on pay, the DoD received approval for Cyber Excepted Service pay rates for 2021, which supplement pay rates in target markets. However, there are still gaps in the pay that can be offered by the DoD when compared to the private sector. For example, for an entry-level cyber position where the candidate has a bachelor's degree and no previous experience:

- the DoD can offer a starting salary of $50,784; but
- the private sector offers a median starting salary of $79,267.[95]

This is a nearly $30,000 pay discrepancy when comparing the DoD to the private sector. However, salary is not the only mechanism for recruiting cyber professionals. The DoD has developed several programs and initiatives such as direct hire authorities, special and incentive pay, and private industry practices such as remote work, flexible working hours, and performance bonuses. A 2021 RAND Corporation study found that incentive pay such as recruitment, relocation, and retention awards were not heavily used in the DoD civilian cyber workforce, based on data from 2010 through 2018.[96] In addition to incentives, the DoD mission can be an advantage when

[93] National Security Commission on Artificial Intelligence, "Final Report," 2021.

[94] *FedScoop*, "DoD Grapples With the Future of its Cyber Workforce," April 22, 2021.

[95] The DoD pay is based on the Cyber Excepted Service pay for 2021 for a GG-7 grade. The private sector pay is based on Salary.com for an entry level cyber security analyst as of October 2021. Salary.com uses salary information reported by human resources departments to estimate low, median, and high pay for a particular labor field.

[96] RAND Corporation, "DoD Cyber Excepted Service Labor Market Analysis and Options for Use of Compensation Flexibilities," 2021.

An instructor for the Information Technology Training Center, National Guard Professional Education Center, observes a recruit during the Interactive War Games cyber recruiting drive beta test at Robinson Maneuver Training Center, North Little Rock, Arkansas, on March 13, 2021. The Interactive War Games cyber recruiting drive is a program that former National Guard Marksmanship Training Center members created to encourage service through cyber warfare technology using video games.

Source: The Army National Guard.

competing with the private sector, because working for the DoD may appeal to an individuals' sense of duty.

The DoD continues to face challenges in recruiting and retaining top-tier cyber talent. During an April 2021 hearing on the cyber workforce before the Senate Armed Services Subcommittee on Personnel, the Joint Staff Chief Information Officer (CIO) stated that DoD Cyber recruitment and retention initiatives are meant to narrow the skills gap, but it may not be enough to keep pace with the DoD's demand for a talent level that we have not seen before. The Joint Staff CIO further stated, "The human-machine interface brings a demand that is going to have to be found, cultivated, and educated to get to the level of experience needed as we learn and work our way through the implementation of new capability sets." These skills will be especially important with the increase in use of AI and the "zero trust" model for purchasing information technology, which assumes that there is no implicit trust granted to assets or user accounts based solely on their physical or network location. For more information on AI and the zero trust model, see Management Challenge 3, "Strengthening DoD Cyberspace Operations and Securing Systems, Networks, and Data." For more on the zero trust model for procuring microchips, see Management Challenge 4, "Reinforcing the Supply Chain While Reducing Reliance on Strategic Competitors."

UNDERSTANDING THE REQUIREMENTS AND PLANNING FOR THE CYBER WORKFORCE

The DoD must have the right information to effectively plan and develop its cyber workforce. The DoD is still struggling to identify all of its critical cyber work roles and skill gaps.

In 2015, the Federal Cybersecurity Workforce Assessment Act required the DoD to code cyber positions in accordance with national guidance so that the cyber work roles are accurately describing the responsibilities, knowledge, skills, and abilities needed for that role. In a 2019 report, the Government Accountability Office determined that the DoD did not appropriately assign work role codes to vacant positions, categorize work codes, or categorize work codes consistent with their position descriptions for the IT management occupational job series.[97]

In 2021, the DoD updated its Cyber Workforce Management Framework to require Components to identify their cyber workforce and code the positions according to specialty areas that best describe the work they perform within the cyber domain.[98] However, in August 2021, the DoD OIG found that DoD Components had not coded, or had incorrectly coded, some of their civilian cyber workforce positions in accordance with the DoD Coding Guidance.[99] The Office of the DoD CIO is currently developing DoD-wide guidance to clarify the process for coding the cyber workforce and establishing recruitment, retention, and qualification standards.

Without complete and accurate data, the DoD will continue to be challenged to identify gaps in the cyber workforce and effectively develop or modify existing DoD Cyber workforce hiring priorities and recruitment initiatives.

RETAINING THE DOD CYBER WORKFORCE

The DoD needs to improve its cyber workforce retention programs. During the April 21, 2021 hearing before the Senate Armed Services Subcommittee on Personnel, the Joint Staff CIO stated, "I don't think we know our target audience as well as we need to. We need to find out what really motivates individuals to want to serve in the capacity that we're offering." For example, the Military Services all have different retention bonuses, rotation cycles, and retention incentives. To address the retention problem, the Office of the DoD CIO is developing a pilot training program for human resources personnel to learn how to better attract and retain technical talent.

An example of how the DoD is challenged with retaining well-trained cyber personnel in the Military Services is with the U.S. Cyber Command and its subordinate commands. The U.S. Cyber Command uses retention tools such as the DoD's Assignment Incentive Pay program and providing Service members with specialty cyber training that may take up to 9 months to complete. However, the Military Services control the personnel assignments and promotion criteria for the Service members. Consequently, there is no guarantee that after completing specialty cyber training and receiving the incentive pay that the Service member will remain in the U.S. Cyber Command or use that specialized cyber training again in their next assignment. For example, if Service members in the Navy want to be competitive for promotion, they must serve in leadership positions in their original rating, or military occupational specialty. These positions may not be in a cyber command, so the Service members will not likely be applying their cyber skills. By not ensuring that its cyber-trained

---

97 Report No. GAO-19-144, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," March 12, 2019.

98 DoD Directive 8140.01, "Cyberspace Workforce Management," effective October 5, 2021.

99 Report No. DODIG-2021-110, "Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce," July 29, 2021.

Table 1. Underrepresentation of Minority Groups and Women in DoD SES Positions

Race, Ethnic Group, or Gender	Estimated Percent of U.S. Population[1]	Percent of DoD SES[2]	Percentage Point Disparity
American Indian and Alaska Native	1.3	0	1.3
Asian and Pacific Islanders	5.9 (Asian) 0.2 (Pacific Islander)	3	2.9
Black or African American	13.4	6.3	7.1
Hispanic	18.5	3.2	15.3
Women	50.8	33.3	17.5

[1] As of July 1, 2019.

[2] Data from 2020 or 2021.

Source: U.S. Census Bureau, DoD Office for Diversity Equity and Inclusion, and Defense Manpower Data Center and Individual DoD Agencies Civilian Personnel Data Systems.

Service members continue to work in the cyber community, the DoD risks the readiness and competitive advantage of its cyber workforce.

Cyber is only one example of critical skills gaps in the STEM fields and the competition that the DoD faces from the private sector in recruiting highly skilled personnel in STEM fields. As previously discussed, a December 2019 report to Congress from the Office of the Under Secretary of Defense for Research and Engineering identified a need for 7,500 more personnel in the STEM fields to work in the Military Services laboratories. These STEM workers are needed to support DoD activities related to new and emerging technologies, but the DoD must compete with the private sector for these highly skilled workers. Recruiting and retaining interested and qualified individuals in the STEM fields will remain a persistent challenge for the DoD.

DEVELOPING A DIVERSE AND INCLUSIVE WORKFORCE

A diverse and inclusive civilian and military workforce that represents the American public enables the DoD to benefit from a diversity of backgrounds, thoughts, and experiences. According to data from the DoD's Office of Diversity, Equity, and Inclusion and the U.S. Census Bureau, the DoD has racial, ethnic, and gender disparity in its civilian and military workforce. Table 1 shows the disparity in minority groups and women in DoD Senior Executive Service (SES) positions when compared to the overall U.S. population.

As Table 1 shows, the largest disparities in DoD SES positions are with women and Hispanics, with disparities of more than 15 percentage points when compared to the U.S. population. DoD data also shows racial and ethnic underrepresentation at the general and flag officer pay grades and the senior noncommissioned officer (NCO) pay grades in DoD Active and Reserve components. Table 2 shows the disparity in minority groups when the military leadership positions for the Active component are compared to the overall U.S. population.

As shown in Table 2, there is better minority representation in senior NCO positions than in the general and flag officer positions; however, a few minority groups remain underrepresented in senior NCO positions. Data for the Reserve component also shows underrepresentation

Table 2. Underrepresentation of Minority Groups in Active Component General and Flag Officer and Senior NCO Pay Grades

Race or Ethnic Group	Estimated Percent of U.S. Population*	General and Flag Officers		Senior NCOs	
		Percent of O-7	Percent of O-10	Percent of E-8	Percent of E-9
White	76.3	86.0	92.0	56.0	61.0
American Indian and Alaska Native	1.3	0	0	1.0	1.0
Asian	5.9	2.0	3.0	4.0	3.0
Pacific Islander	0.2	0	0	1.0	1.0
Black or African American	13.4	8.0	5.0	19.0	20.0
Hispanic	18.5	3.0	0	16.0	13.0
Multiracial	2.8	1.0	0	3.0	3.0

* As of July 1, 2019.

Note – The general and flag officer and senior NCO data is from 2020.
Source: U.S. Census Bureau and DoD Board on Diversity and Inclusion Report.

of minority groups, and the disparity in representation is worse than in the Active component. For the Reserve component every minority group is underrepresented in the O-7 grade. Similar to the Active component, the senior NCO positions in the Reserve component have better minority representation, but each minority group is underrepresented in both the E-8 and E-9 grades.

The DoD, Congress, and Administration recognized the need to identify, evaluate, and mitigate barriers to diversity and inclusion in the DoD. For example, the Department of the Army mandated the removal of photographs and demographic information from promotion and selection boards and expanded this practice to

Sailors and Marines pay tribute to the victims of the 9/11 attacks on the flight deck of the USS *Arlington*, on September 6, 2021.
Source: The Navy.

other types of selection boards.[100] While this policy is a good step toward reducing implicit or explicit bias during the selection process, there is still the potential for bias.

Congress included a requirement in the National Defense Authorization Act for FY 2021 for the Secretary of Defense to establish a Deputy Inspector General with the responsibility to conduct and supervise audits, investigations, and evaluations of DoD policies, programs, systems, and processes related to supremacist, extremist, and criminal gang activity in the force. In addition, the Administration issued a January 20, 2021 Executive Order that required each Federal agency to "assess whether, and to what extent, its programs and policies perpetuate systemic barriers to opportunities and benefits for people of color and other underserved groups" and report on the results of the assessment within 200 days of the order.[101] The DoD completed the required report on August 9, 2021; however, the document is marked as controlled unclassified information, so the results cannot be shared publicly.

To achieve a diverse and inclusive workforce, the DoD must ensure that it understands the demographics of its workforce across all levels, and recruit, promote, and retain a diverse group of qualified and high-performing individuals. The underrepresentation of women and minorities in DoD senior leader positions means a lack of diversity in perspectives, analysis, and ideas. A diverse workforce can collectively reduce blind spots because of the variety of viewpoints and skillsets it possesses. The DoD must continually evaluate its policies, procedures, and actions to demonstrate a commitment to a diverse, inclusive workforce, otherwise it risks losing future leaders as they leave civil and military service.

CONCLUSION

With the largest workforce in the United States, the DoD is in a unique position to lead the U.S. Government in recruiting and retaining a highly skilled workforce capable of addressing the dynamic threat environment the DoD faces. Key to this workforce are those in the STEM fields who are needed to advance DoD progress in new and emerging technologies. Within the STEM fields, recruiting and retaining cyber workers continues to challenge the DoD as it competes with the private sectors and develops attractive incentives. Furthermore, the DoD should continue to take steps to ensure that its civilian and military senior leaders represent the diversity of the American people.

---

[100] Secretary of the Army Memorandum, "Elimination of Department of the Army (DA) Photos, and Race, Ethnicity and Gender Identification Data for Officer, Warrant Officer, and Enlisted Selection Boards (Updated), June 26, 2020. Assistant Secretary of the Army (Manpower and Reserve Affairs) Memorandum, "Updated Guidance Regarding the DA Photo and Use of Race, Ethnicity, and Gender Identifying Data in Assignment and Slating Processes," October 19, 2020.

[101] Executive Order 13985, "Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," January 20, 2021.

Airmen prepare a U.S. flag at Dover Air Force Base, Delaware, on August 5, 2021.

Source: The Air Force.

A Marine Corps officer candidate recites the Oath of Office, completing Officer Candidates School on Marine Corps Base Quantico, Virginia, on August 14, 2021. (U.S. Marine Corps photo)

Challenge 10. Preserving Trust and Confidence in the DoD

INTRODUCTION AND OVERVIEW

The DoD's continued response to several critical issues, highlighted by events in the last few years, will affect how DoD personnel and the public perceive the Department. The sexual harassment and death of Army Specialist Vanessa Guillen at Fort Hood, Texas, focused renewed attention on the DoD's struggle to prevent sexual harassment and sexual assault. The demonstrations and civil unrest in 2020 to bring awareness to racism and discrimination focused attention on diversity and disparate treatment within the DoD. Finally, the protest and rioting at the U.S. Capitol campus on January 6, 2021, focused attention on what constitutes extremism and when it should be reported and investigated.

In January 2021 testimony to the Senate Armed Services Committee, the Secretary of Defense stated, "I will fight hard to stamp out sexual assault … to rid our ranks of racists … and to create a climate where everyone fit and willing has the opportunity to serve this country with pride and with dignity. The Defense Department's job is to keep America safe from our enemies. But we can't do that if some of those enemies lie within our own ranks." The DoD continues to face challenges in preventing and addressing sexual harassment and sexual assault, disparate treatment, and extremism within the ranks. These complex challenges are fundamentally at odds with the DoD's values, and if left unchecked, they will erode trust and confidence in the DoD.

In addition to each challenge's unique elements, they share certain contributing factors, including the lack of effective training programs, reliable data for making informed decisions, and transparency and accountability of processes. By addressing these challenges and contributing factors, the DoD has the opportunity to bolster the public's trust and confidence, and even more importantly, to preserve the trust and confidence of its most valuable asset—its military and civilian personnel.

SEXUAL HARASSMENT AND SEXUAL ASSAULT

The DoD has a responsibility to prevent and respond to sexual harassment and sexual assault within its workforce, and has worked to address these serious issues.[102] There have been many comprehensive reports, studies, and investigations to identify, assess, and recommend ways to eradicate sexual harassment and sexual assault within the DoD. In a February 2021 memorandum, the Secretary of Defense stated, "[S]exual assault and harassment remain persistent and corrosive problems across the Total Force." The Secretary acknowledged limited progress and said that progress fell short of making any lasting change.[103] Addressing the prevalence of sexual harassment and sexual assault is critical for the DoD because of their effects on individuals and the readiness of the Total Force. The negative effects include psychological and physical health problems, which can lead to substance abuse and suicide.

Sexual harassment and sexual assault continue to be underreported. According to the DoD, in 2018, more than 20,000 Service members (13,000 women and 7,500 men) responded to a survey that they were sexually assaulted; however, fewer than 8,000 Service members reported their assault.[104] Marginalized populations within the DoD, including racial and ethnic minorities and LGBTQ+ Service members experience sexual violence in far greater proportions than other populations. For example, according to a 2017 RAND Corporation report, Service members who identify as LGBTQ+ make up 12 percent of the active duty population but represent 43 percent of all sexual assaults among Service members.[105] Recent studies found that victims from all backgrounds did not report their abuse because they believed that the allegations would be mishandled, they would be ostracized, they would be retaliated against, or their perpetrators would not be held accountable.[106]

In February 2021, the Secretary of Defense commissioned an independent review of sexual assault in the military, which identified many areas of concern, such as lack of leader accountability, broken systems, deficiencies in training, and outdated gender and social norms. To address these concerns, the July 2021 Independent Review Commission (IRC) Report recommended reforms aimed at improving services and care; resource programs; responses to domestic violence; data collection, research, and reporting; accountability; prevention; and climate and culture. In response to the July 2021 IRC Report, the President stated that these reforms will be some of the most significant that the military has undertaken in recent history.[107]

Congress continues to engage with the DoD on the role of commanders in addressing sexual harassment and sexual assault. Congress has recently taken bipartisan steps to enact legislation to remove sexual assault prosecution decisions from the chain of command to attorneys with significant trial experience, offering victims an independent resource to make prosecution

[102] Report No. GAO-21-113, "Sexual Harassment and Assault – Guidance Needed to Ensure Consistent Tracking, Response, and Training for DoD Civilians," February 9, 2021.

[103] Secretary of Defense Memorandum, "Immediate Actions to Counter Sexual Assault and Harassment," February 26, 2021.

[104] DoD Sexual Assault and Prevention Office, "Department of Defense Annual Report on Sexual Assault in the Military, Fiscal Year 2019," April 17, 2020 (FY 2020 Annual Report on Sexual Assault).

[105] RAND Corporation, "Sexual Assault of Sexual Minorities in the U.S. Military," 2021.

[106] RAND Corporation, "Sexual Assault of Sexual Minorities in the U.S. Military," 2021. Independent Review Commission (IRC) on Sexual Assault and the Military, "Hard Truths and the Duty to Change: Recommendations From the Independent Review Commission on Sexual Assault in the Military," July 2021. FY 2020 Annual Report on Sexual Assault.

[107] The White House, "Statement of President Joe Biden on the Results of the Independent Review Commission on Military Sexual Assault," July 2, 2021.

decisions, among other provisions.[108] However, as of October 5, 2021, this legislation had not been enacted.

In a May 2021 letter to the ranking member of the Senate Armed Services Committee, the Chairman of the Joint Chiefs of Staff stated, "[We] have not made sufficient progress in recent years to eliminate sexual assault, and have consequently lost the trust and confidence of many Soldiers, Sailors, Airmen, Marines, and Guardians in the chain of command's ability to adjudicate these serious crimes."[109] The DoD must remain steadfast and focused on addressing sexual harassment and sexual assault and find ways to make real and measurable progress to preserve trust with the American public and DoD personnel.

DISPARATE TREATMENT

The existence of disparities for both military and civilian personnel remains front and center for the DoD. A May 2019 Government Accountability Office report determined that Black Service members were twice as likely to be investigated as White Service members in each branch.[110] The Government Accountability Office also determined that the Military Services did not collect and maintain consistent information about race and ethnicity in their investigations, military justice, and personnel databases, making it difficult to identify disparities.

A 2020 Department of the Air Force Office of Inspector General review confirmed that racial disparity exists for Black or African American Service members in the areas of law enforcement apprehensions, criminal investigations, military justice, and personnel databases, including disparities in administrative separations, certain promotion rates, and career developmental opportunities. In 2020, a RAND Corporation study of the Air Force civilian workforce found that Black or African American and Hispanic men started at lower entry grades than White men.[111] The study further identified a low advancement rate for Asian males and individuals with disabilities, and that women were underrepresented as civilians in the most senior grades. The RAND study found that women also tend to enter the civil service at lower pay than their male counterparts and that civilian employees who start at a lower grade struggle to "catch up," limiting their senior leadership opportunities.

A second Air Force Office of Inspector General review on racial and ethnic disparities found that the largest gaps for females, Asian Americans, American Indians or Alaska Natives, Pacific Islanders, and Hispanics were in the operational career fields, which include pilots and other combat-related positions.[112] For example, in May 2020, nearly 84 percent of the pilots in the active duty Air Force were white, and more than 92 percent were male. July 2019 estimates from the U.S. Census Bureau show that White people were 76.3 percent of the population and men were 49.2 percent of the population. For Air Force pilots, women and racial and ethnic minorities were underrepresented, with the largest racial and ethnic disparity in Hispanics. Furthermore, the review found that statistically, ethnic and gender disparities have not changed over the years.

While Federal law prohibits discrimination, structural inequality and policies that foster unfairness are catalysts for disparate treatment and remain a systemic challenge for

[108] Vanessa Guillén Military Justice Improvement and Increasing Prevention Act of 2021.

[109] Chairman of the Joint Chiefs of Staff Letter to Senator James M. Inhofe, May 19, 2021.

[110] Report No. GAO-19-344, "Military Justice: DoD and the Coast Guard Need to Improve Their Capabilities to Assess Racial and Gender Disparities," May 30, 2019.

[111] RAND Corporation, Project Air Force study, "Advancement and Retention Barriers in the U.S. Air Force Civilian White Collar Workforce: Implications for Demographic Diversity," 2020.

[112] Department of the Air Force Inspector General, "Report of Inquiry (S8918P) Disparity Review," September 2021.

the DoD. Structural inequality is caused by embedded biases in the fabric of organizations, institutions, governments, or social networks that provide advantages for some, while providing disadvantages for others. There is evidence of structural inequality in the selection of general, flag, and senior noncommissioned officers in both DoD Active and Reserve components. At the E-8, E-9, O-7, and O-10 grades, nearly all minority race or ethnic groups are underrepresented. The most underrepresentation in those grades is with Blacks or African Americans and Hispanics. A January 20, 2021 Executive Order stated that advancing equity requires a systemic approach to embedding fairness in decision-making processes, and "executive departments and agencies must recognize and work to redress inequities in their policies and programs that serve as barriers to equal opportunity."[113] For more information on a diverse and inclusive workforce, see Management Challenge 9, "Recruiting and Retaining a Modern Workforce."

Since the Civil Rights Act of 1964, the United States, including the DoD, has aimed to protect its people from discrimination and disparate treatment. Progress continues to be made, but disparate treatment based on race and gender persists in the DoD both in the civilian workforce and in the military. To preserve trust and confidence, the DoD must examine root causes for inequities, such as policies and programs that limit equal opportunity for women and minority groups, and break those barriers down. Senior leader involvement is critical in promoting ethical work culture and addressing disparities through open communication systems that foster a better work culture for all. A climate that fosters diversity and inclusion is paramount to neutralize biases.

EXTREMISM

The DoD is aware of few incidents where military members were involved with extremist organizations and activities, with only 45 incidents being tracked by the DoD as of January 2020. However, the full scope of the potential problem is unknown. As the Secretary of Defense noted in an April 2021 memorandum, any extremist activity in the force can have a disproportionately large impact.[114] With social media and the emboldened attitude of many extremist groups and their sympathizers, extremist ideology now spreads with unprecedented speed and pervasiveness.[115] On May 27, 2021, the Chairman of the Joint Chiefs of Staff testified to the House Appropriations Committee that even a small percentage of neo-Nazis, Ku Klux Klan members, or other similar extremists in the force would be unacceptable. The presence of even a few extremists in the military poses a national security concern not only because of Service members' warfighting training and education, but also because of the reputational risk to the DoD from Service member involvement in high-profile incidents.

Congress and the DoD are moving aggressively to address extremism in the military. In section 554 of the National Defense Authorization Act (NDAA) for FY 2021, Congress required the Secretary of Defense to establish a Deputy Inspector General with the responsibility to conduct and supervise audits, investigations, and evaluations of DoD policies, programs, systems, and processes related to supremacist, extremist, and criminal gang activity in the force. Congress also established an annual DoD reporting requirement for these types of incidents and the policies, processes, and mechanisms implemented to

[113] Executive Order 13985, "Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," January 20, 2021.

[114] Secretary of Defense Memorandum, "Immediate Actions to Counter Extremism in the Department and the Establishment of the Countering Extremism Working Group," April 9, 2021.

[115] Secretary of Defense, "Remarks on Extremism in the Military," February 19, 2021.

Noncommissioned officers from the Oklahoma Army National Guard discuss placement of their Soldiers as they provide security around the U.S. Capitol building on January 19, 2021. At least 25,000 National Guard Soldiers were activated to conduct security, communication, and logistical missions in support of federal and District authorities leading up to and through the 59th Presidential Inauguration.

Source: The National Guard Bureau.

report and track the incidents. In April 2021, the Secretary of Defense stood up the Countering Extremism Working Group and tasked it with addressing such immediate actions as:

- reviewing and updating DoD Instruction 1325.06, "Handling Dissident and Protest Activities Among Members of the Armed Forces";
- updating pre-separation checklists to create awareness and present reporting options related to extremist recruiting;
- reviewing and standardizing screening questionnaires for new recruits; and
- commissioning a study on extremist activity within the Total Force.[116]

The DoD OIG has an ongoing evaluation to determine the extent to which the DoD and the Military Services have implemented policies and procedures that prohibit active advocacy and participation related to supremacist, extremist, or criminal gang doctrine, ideology, or causes.

While addressing extremist activity in the ranks is urgent, attempts to re-address the scope of individual civilian and military member rights to speech and association in light of this heightened focus pose a complex challenge. The Supreme Court has repeatedly recognized that while Federal employees do not automatically relinquish their rights under the First Amendment by accepting U.S. Government employment, the U.S. Government may impose reasonable restraints on the job-related speech of public servants that would be unconstitutional if applied to private citizens. This is especially true for military personnel, where a Service member's constitutional rights may be restricted

[116] Secretary of Defense Memorandum, "Immediate Actions to Counter Extremism in the Department and the Establishment of the Countering Extremism Working Group," April 9, 2021.

in furtherance of national defense.[117] However, DoD policy has historically endorsed preserving a Service member's right of expression to the maximum extent possible while considering good order, discipline, and national security.[118]

In February 2021, the Secretary of Defense noted that actively espousing ideologies that encourage discrimination, hate, and harassment against others is counter to the core principles of dignity and mutual respect, and counter to military members' oath to uphold the Constitution.[119] While responding to extremism in the DoD poses complex challenges, the DoD must continue to take action to meet those challenges in order to preserve trust and confidence.

CROSS-CUTTING CONTRIBUTING FACTORS

There are contributing factors that affect the DoD's ability to respond to sexual harassment and sexual assault, disparate treatment, and extremism. The DoD must ensure that it is offering the right training at the right time, has access to complete and accurate data and expertise to analyze and interpret that data, and is accountable for its actions. By addressing these cross-cutting factors, the DoD can make strides in preserving trust and confidence in the DoD.

The first contributing factor is the lack of appropriate training or the lack of information on whether training was effective. Military leaders need to know whether they are providing the right training, to the right people, in an effective manner. This includes preventive training, such as training on the expectations of public service and professional interpersonal conduct, as well as training on the processes for addressing complaints of sexual harassment and sexual assault, disparate treatment, and extremism. In some cases, the DoD will implement training and treat the training itself as a solution. However, the DoD must gather data and allow time to assess whether the training had the intended effects. Issue-specific challenges, such as the absence of a precise definition of extremism, also hinder the DoD's ability to develop training that provides robust guidance to both Service members and commanders about the scope of permissible speech and association.

The second contributing factor is lack of access to high-quality consistent data and, in some cases, expertise to interpret and analyze that data to make evidence-based decisions. For example, according to the July 2021 IRC Report, personnel leading prevention activities for sexual harassment and sexual assault are often dual-hatted or tasked as collateral duty sexual assault responders. Therefore, these personnel generally do not have the expertise to design, implement, and evaluate comprehensive prevention activities. High-quality data requires knowing what data to collect, the systems in which the data is stored, as well as the active involvement of victims, witnesses, and other personnel who possess the data. In the area of sexual assault, reporting continues to pose challenges even after extensive DoD efforts to encourage reporting. According to the July 2021 IRC Report, getting victims to come forward continues to be impeded by the social stigma of peers, which has proven relatively intractable, even after congressional action that required direct involvement from commanders.

---

117 *Pickering v. Board of Ed. Of Township High School Dist.*, 391 U.S. 563 (1968); Opinion of the Judge Advocate 2000-71, October 2, 2000, as certified September 20, 2015.

118 DoD Instruction 1325.06, "Handling Dissident and Protest Activities Among Members of the Armed Forces," November 27, 2009; DoD Directive 1325.6, "Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces," October 1, 1996; DoD Directive 1325.6, "Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces," September 12, 1969.

119 Secretary of Defense, "Remarks on Extremism in the Military," February 19, 2021.

The July 2021 IRC Report also highlighted the lack of data on offender motivation, which can limit the effectiveness of sexual assault prevention.

The lack of data and the ability to interpret data is a problem for not just sexual harassment and sexual assault, but also extremism and disparate treatment. The DoD must continue to ensure that it gathers the appropriate kind of data, analyzes that data, and provides useful information to decisions makers so they can identify root causes and effectively combat the problems at their sources. Section 554 of the FY 2021 NDAA included multiple reporting requirements to ensure that the DoD has sufficient data related to allegations of extremism and the outcomes of those allegations. With regard to extremism, although Congress made a concerted effort to track extremist activity, the Military Services are working to develop a mechanism to track data effectively. According to the DoD's January 2020 report to Congress on military personnel and extremist ideologies, the Military Services each have numerous channels through which such incidents may be discovered.[120] However, none of these channels isolates or clearly identifies extremist activity, and each may overlap the others or have gaps in their reporting. As a result, incidents may be counted multiple times, or missed entirely, and current DoD data provides only a limited sense of the scope of the problem.

The third contributing factor is lack of accountability or transparency in the investigative process. Both DoD personnel and the public want allegations of sexual harassment and sexual assault, disparate treatment, and extremist activity to be addressed appropriately and equitably. For example, the July 2021 IRC Report stated that victims of sexual harassment and sexual assault believe they have been let down by their leaders when those behaviors were allowed to continue; appropriate actions were not taken; retaliation, ostracization, and re-victimization was allowed; and confidentiality was violated. Military leaders continue to face the additional challenge of showing that they are thoroughly investigating allegations in accordance with requirements while balancing the need to protect the privacy of those involved, including the accused. Through a thorough and, to the extent possible, transparent investigative process, DoD leadership can demonstrate that it holds perpetrators accountable and protects its people.

CONCLUSION

The Chairman of the Joint Chiefs of Staff stated at a May 2021 Howard University Reserve Officer Training Corps commissioning,"[Y]ou are about to take an oath, and this will forever be your North Star, your home base in a storm. Your moral center. … We will stay true to that oath and the American people." This moral center includes honesty, integrity, character, and selflessness, which are the essence of ethical conduct. According to the Secretary of Defense, ethical conduct means, "demonstrating in real and meaningful ways the degree to which we take seriously our role as good stewards of the taxpayers' dollars and of their trust and confidence. [It] means rededicating ourselves, constantly, to the privilege of being public servants."[121] To preserve the trust and confidence of the public and DoD personnel, the DoD must take meaningful steps to address the threats that sexual assault and sexual harassment, extremist activity, and disparate treatment pose to DoD personnel.

[120] Office of the Under Secretary of Defense for Personnel and Readiness, "Report to Congress on Military Personnel and Extremist Ideologies," January 2020.

[121] Secretary of Defense Memorandum, "Reaffirming Our Values and Ethical Conduct," March 1, 2021.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Coordinator's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. For more information, please visit the Whistleblower Protection Coordinator's webpage at:

https://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Protection-Coordinator/.

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