INSPECTOR GENERAL

U.S. Department of Defense

FISCAL YEAR 2020

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, 2019

The Reports Consolidation Act of 2000 requires each Inspector General (IG) to prepare an annual statement that summarizes 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 also be included in the Agency Financial Report.

This document, the FY 2020 Top DoD Management Challenges, outlines the DoD OIG's independent assessment of the DoD's most significant management challenges. This document is forward looking and identifies the top challenges facing the DoD in FY 2020 and beyond. The DoD OIG also uses this document as a critical part of the DoD OIG's oversight planning process, which seeks to ensure that the DoD OIG's planned oversight of DoD programs and operations addresses the DoD's most significant management challenges.

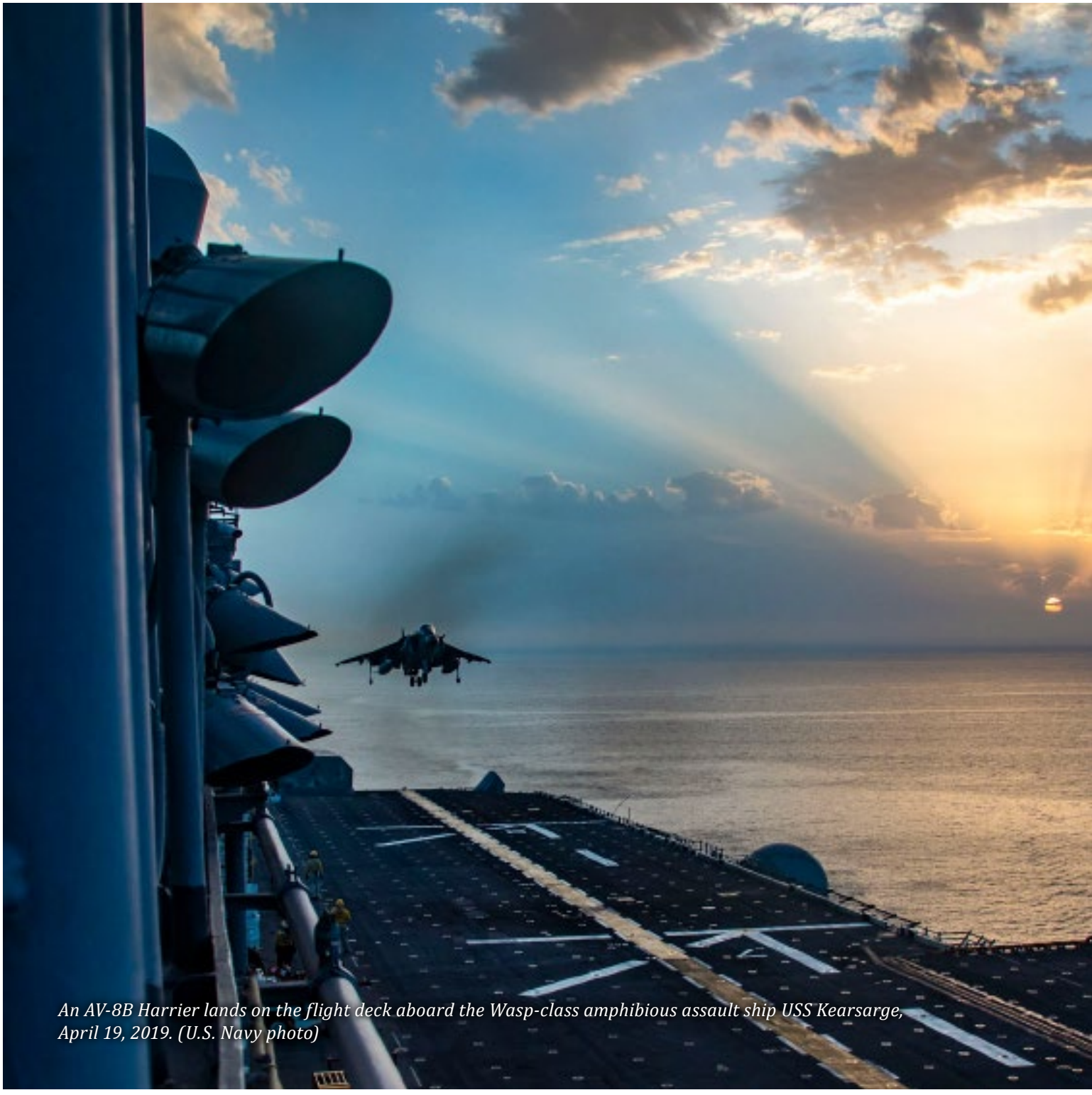
The DoD OIG independently identifies these challenges based on a variety of factors, including our independent research, assessment, and judgment; oversight work completed by the DoD OIG and other oversight organizations; congressional hearings and legislation; input from DoD officials; and issues highlighted by the media that are adversely affecting the DoD.

This year, many of the challenges remain from previous years, because they are persistent, long-standing challenges that the DoD will continue to face. The DoD OIG added two new management challenges this year, focused on the welfare and well-being of service members and their families and on supply chain management and security. Both of these are critical issues that contribute to the readiness of the DoD and its ability to pursue its mission.

In this document, we discuss each challenge, the actions taken by the DoD to address the challenge, and we assess the DoD's progress towards addressing each challenge. We also discuss completed oversight work and ongoing and planned DoD OIG oversight work related to the challenges.

The DoD OIG will continue to assess these challenges and conduct independent oversight to help promote the economy, efficiency, and effectiveness of the DoD; detect and deter fraud, waste, and abuse in DoD programs and operations; and ensure ethical conduct throughout the DoD.

Glenn A. Fine
Principal Deputy Inspector General
Performing the Duties of Inspector General



An AV-8B Harrier lands on the flight deck aboard the Wasp-class amphibious assault ship USS Kearsarge, April 19, 2019. (U.S. Navy photo)

Summary of Management and Performance Challenges Facing the DoD

FISCAL YEAR 2020

U.S. Army paratroopers assigned to 1st Squadron, 91st Cavalry Regiment, 173rd Airborne Brigade perform an airborne proficiency jump over Bunker Drop Zone in Grafenwoehr Training Area, August 14, 2019. (U.S. Army Photo)

Executive Summary

The DoD OIG independently identifies the top management challenges after soliciting input from across the DoD, reviewing congressional legislation and hearings, considering oversight work completed by the U.S. Government Accountability Office and other Defense oversight organizations, and examining issues highlighted by the media that are adversely affecting the performance of the DoD. The DoD OIG also assesses the DoD's progress towards addressing previously reported findings and recommendations from completed audits, evaluations, and investigations.

FY 2020 TOP DOD MANAGEMENT CHALLENGES

The FY 2020 Top DoD Management Challenges are:

1. Countering China, Russia, Iran, and North Korea
2. Countering Global Terrorism
3. Ensuring the Welfare and Well-being of Service Members and Their Families
4. Ensuring Ethical Conduct
5. Financial Management: Implementing Timely and Effective Actions to Address Financial Management Weaknesses Identified During the First DoD-Wide Financial Statement Audit
6. Enhancing DoD Cyberspace Operations and Capabilities
7. Enhancing Space-Based Operations, Missile Detection and Response, and Nuclear Deterrence
8. Improving Supply Chain Management and Security
9. Acquisition and Contract Management: Ensuring That the DoD Gets What It Pays For On Time, at a Fair Price, and With the Right Capabilities
10. Providing Comprehensive and Cost-Effective Health Care

These challenges are not listed in order of importance or by magnitude of the challenge. All are critically important management challenges facing the DoD.

NEW DOD MANAGEMENT CHALLENGES

Many of the top management challenges facing the DoD are enduring challenges that do not change each year. However, each year the OIG assesses the challenges, deleting some, adding others, and modifying the scope of some of the challenges.

This year, the DoD OIG added two new management challenges focused on the welfare and well-being of service members and their families and supply chain management and security. The FY 2019 Management Challenge "Implementing DoD Reform Initiatives" is no longer a standalone challenge, although the DoD OIG's oversight work continues to assess the effectiveness of DoD reform initiatives. Additionally, the DoD OIG revised the management challenge that traditionally addressed operational readiness to focus on the welfare and well-being of service members and their families.

The first new challenge, Management Challenge 3, "Ensuring the Welfare and Well-being of Service Members and Their Families," highlights the importance of taking care of the DoD's most important asset, its people. In July 2019, when he became the Secretary of Defense, Secretary Mark Esper stated during his welcoming ceremony:

> [A]s a personal priority of mine, we will place a particular focus on the well-being of our families. Our military spouses and civilians and children make tremendous sacrifices for this country [a]nd in return, I am committed to ensuring they are properly cared for. . . . They know that this administration, that this Congress and the American people have their back. And they know that when they are deployed far away from home, their families will be taken care of.

This management challenge discusses issues related to the quality and effectiveness of measures that affect the welfare and well-being of service members and their families, such as substance abuse programs, sexual assault prevention and response programs, suicide prevention programs, installations and housing, child care services, and spousal employment.

The second new challenge is Management Challenge 8, "Improving Supply Chain Management and Security." In today's global and integrated world, ensuring the security of the DoD's supply chain is critical to the DoD's mission. This management challenge examines the risks of diminishing supplies and reliance on sole-source suppliers, repairing existing parts economically and efficiently, identifying and prosecuting fraudulent parts suppliers, expanding limited distribution networks and transportation capabilities, improving asset visibility and property accountability, and maintaining cybersecurity in the supply chain.

ENDURING DOD MANAGEMENT CHALLENGES

Some challenges remain persistent, even as the DoD continues to address them.

Management Challenge 1, "Countering China, Russia, Iran, and North Korea," and Management Challenge 2, "Countering Global Terrorism," discuss the continued threats to the United States and to international and regional stability from these countries and terrorist groups. In this challenge, the DoD must maintain technological superiority and military readiness to deter military operations from U.S. adversaries; prevent increased development of nuclear weapons; counter support of terrorism; and combat cyber intrusions and technological theft from the U.S. Government, corporations, and allies.

Management Challenge 4, "Ensuring Ethical Conduct," discusses the need to maintain high ethical standards and ensure appropriate accountability for any misconduct. According to a June 2019 Gallup poll on confidence in institutions, the U.S. military remains the most highly trusted public institution, with more than 70 percent of Americans having a great deal of trust in the U.S. military, which is higher than any other U.S. institution. This management challenge focuses on trends in ethical misconduct and how investigations of senior officials, investigations of whistleblower reprisal and restriction, and

criminal investigations support the DoD's efforts to maintain the American public's trust and execute its mission.

Management Challenge 5, "Financial Management: Implementing Effective Correction Action Plans to Correct Identified Financial Management Weakness," another persistent challenge, focuses on the importance of accurate and comprehensive financial records. Last year, the DoD OIG completed and oversaw the first ever full scope financial statement audit of the DoD. While the DoD received a disclaimer of opinion the benefit of the audit was in the findings and deficiencies the audit identified. If corrected, these findings can help the DoD address longstanding financial management challenges that continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information to support reported financial statement balances. The lack of reliable financial information can adversely affect the DoD's operating, budgeting, and policy decisions.

Management Challenge 6, "Enhancing DoD Cyberspace Operations and Capabilities," highlights the threat to the DoD from cyber attacks that seek to collect intelligence, target DoD critical infrastructures, manipulate information, conduct cyber attacks, and disrupt or extort critical U.S. Defense contractors. To counter these threats, the DoD is conducting offensive and defensive cyber operations to protect its cyberspace networks and is attracting and retaining a skilled cyber workforce.

Management Challenge 7, "Enhancing Space-based Operations, Missile Detection and Response, and Nuclear Deterrence," is an increasingly important challenge. The DoD is heavily investing in space-based operations, ballistic missiles, and nuclear weapons to counter threats from adversaries. According to the 2019 Missile Defense Review, Russia, China, and North Korea are investing substantially in their missile capabilities, enhancing their ground and sea-launched missile arsenals with short, intermediate, and intercontinental-range systems, in addition to fielding mobile missiles to challenge the U.S. ability to detect their launch preparations. To ensure that the United States maintains its dominance in these areas and to protect itself and its allies, the DoD must modernize and replace these systems to meet current and future threats.

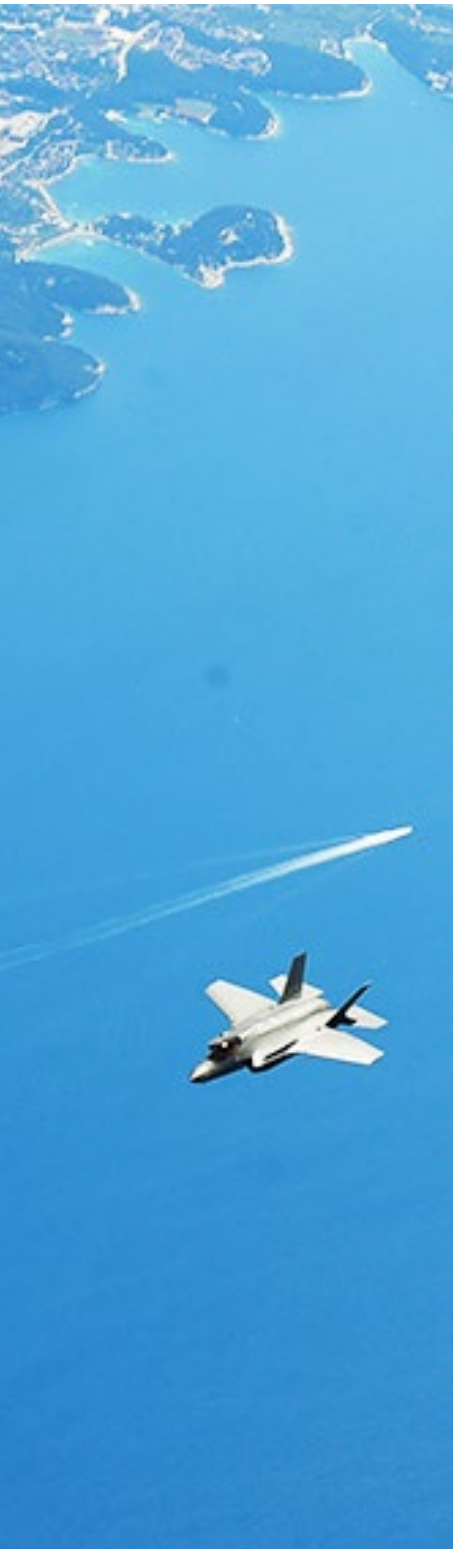
Management Challenge 9, "Acquisition and Contract Management: Ensuring That the DoD Gets What It Pays For On Time, at a Fair Price, and With the Right Capabilities," recognizes long-standing challenges in acquisition and contract management. Without clearly defined requirements, acquisitions of weapons systems that are regularly experiencing cost overruns and schedule delays may reduce the DoD's capabilities and readiness. The complexity of developing major systems, while also addressing cyber security challenges within the acquisition process and deterring contactor fraud in DoD acquisition programs, further compounds the challenge for the DoD. In addition, the DoD obligates hundreds of billions of dollars for goods and services each year, which if not managed properly, creates the potential for significant fraud, waste, and abuse.

Management Challenge 10, "Providing Comprehensive and Cost-Effective Health Care," discusses the challenges DoD faces in providing high-quality health care, at a reasonable cost, for 9.4 million beneficiaries, including service members, retirees, and eligible family members. Annual appropriations for Defense Health Programs have increased from $31.4 billion in FY 2015 to $33.3 billion in FY 2019, an increase of 6.1 percent. The DoD will also transfer the administration and control of military medical treatment facilities to the Defense Health Agency in FY 2020, as part of broader reform of the military healthcare system. This transition will create additional challenges, while the DoD seeks to reduce vulnerabilities and inefficiencies in the health care system, prevent health care fraud, and improve the integration of health records with the Department of Veterans affairs.

While there are other challenges facing the DoD, the DoD OIG considers these the top 10 challenges facing the DoD.

U.S. and Italian air force aircraft fly in formation over the Adriatic Sea during Exercise Astral Knight 19, June 4, 2019. (U.S. Air Force photo)

Challenge 1. Countering China, Russia, Iran, and North Korea



The National Security Strategy and National Defense Strategy identify major power competitors—China and Russia—as the top challenge for the DoD. The two strategies state that China and Russia seek to shape a world "antithetical to U.S. values and interests" and to expand their influence and power at the expense of the sovereignty of other countries. The strategies also characterize North Korea and Iran as rogue regimes that are destabilizing regions through their pursuit of nuclear weapons or the sponsorship of terrorism.

DoD leaders have regularly highlighted the threats to U.S. interests from these countries. For example, during an interview on August 21, 2019, Secretary of Defense Mark Esper said that China has engaged in the "greatest theft of intellectual property in human history" and is also expanding its military to "push the United States out of the [Indo-Pacific] theater." In his March 14, 2019, testimony before the Senate Armed Services Committee, former Chairman of the Joint Chiefs of Staff General Joseph Dunford stated that Russia uses "information, cyber, unconventional operations combined with economic and political influence to advance their interests while seeking to undermine the credibility of NATO."

Exacerbating the challenge to the DoD, China and Russia are aggressively modernizing their military forces. According to the Office of the Director of National Intelligence's (ODNI) 2019 Worldwide Threat Assessment, China seeks military advantage through a strategy of military-civil fusion; undermines international law and freedom of navigation in crucial waterways such as the South China Sea; and uses predatory economic statecraft to weaken its rivals, including the United States, to give China decisive strategic leverage over its neighbors. The Assessment also stated that China systematically steals science and technology from the U.S. Government, corporations, and allies.

Russia pursues its regional and global influence by using proxy forces to invade neighboring states, and employing cyberwarfare and other tactics to undermine other nations' political systems. Russia's conventional military capabilities threaten its neighbors, and Russia also uses information warfare to undermine and weaken NATO and the European Union.

In addition, Russia is modernizing its nuclear weapons, including improving its non-strategic nuclear weapons and developing a ground-launched cruise missile that violated the Intermediate-Range Nuclear Forces Treaty.[1]

North Korea also presents a dangerous threat to the United States and its allies. According to the Commission on the National Defense Strategy, North Korea may already be able to launch a nuclear weapon capable of reaching the United States. North Korea also uses an extensive campaign of cyber attacks to steal and launder money and cryptocurrency from international financial institutions, which it uses to fund its weapons development programs.

Recent developments in Iran have increased its threat to the United States and to the international community. In September 2019, according to intelligence experts, Iran was responsible for launching the drone and cruise missile attack on two Saudi oil facilities. Iranian forces have attacked or seized oil tankers traveling through or near the Strait of Hormuz. Iran continually supports terrorism in the Middle East, relies on proxy forces, and employs sophisticated cyberterrorism tactics to expand its malign influence in the region.

The DoD must ensure its readiness and capabilities to confront each of these diverse threats at the same time, which is a significant and continual challenge. The following sections of this management challenge discuss in more detail the threats from each of these countries and the challenge they present to the DoD.

CHINA

During a visit to Australia in August 2019, Secretary of Defense Esper stated that the United States will not "stand by idly while any one nation attempts to reshape the region to its favor at the expense of others, and we know our allies and partners will not either." He stated that China is "weaponizing the global commons using predatory economics and debt-for-sovereignty deals and promoting state-sponsored theft of other nations' intellectual property."

The Assistant Secretary of Defense for Indo-Pacific Security Affairs, Randall Schriver, similarly stated during a May 2019 Pentagon briefing that China continues to build up its military to challenge and supplant the United States as the preeminent power in the Indo-Pacific region. He said that China is investing money and time into capabilities and capacity by expanding and improving its missile forces; building its conventional ground, sea, and air forces; and improving technological capabilities of its military.

In March 2019, China's Ministry of Finance announced an annual military budget of 1.19 trillion yuan ($177.5 billion), a 7.5-percent increase from its 2018 budget of 1.11 trillion yuan ($167.4 billion).[2] According to the DoD 2019 Indo-Pacific Strategy report, China is investing in a broad range of military programs and weapons, including those designed to support expeditionary warfare; modernize its

[1] Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission, November 2018.

[2] According to the Center for Strategic and International Studies, how much China actually spends on its military is widely debated. The Stockholm International Peace Research Institute estimates the overall 2018 figure at $250 billion, and the International Institute for Strategic Studies puts the number at $209 billion in 2017. The DoD concludes that China's 2018 defense budget likely exceeded $200 billion.

nuclear forces; and conduct increasingly complex operations in domains such as cyberspace, space, and electronic warfare operations.

China is also developing a wide array of capabilities known as anti-access/area denial, which could be used to prevent the United States and other countries from operating in areas near China, including maritime and air domains that by international law are open to use by all countries.[3] For example, according to the Indo-Pacific Strategy report, China's goal in both the East and South China Seas is to push the U.S. Navy, and its carrier groups, out of striking range of mainland China. China's strategy seeks to dominate the South China Sea, through the buildup of its military bases in the Spratly Islands, and through harassing U.S. and allied ships and aircraft in the region.

China is also developing a variety of space capabilities designed to limit or prevent an adversary's use of space-based assets during a conflict. China is investing in research and development of satellite jammers and directed-energy weapons to blind or damage space-based optical sensors, such as those used for remote sensing or missile defense. China's potential use of weapons to blind or disable military communications, missile warning, and global positioning systems presents an extreme risk to the DoD's ability to command and control U.S. forces effectively, or at all, in the event of conflict.

China has made progress in its offensive space weapons, such as the anti-satellite missile system. China launched its first successful kinetic, physical anti-satellite weapon in 2007 when it destroyed an aging satellite in low-earth orbit. Since that time, according to the Center for Strategic and International Studies space threat assessment in 2019, China has conducted several "high-altitude direct-ascent anti-satellite tests that could reach satellites as high as geosynchronous orbit, which includes U.S. defense satellites used for missile warning; military communications; Global Positioning System; and Information Surveillance and Reconnaissance." Additionally, according to a January 2019 Defense Intelligence Agency report, China employs sophisticated satellite operations and is testing co-orbital satellite capabilities that serve as both on-orbit servicing and inspection satellites for peaceful purposes and as potential offensive space weapons capable of disabling or destroying the satellites of China's foes.[4] The DoD OIG is currently conducting an evaluation in this area to assess how U.S. Indo-Pacific Command has integrated space operations within its military deception plans to protect the United States and its allies against an adversary's space capabilities.

According to the Defense Intelligence Agency's January 2019 report on China's military power, the People's Liberation Army of China is positioned to use its cyberwarfare capabilities to support military operations in three key areas: (1) cyber reconnaissance, (2) cyber attack capabilities, and (3) cyberwarfare capabilities. According to a 2015 U.S.-China Economic and Security Review report, Chinese military writings and research efforts indicate that in a conflict China would attempt to conduct cyber attacks against U.S. satellites and ground stations.[5]

[3] DoD, "Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting A Networked Region," June 1, 2019.

[4] Defense Intelligence Agency, "China Military Power: Modernizing a Force to Fight and Win," January 2019.

[5] U.S.-China Economic and Security Review Commission, "2015 Report to Congress."

In addition, China has designed its research and development apparatus to identify and maximize the use of emerging science and technology for military use. For example, according to the DoD 2019 Annual Report to Congress on Military and Security Developments Involving the People's Republic of China, the Chinese 2017 National Artificial Intelligence Plan describes steps for China to become the "world's major artificial intelligence innovation center" by 2030 and calls for China to accelerate the integration of artificial intelligence with its economy, society, and national defense.

In its January 2019 report on China's military power, the Defense Intelligence Agency reported that the United States currently leads China in the development of military artificial intelligence, employing artificial intelligence in existing weapons systems such as the F-35 advanced jet fighter. However, China is increasingly competitive in artificial intelligence applications and its uses, including computer processing and secure communications. A recent article from the Center for a New American Security, "Beating the Americans at their Own Game," asserted that the "Chinese believe artificial intelligence, big data, human-machine hybrid intelligence, swarm intelligence, and automated decision-making, along with artificial intelligence-enabled autonomous unmanned systems and intelligent robotics, will be the central feature of the emerging economic and military-technical revolutions."[6]

CHINA'S THEFT OF INTELLECTUAL PROPERTY

In a recent CNBC poll, one in five corporations reported that China had stolen their intellectual property within the last year. Referring to China's theft of intellectual property, Secretary of Defense Esper recently stated, "It's a state-run organized effort to go after technologies, whether they are defense or non-defense technologies, to go up against other, all other types of intellectual property, even commercial goods." In an August 2019 Congressional Research Service report, the U.S. National Counterintelligence and Security Center described China as having "expansive efforts in place to acquire U.S. technology to include sensitive trade secrets and proprietary information," warning that if not addressed, the threat "could erode America's long-term competitive economic advantage."[7] According to the DoD Indo-Pacific Strategy Report, the theft of intellectual property puts at risk U.S. service members who rely on that technological advantage to accomplish their missions safely. It can also cost the United States billions of dollars to develop and field new defense technologies, only to have their effectiveness compromised by a data breach.

CHINA'S ASSERTIVE CLAIM TO THE SOUTH AND EAST CHINA SEAS

The South China Sea, with more than 200 islands, rocks, and low-tide elevations, is a gateway to global sea routes where approximately $3.4 trillion in trade passes annually. China continues to militarize the

[6] Center for a New American Security, "Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics," June 2019.

[7] Congressional Research Service, "U.S.-China Trade and Economic Relations: Overview," August 7, 2019.

South China Sea by placing anti-ship cruise missiles and long-range surface-to-air missiles on the disputed Spratly Islands. China has used its maritime militia to advance its disputed sovereignty claims throughout the South China Seas, as China takes possession of islands that are also claimed by other countries. China recently began conducting a series of anti-ship ballistic missile tests in the South China Sea. Figure 1 shows the general location of the disputed areas in the South China Sea.

Figure 1. South China Sea

Source: Congressional Research Service.

China's attempted control over disputed areas is not limited to the South China Sea. According to the 2019 DoD Indo-Pacific Strategy Report, near the Japan-administered Senkaku Islands in the East China Sea, Chinese patrols with maritime law enforcement ships and aircraft endanger the free flow of trade, threaten the sovereignty of other nations, and undermine regional stability. The DoD is seeking to maintain sufficient naval forces in the region to guarantee the free flow of maritime shipping. In the past year, U.S. Navy and allied warships increased the number of freedom of navigation operations in international waters to challenge China's territorial claims.

China is building other military bases to project its military presence around the world. For example, in July 2019 China signed an agreement with Cambodia allowing the Chinese armed forces to use a Cambodian navy base near Sihanoukville. The agreement gives China exclusive rights to part of a Cambodian naval installation on the Gulf of Thailand, not far from a large airport now under construction by a Chinese company. The Ream Naval Base covers approximately 190 acres and includes two facilities built with U.S. funding and used by the Cambodian navy. Military operations from the naval base, the airport, or both, would sharply increase Beijing's capacity to enforce territorial claims and economic interests in the South China Sea, to threaten U.S. allies in Southeast Asia, and to extend its influence over the strategically important Malacca Strait.

The continued modernization of the People's Liberation Army also strengthens China's ability to operate farther from its borders. For example, according to the Indo-Pacific Strategy Report, the People's Liberation Army is reorganizing with the objective of improving its capability to conduct complex operations and improving its command and control, training, personnel, and logistics systems.

RARE EARTH ELEMENTS IMPACTING THE DOD

Defense and technology applications rely heavily on base rare earth metals or other post-oxide materials. Rare earth elements are a group of 17 chemical elements used in critical military applications such as high-powered lasers, "smart" munitions, and directed-energy weapons, as well as in consumer products, ranging from iPhones to electric car motors.

Most rare earth metals, alloys, and other post-oxide materials are refined in China, which has 37 percent of the global rare earth reserves.

Most U.S. and NATO technologies and weapon systems depend on rare-earth metals. China could limit export of rare metals to the United States, an action it had already taken against Japan. Between 2004 and 2017, China accounted for 80 percent of U.S. rare earth imports. Few alternative suppliers have been able to compete with China. While China has not restricted rare earth sales to the United States, articles in the Chinese media have implied this will happen.

In sum, Secretary of Defense Esper recently told reporters that China is the number one priority for the DoD, that China is clearly professionalizing and expanding the capabilities of its military, and that China's theft of intellectual property is a significant problem. Because of the threat that China poses in the Indo-Pacifica region, the DoD must maintain sufficient forces in the region to guarantee the free flow of maritime trade, as well as to support freedom of navigation operations in both the East and South China Sea. The DoD must also maintain technological superiority in emerging areas of artificial intelligence, cyberspace, and space to detect, defend, and counter potential Chinese aggression in these area. To deter the theft of military intellectual property attributed to Chinese entities, the DoD must continue to improve its cybersecurity and must work with U.S. and international partners to counter Chinese theft and aggression.

RUSSIA

In March 2019 written testimony before the Senate Armed Services Committee, Secretary Esper and the Chairman of the Joint Chiefs of Staff and former Army Chief of Staff, General Mark Milley, stated, "Russia is likely to threaten our interests for the next 20 years, as they attempt to regain control of historic spheres of influence." In order to meet its goals, Russia invests in strategic weapons systems as a key element of its national security strategy, combined with selective upgrades to conventional forces. Russia also continues its aggression against its neighbors in Europe, including Ukraine and Georgia. It conducts activities around the world short of armed conflict, such as cyber attacks and social media misinformation campaigns, to sow discord in various countries.

In its latest national security strategy, Russia declared that it plans to increase its Gross Domestic Product to one of the world's largest in the coming years to maintain its status and prestige as one of the world's great powers. Despite its size and these aspirations, Russia is in 11th place in the World Bank's 2018 database of Gross Domestic Product rankings by nation. Its economy remains pressured by international economic sanctions, net outflows of capital, lack of foreign investment, and low energy prices. These economic challenges limit the resources it can apply to military modernization. The most recent Russian defense budget, in 2018, was less than one-tenth of the 2019 U.S. military budget, and was far surpassed by the 29 NATO members' $963 billion combined military expenditure.

RUSSIA MODERNIZES ITS NUCLEAR ARSENAL

Despite its economic challenges, Russia is devoting resources to modernizing its nuclear weapons and strategic capabilities. In May 2019 remarks at the Hudson Institute, the Director of the Defense Intelligence Agency stated that Russia's inventory of nuclear warheads will most likely "grow significantly" in the coming decade and that Russia views such weapons as

its "guarantor" of survival in an era of renewed great power competition. According to the Defense Intelligence Agency, Russia has the capability to conduct a massive nuclear strike on the United States within minutes, and Russia has not ruled out a nuclear first-use strike against U.S. allies. In the DoD's 2018 Nuclear Posture Review, the DoD stated that it must be able to deter Russia from a nuclear attack of any scale by making certain Russia understands its use of nuclear weapons will come at "incalculable and intolerable" cost.

In December 2018, Russia tested the hypersonic *Avangard* intercontinental missile. Hypersonic glide vehicles such as *Avangard* challenge U.S. missile defense capabilities because they are maneuvering vehicles that glide at velocities typically greater than Mach 5. Such unprecedented speed, at altitudes lower than a ballistic missile, makes intercept exceedingly difficult because the incoming warhead may not be detected until very late in its flight.

RUSSIA VIOLATED THE INTERMEDIATE-RANGE NUCLEAR FORCES TREATY

Russia is also the only country other than the United States with an operational strategic nuclear weapons delivery triad of land-based missiles, bombers, and submarine-launched missiles. Russia's continued deployment of ground-launched, nuclear-capable cruise missiles violated the 1987 Intermediate-Range Nuclear Forces Treaty and led the United States to withdraw from the agreement in August 2019. This longstanding treaty obligated the United States and Russia "not to possess, produce, or flight-test a ground-launched cruise missile with a range capability of 500 kilometers to 5,500 kilometers." According to NATO Secretary-General Jens Stoltenberg, the Russian missiles, which can be fired from mobile systems against targets virtually anywhere in Western Europe, put European security at risk. He said, "There are no new U.S. missiles in Europe, but there are new Russian missiles in Europe."

Additionally, according to U.S. officials, the collapse of the Intermediate-Range Nuclear Forces Treaty could impede U.S. and Russian negotiations to extend the New Strategic Arms Reduction Treaty, which limits offensive nuclear weapons, beyond its February 5, 2021, expiration.

Without an extension, the New Strategic Arms Reduction Treaty's expiration would end all restrictions on the deployment of offensive nuclear weapons, potentially instigating a costly and dangerous nuclear arms race.

RUSSIA DEMONSTRATES CAPABILITIES IN THE "GRAY ZONE" BETWEEN WAR AND PEACE

In addition to modernizing its strategic and conventional forces, Russia engages in a wide range of activities in the "gray zone" of coercion and manipulation—including cyber operations, social media disinformation campaigns aimed at civilian populations, and deployment of proxy-force mercenaries—to pursue its goals while keeping its overall defense costs in check. According to a 2019 RAND Corporation report, gray zone tactics fall below the threshold of conventional war and typically are not directly attributable, thereby offering Russia plausible deniability.

The Department of Homeland Security and the Federal Bureau of Investigation have reported that cyberwarfare agents of the Russian government are targeting U.S. Government entities and critical infrastructure sectors such as air traffic control networks, energy distribution nodes, commercial facilities,

and water and electrical utility systems. For example, a cyberinfrastructure alert released last year by the Department of Homeland Security and the Federal Bureau of Investigation describes how Russian agents created fake network administrator accounts, accessed Virtual Private Network connections, used innocuous e-mail attachments to "spear-phish," and compromised websites to display malicious or misleading content.

The damage from such actions can be significant. The DoD OIG issued a July 2019 audit report identifying 248 security incidents reported to the DoD Cyber Crime Center, including unauthorized access to contractors' networks, data exfiltration, and the exploitation of network and system vulnerabilities. Although the cyber attacks against the DoD were not attributed to Russia in the report, the DoD OIG noted, "Malicious actors can exploit vulnerabilities and steal information related to some of the nation's most valuable advanced defense technologies."[8]

In addition to conducting cyber warfare and malign social media campaigns, Russia deploys contract mercenaries to other countries, such as Syria, Ukraine, Central African Republic, Sudan, Libya, and Venezuela, to conduct military operations. By using skilled paramilitary troops supplied with Russian weapons and equipment but wearing uniforms without identifying insignia, Russia denies official involvement.

RUSSIAN AGGRESSION IN UKRAINE

Asked which one place in the world could potentially become the focal point for a conflict between the United States and Russia, Secretary of Defense Esper identified the eastern flank of NATO and Ukraine, which is on the Black Sea and bordered by four NATO members, as the "seam between Russia and our alliance partners." Ukraine has fought Russian-backed pro-separatist rebels since 2014 in a conflict that has resulted in more than 10,000 deaths. In November 2018, Russian forces intercepted then rammed and opened fire on two small Ukrainian patrol boats and a tugboat transiting between Ukrainian Black Sea ports via the narrow Kerch Strait—the sole entrance to the Sea of Azov that separates Ukraine from Russia to the east. In what Ukraine characterized as an "act of aggression" and a flagrant violation of international law, Russian special forces boarded the three Ukrainian vessels, injuring several sailors and seizing both the vessels and their crews.

According to the National Defense Authorization Act for FY 2019, the United States is pursuing a "strategy backed by all elements of United States national power to deter, and if necessary, defeat Russian aggression." A key aspect of this strategy is to modernize the U.S. nuclear arsenal. According to the 2018 Nuclear Posture Review, the DoD plans to invest approximately 6.4 percent of its base budget to sustain and modernize its nuclear triad; nuclear command, control, and communications systems; and the nuclear enterprise infrastructure. Other U.S. systems under development to support the triad include the B-21 nuclear-capable stealth bomber, the *Columbia*-class ballistic missile submarine, and a ground-based strategic deterrent system to replace the aging Minuteman III intercontinental ballistic missile.

Many of the U.S. bombers and refueling aircraft currently in use, such as B-52s and KC-135s, were placed in service decades ago and are older than their crews. Aircraft readiness—the percentage of aircraft able to fly and perform their mission at any given time—

[8] Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on ContractorOwned Networks and Systems," July 25, 2019.

continues a downward trend dating back to at least 2012. In May 2019, the DoD OIG initiated an evaluation to determine whether the Air Force has the mission capable KC-135 aerial refueling aircraft, associated aircrews, and required installation support necessary to meet U.S. Strategic Command's nuclear mission readiness requirements.

Gray zone operations, including cyberwar, also require the DoD to view the challenge from Russia not just through a lens of either war or peace, but as a long-term rivalry, which can fall short of overt use of armed force. According to the DoD's cyber strategy, the DoD "must take action in cyberspace during day-to-day competition to defend U.S. interests" and focus on great power competitors that "pose strategic threats to U.S. prosperity and security, particularly China and Russia." Speaking in August 2018 to the Intelligence and National Security Alliance, General Paul Nakasone, the Commander of U.S. Cyber Command, stated, "We've got to act forward outside of our boundaries, something that we do very, very well at Cyber Command in terms of getting into our adversary's networks. That's this idea of persistent engagement—the idea that the adversary never rests, so why would we ever rest."

In sum, despite a weak economy, Russia is modernizing its military, especially its strategic nuclear forces. Russia also uses gray zone tactics short of traditional armed force, such as cyber attacks, mercenaries, and coordinated social media misinformation campaigns to intimidate its neighbors and undermine other countries. The challenge facing the DoD is to deter Russia from using nuclear weapons, while protecting U.S. and NATO forces from recently deployed Russian ground-launched intermediate range missiles. The DoD must defend U.S. critical infrastructure, including non-DoD-owned networks and systems, from Russian cyber activity. Additionally, the DoD must respond, along with international allies and partners, to deter and counter destabilizing Russian malicious gray zone activities throughout the world.

IRAN

Iran threatens the security and stability in the Middle East and Southwest Asia because of its regional destabilizing activities, advancement of nuclear weapon and advanced missile capabilities, and support of the militant Shia terrorist organization Hezbollah in Syria and Lebanon. According to General Dunford, Iran's widespread malign activity poses a "campaign-like" threat that continues to challenge U.S. security interests.

IRAN AND IRANIAN-BACKED GROUPS THREATEN THE CENTRAL REGION

The Department of State's 2018 annual survey of global terrorism reported that Iran is the world's most active state sponsor of terrorism through its funding of terrorist networks and operation cells established throughout the world. In April 2019, the U.S. Government designated Iran's Revolutionary Guard Corps (IRGC) as a Foreign Terrorist Organization. Iran's extraterritorial unit, the Quds Force, was also designated as a Foreign Terrorist Organization because it directly supports and guides terrorist organizations such as the Lebanese Hezbollah, the Taliban, and various Shia Iraqi militias. The Quds Force has 200,000 members who are trained, armed, and motivated to target U.S forces stationed throughout the Middle East.

U.S. Secretary of State Mike Pompeo stated that Iran has ties to al Qaeda, and according to the ODNI, Iran's support to the Houthi

rebels undermines U.S. interests and the counterterrorism efforts of Saudi Arabia and the United Arab Emirates in Yemen.

IRAN'S ACTIONS THREATEN U.S. OPERATIONS IN THE PERSIAN GULF

The ONDI's 2019 Worldwide Threat Assessment noted that Iran's strategic position atop the Strait of Hormuz gives it the capability to interfere with regional commerce and transit. According to the International Crisis Group Organization, the Strait of Hormuz, which lies between the Persian Gulf and the Gulf of Oman, is the world's most important oil trade chokepoint. About 20 percent of the world's oil flows through the Strait, which makes it vital to the national and economic interests of many nations around the world. The Strait is regulated by the 1982 United Nations Convention on the Law of the Sea; however, Iran has not ratified the convention. In 2018, the United States imposed sanctions on Iran to deter countries from importing Iranian oil. In response, Iran threatened to block all oil exports through the Strait.

Since May 2019, six oil tankers traveling through or near the Strait have been attacked. On May 12, 2019, four oil tankers were sabotaged off the United Arab Emirates coast of Fujairah. On June 13, 2019, two commercial vessels, one Japanese and the other Norwegian, were attacked. Iran denied any involvement in the attacks, but U.S. Secretary of State Pompeo stated that Iran was responsible for the attacks. Analysts at the Eurasia Group also stated that the attacks were part of a systematic Iranian effort to demonstrate that peace in the Gulf is contingent on Iran's economic stability. In that effort, Iran's Navy has seized or harassed oil tankers passing through the Strait.

For several years, the Iranian Navy and the IRGC have harassed U.S. warships operating in the Strait. The U.S. Navy classified approximately 10 percent of these interactions as "unprofessional or unsafe." For example, in August 2017 an unarmed Iranian drone without any aircraft navigation lights came within 1,000 feet of the USS Nimitz as the aircraft carrier conducted night flight operations. On June 20, 2019, Iran shot down a U.S. unmanned aerial vehicle over the Strait. Iran contended that the drone violated its territorial airspace, although the United States stated that the shooting was an "unprovoked attack" in international airspace.

Iran continues to improve its military capabilities, such as submarines, armed unmanned aerial vehicles, advanced naval mines, unmanned explosive boats, advanced torpedoes, and anti-ship and land-attack cruise missiles.

POTENTIAL THREATS RELATED TO IRANIAN MINES

According to Admiral (Ret) James Stavridis, the former supreme allied commander of NATO, Iran will likely increase its aggression toward merchant shipping by placing mines in the Strait of Hormuz. The U.S. minesweeping fleet is the primary tool for finding and neutralizing mines. Clearing mines from the Persian Gulf requires multiple naval ships that are fully mission-capable. However, according to Naval personnel, the U.S. minesweeping ships are old and in a frequent state of disrepair, and there is a shortage of spare parts to maintain the aging minesweepers. The DoD needs to ensure its minesweeping technology and the Navy's minesweeping fleet is maintained, updated, and prepared to mitigate the threat to shipping.

IRAN'S BALLISTIC MISSILE PROGRAM AND DEVELOPMENT OF CHEMICAL WEAPONS THREATEN THE REGION

Iran has the largest inventory of short- to intermediate-range ballistic missiles in the Middle East, which threatens U.S. and allied personnel and their bases. Iran has also developed, tested, and produced an intercontinental ballistic missile. Additionally, according to the ODNI's 2019 Worldwide Threat Assessment, Iran is non-compliant with its obligations under the Chemical Weapons Convention, and Iran is developing chemical agents intended for incapacitation and offensive military purposes.

IRAN IS BUILDING ITS CYBERWARFARE CAPACITY

In the 2019 Worldwide Threat Assessment, the ODNI stated that Iran has sophisticated cyber techniques and capabilities for conducting espionage. For example, Iran has used social media platforms to target the United States and its allies by collecting intelligence and gaining access to associated accounts and networks. In February 2019, a former U.S. counterintelligence agent assisted Iranian intelligence services by using fictional and imposter social media accounts to deploy malware that would provide the IRGC access to the networks of her former fellow agents. Iran has also conducted data deletion attacks against dozens of Saudi government and privatesector networks. According to a Center for Strategic and International Studies article on Iran and cyber power, Iran has created a sophisticated organization connected to the Iranian government to wage cyber conflict.

The 2019 Worldwide Threat Assessment discussed Iran's desire to penetrate U.S. and allied partner networks to attack critical infrastructure. Speaking at the 2019 Aspen Security Forum, Microsoft's senior vice president of customer security and trust stated, "Cyber activity originating in Iran and targeting entities across the United States spiked" after the United States announced its withdrawal from the nuclear deal with Iran (the 2015 Joint Comprehensive Plan of Action) in May 2018. Iran has also targeted U.S. Government officials, organizations, and companies to gain intelligence information and position themselves for future cyber disruptions. The 2019 Worldwide Threat Assessment stated that Iran is capable of causing localized disruptive effects, such as disturbing the corporate networks of large companies for days or weeks.

THE UNITED STATES' ACTIONS TO DETER IRANIAN THREATS

After the United States withdrew from the Joint Comprehensive Plan of Action in 2018, former Secretary of Defense James Mattis testified to the Senate Appropriations defense subcommittee that the United States needed to confront Iran not only because of its nuclear program, but also because of its development of ballistic missiles, support of terrorism, cyber attacks, and threats to international commerce.

In 2019, the United States re-imposed economic sanctions that it had lifted under the agreement. The sanctions target Iranian purchases of U.S. dollars, metals trading, coal, industrial software, and the Iranian auto sector.

Beyond economic sanctions, the DoD has increased its troop presence in the Middle East to counter the Iranian threat. In a May 2019 briefing, Vice Admiral Michael Gilday, the Commander of the U.S. 5th Fleet, stated, "[W]e have multiple credible reports that Iranian proxy groups intend to attack U.S. personnel in the Middle East." In response to the reports, the DoD sent 1500 troops, along with drones and fighter jets, to the Middle East.

In sum, Iran continues to be the world's foremost state sponsor of terrorism. Iran has used support for insurgent groups, cyber warfare, and control of the Strait of Hormuz to expand its influence across the Middle East. Iran's aggressive behavior in the Strait of Hormuz threatens freedom of navigation, international shipping, U.S. military facilities, and critical infrastructure in the Persian Gulf. Iran also continues to improve its ballistic missile program and develop more sophisticated cyber techniques to threaten the United States and global partners.

NORTH KOREA

North Korea's pursuit of ballistic missile and nuclear weapons technology continues to threaten the United States and its allies. With advances in weapons capabilities, North Korea has evolved from a threat to U.S. interests in East Asia to a potentially direct threat to the U.S. homeland. In his 2019 command posture statement, U.S. Indo-Pacific Command Commander Admiral Philip Davidson stated that North Korea will remain the most immediate challenge in the Indo-Pacific until its final, fully verifiable denuclearization is achieved.

NORTH KOREAN INTERNATIONAL THREAT

North Korea has adopted a national security strategy based on the development of weapons of mass destruction. North Korea continues to build its ballistic missile capabilities and nuclear weapons program, despite publicly declaring at times its support for the denuclearization of the Korean Peninsula. According to the Arms Control Association, as of June 2019, North Korea was estimated to have 20 to 30 nuclear warheads and is actively expanding its ballistic missile arsenal, including the development of intercontinental ballistic missiles.

After a moratorium of nearly 18 months, North Korea resumed its short-range ballistic missile testing in 2019, including two launches in May, one in July, and six during August. Statements from North Korea's Ministry of Foreign Affairs claim that North Korea's actions have been in response to "hostile military moves" against it by the United States and South Korea.[9] North Korean officials cited the August 2019 joint exercise between U.S. and South Korean troops and South Korea's procurement of F-35A fighter jets to justify the surge in missile tests. North Korean officials also regularly denounce the alliance between the United States and South Korea, stating that North Korea has "no other choice but to develop and test the special armaments to completely destroy the lethal weapons reinforced in [S]outh Korea."[10]

According to U.S. Indo-Pacific Command and the Department of State, North Korea continues to evade international sanctions and generate illicit revenue through activities such as cross-border smuggling operations and exploitative overseas labor contracts with foreign governments, mainly China and Russia.[11] Adding to this concern is North Korea's history of distributing conventional arms, nuclear technology, and chemical agents to other counties, such as Iran and Syria.

Cyber activities remain a key means for North Korea to earn foreign currency. North Korea has used cyber attacks to steal and launder money from financial institutions and cryptocurrency exchanges across many

---

9 Ministry of Foreign Affairs, Democratic People's Republic of Korea, "Spokesperson for Ministry of Foreign Affairs of DPRK Issues Press Statement," August 6, 2019.

10 Ministry of Foreign Affairs, Democratic People's Republic of Korea, "S. Korean Authorities Slammed," July 11, 2019.

11 U.S. Indo-Pacific Command Posture; Department of State, "2019 Trafficking in Persons Report," June 20, 2019.

countries. According to the United Nations, these attacks generated an estimated $2 billion in illicit revenue for North Korea, helping to fund the country's nuclear and ballistic missile programs.

U.S. RESPONSES TO NORTH KOREAN THREATS

The 2017 National Security Strategy and the 2018 National Defense Strategy stated that the United States will focus on the deployment of a layered missile defense system to defend the U.S. homeland against the North Korean ballistic missile threat. In FY 2018, Congress passed the Missile Defeat and Defense Enhancements Act as an "emergency requirement" for the DoD to counter the increased threat from North Korea. Under the Act, the Missile Defense Agency was tasked with improving ballistic missile defense capabilities against North Korea, including the expansion of the U.S.-based missile interceptor network and increased capability for the Terminal High Altitude Area Defense battery deployed to South Korea, which contributes to the layered missile defense system on the Korean Peninsula.

In sum, North Korea remains a persistent and dangerous U.S. foreign policy and military challenge. The North Korean government has used regional military exercises between the United States and South Korea as justification for its continued ballistic missile testing, much of which is funded through illicit international cyber-theft activities. North Korea also continues to build its nuclear weapons capability, despite repeated efforts by the international community to push for denuclearization. North Korea's actions heighten the need for improved missile defense capabilities for the continental United States, as well as to protect U.S. interests on the Korean Peninsula and within the Indo-Pacific region.

CONCLUSION

In summary, the United States and the DoD face formidable challenges in countering the formidable threats from China, Russia, Iran, and North Korea. Each nation presents the DoD with challenges ranging from emerging nuclear capabilities, cyber attacks, and conventional military capabilities. Each is modernizing its weapons systems and pursuing various technological advances. The DoD must maintain technological superiority and military readiness to deter these threats, to prevent increased development of nuclear weapons, to counter support of terrorism, and to combat cyber attacks and theft of technology and intellectual property from the United States and its allies.

A U.S. Marine Corps crew chief with Marine Medium Tiltrotor Squadron (VMM) 364 mans an M240-D machine gun on an MV-22 Osprey during a tactical recovery of aircraft and personnel exercise September 8, 2019. A Marine Air Ground Task Force is specifically designed to be capable of deploying aviation, ground, and logistics forces forward at a moment's notice. (U.S. Marine Corps photo)

Challenge 2. Countering Global Terrorism

According to the U.S. National Security Strategy, terrorism, particularly violent attacks by al Qaeda, the Islamic State in Iraq and Syria (ISIS), and other violent extremist groups, remains a persistent worldwide threat. According to the Intelligence Community's 2019 Worldwide Threat Assessment, violent extremist organizations in the Middle East, Africa, South Asia, and East Asia continue to create regional instability and, in many cases, seek to threaten the U.S. homeland. The threat assessment stated that while violent extremist organizations such as al Qaeda and ISIS have experienced significant setbacks in recent years, they are rebuilding their operational capabilities.

The DoD seeks to deter, disrupt, and defeat these violent extremist threats through a variety of counterterrorism activities, ranging from direct military operations against the enemy to long-term security cooperation and other support to partner forces as they conduct counterterrorism operations and build their counterterrorism capability. These activities, which address a diverse range of violent extremist organizations in often-austere locations, involve several significant challenges for the DoD.

First, while the DoD recognizes the continued threat posed by violent extremists, it has begun to shift its focus more toward other threats in alignment with the National Defense Strategy. Former Chairman of the Joint Chiefs of Staff General Joseph Dunford said in August 2019 that the DoD has shifted to plans that are globally oriented on each of the five primary challenges addressed in the National Defense Strategy—China, Russia, Iran, North Korea and violent extremism. As noted in Management Challenge 1, according to Secretary Esper, strategic competitors such as China and Russia are deliberately building up and modernizing their military forces to challenge the United States and enable their geopolitical aspirations. At the same time, regional adversaries such as Iran and North Korea continue to promote instability.

However, the threat from violent extremists remains, and the DoD is faced with the difficult task of addressing all of these strategic challenges at the same time.

Second, when the DoD conducts direct operations against violent extremist organizations, it must coordinate with and work with partner forces, which can present cultural, political, and practical challenges. Working with host country forces also adds additional risk of insider attacks, as seen in Afghanistan.

Third, as the DoD trains and equips partner forces to build their counterterrorism capacity, the DoD must track equipment and weapons it provides to ensure they are not diverted to unintended use. The DoD must also monitor contractors in their execution of supporting efforts and ensure the progress of its partner forces.

Fourth, the DoD must coordinate with other Federal agencies, such as the U.S. Agency for International Development and the Department of State, as well as with foreign governments, as they help rebuild essential infrastructure and government institutions.

Finally, in many counterterrorism areas of operation, the DoD must contend with the influence of external adversaries, such as Iran, Russia and China, who may seek to enable or support violent extremist organizations and undermine the DoD's actions.

The following sections discuss each of these challenges in more detail and DoD initiatives to seek to address the challenges.

CURRENT COUNTERTERRORISM ACTIVITIES

The DoD's counterterrorism activities range from high-profile efforts to combat ISIS to small, bilateral security cooperation programs to promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and to provide U.S. forces with peacetime and contingency access, which receive more limited public attention.

The areas of the world with the greatest violent extremist threats where the DoD is operating include the following countries and regions of the world.

Iraq and Syria. Since 2014 when ISIS seized territory and proclaimed a "caliphate," the United States and international partners in the Global Coalition to Defeat ISIS have fought to degrade, dismantle, and ultimately defeat ISIS in Iraq and Syria. Under Operation Inherent Resolve, the United States and its Coalition partners liberated territory in Iraq and Syria previously under ISIS control. However, ISIS is now conducting a clandestine insurgency in those countries, and it retains the capability to conduct attacks, including ambushes, use of improvised explosive devices, and targeted assassinations.

Afghanistan. Under Operation Freedom's Sentinel, U.S. forces and North Atlantic Treaty Organization partners train, advise, and assist the Afghan security forces and ministries to build their institutional capacity. U.S. forces also conduct counterterrorism operations against al Qaeda, ISIS-Khorasan, and other terrorist groups in Afghanistan. In its July 2019 semiannual report to Congress on operations in Afghanistan, the DoD stated that even if ongoing diplomatic talks with Taliban militants produce a successful political settlement, al Qaeda, ISIS-Khorasan, and Taliban hardliners will remain a substantial threat to the Afghan government and its citizens, as well as to the United States.[12]

[12] DoD, "Enhancing Security and Stability in Afghanistan," July 2019.

Yemen. In coordination with the government of Yemen, U.S. forces support counterterrorism operations against al Qaeda and ISIS affiliates to disrupt and destroy militants' attack-plotting efforts, networks, and freedom of maneuver within the region. The U.S. intelligence and defense communities have assessed al Qaeda in the Arabian Peninsula as one of the terrorist groups most committed to and capable of conducting attacks in the United States.

Africa. Al Qaeda affiliates in Africa, including Boko Haram and al Shabaab, have maintained a high pace of terrorist operations and expanded their activities into new countries such as Ghana, Benin, Togo, the Ivory Coast, Mauritania, and Mali. ISIS also has newly established affiliates in Nigeria, Somalia, and other parts of Africa. According to the United Nations Secretary-General, the Islamist insurgency in the Sahel region (a vast semiarid region of North Africa, to the south of the Sahara Desert) shows no signs of weakening, and armed groups have continued to displace millions of people.

East Asia. Under Operation Pacific Eagle–Philippines, U.S. forces support the Philippines in its efforts to counter ISIS affiliates and other violent extremist organizations in the country's southern regions. The DoD provides the Armed Forces of the Philippines with intelligence, surveillance, and reconnaissance support and conducts advise and assist operations, such as supporting mission planning. In other East Asian countries, including Indonesia and Thailand, the DoD also works with local forces to counter criminal and extremist organizations in the region.

OPTIMIZING COUNTERTERRORISM RESOURCES

A key challenge for the DoD is deciding how to deploy its resources to address the full range of global threats. As the DoD shifts to focus more on threats from China and Russia, the DoD must continually review and prioritize how to deploy limited resources—including personnel, equipment, and intelligence capacity—to counterterrorism activities around the world. In addition, long-term planning for counterterrorism operations is difficult because these operations have timelines that normally span leadership changes, annual appropriations cycles, and annual authorizing legislative processes.

The effect of the recent focus on great power competition is evident in Syria, where the reduction of U.S. forces since the beginning of 2019 has decreased the support available to provide training and equipment for Syrian partner forces which are the key to preventing ISIS resurgence. In addition, the Department of State reported that the ordered departure of non-emergency personnel from the U.S. Embassy in Baghdad and the U.S. Consulate in Erbil eroded the ability of the U.S. Government to execute stabilization activities in Iraq.

Resource constraints are also a challenge for the smaller counterterrorism operations in Africa and East Asia. U.S. Africa Command is in the first phase of a plan to streamline, or "right-size," and refocus priorities for countering terrorism in Africa. The plan reduces special operations and conventional troop presence by about 10 percent, with additional reductions possible. Because the violent extremist threat in Africa is geographically dispersed, and infrastructure is much less developed than in Europe and Asia, the DoD needs to prioritize its activities on the continent, but

also be able to respond rapidly to changing threats and requirements on the ground, and rely more on local partner forces to achieve counterterrorism objectives.

A recent DoD Office of Inspector General (OIG) report addressed counterterrorism challenges in the Philippines, the site of smaller U.S. counterterrorism operations. The January 2019 DoD OIG evaluation report found that while the advice and assistance of U.S. forces helped the Armed Forces of the Philippines counter violent extremists in the city of Marawi, the U.S. forces did not provide counterterrorism training to the conventional forces of the Armed Forces of the Philippines, as directed in the Execute Order.[13] In addition, counterterrorism operations in the Philippines rely heavily on intelligence, surveillance, and reconnaissance assets, which are in high demand to support counterterrorism and other operations, deployments, and missions around the world.

While U.S. counterterrorism operations differ, they draw from a finite inventory of financial, equipment, and personnel resources that also support other DoD activities. The DoD shift of resources to address other threats affects counterterrorism operations, and the DoD is seeking to adjust. In some cases, conventional forces, remote advising, or the provision of new systems and equipment may reduce the need for special operations forces in a direct role, and operational responsibility may be shifted more to local forces and other international partners. However, the strategic shift of priority from countering violent extremists may also require the DoD to reduce some of its activities and programs designed to build counterterrorism capacity among partner forces.

EXECUTING DECISIVE OPERATIONS

DoD operations to capture and kill terrorists, liberate captured territory, and support local forces require the DoD to coordinate closely with ally and partner forces and also to address risks to U.S. personnel on the ground.

The DoD has executed successful operations against violent extremists in recent years. In Iraq and Syria, the DoD, working with Iraqi Security Forces, Vetted Syrian Opposition forces, and the Coalition, eventually liberated major cities, such as Mosul and Raqqa, and removed ISIS from the territory in Iraq and Northeast Syria it had seized. In 2017, U.S. special operations forces assisted their Philippine counterparts in expelling ISIS-East Asia fighters from Marawi, the largest city on Mindanao, the island where ISIS-East Asia is most active. In Afghanistan and elsewhere, U.S. counterterrorism forces and their partners have targeted and killed key leaders of violent extremist groups, gathered intelligence to better understand individuals and activities, and disrupted extremist networks, funding, and weapons shipments.

As the global terrorist threat continues to evolve and expand geographically, the DoD will likely rely more on local and international partner forces to execute operations. Security cooperation activities seek to build partner capacity and interoperability with U.S. forces, and in many places, such as Iraq and Afghanistan, the DoD is training, advising, and equipping local conventional and special operations forces. In Afghanistan, the North Atlantic Treaty Organization-trained Afghan Special Security Forces have demonstrated increasing capacity

[13] Report No. DODIG-2019-048 "DoD Efforts to Train, Advise, Assist, and Equip the Armed Forces of the Republic of the Philippines," January 31, 2019.

to conduct operations against ISIS-Khorasan. The longstanding DoD partnership with the Iraqi Counter Terrorism Service has resulted in an increased counterterrorism capacity in Iraq. However, because these special forces are more capable than most conventional forces, they are often misused or overused to conduct conventional operations, which stresses their capacity and undermines their ability to address terrorist threats.

In many places, including Iraq, Syria, and Afghanistan, the DoD works with international partners to conduct counterterrorism operations. However, some Coalition partners have placed restrictions on their participation in the shared missions. For example, some members of the Global Coalition to Defeat ISIS restricted their involvement in Syria because of the risk to their forces and their potential involvement in the ongoing Syrian civil war.

The geographic dispersion of counterterrorism activities and partnerships with foreign forces present other challenges. In Afghanistan, "green on blue" attacks—attacks in which a member of the Afghan security forces attacks a Coalition military advisor—have decreased in recent years, but remain a persistent threat. For example, in October 2018, an Afghan politician's guard opened fire in a meeting in which General Austin Miller, Commander of U.S. Forces-Afghanistan, was present. The attack injured two U.S. personnel and killed a key senior Afghan ally. U.S. forces suspended advisory efforts across Afghanistan until Afghan forces had taken steps to improve screening of personnel who work with international forces. However, this threat persists. In June 2019, an Afghan soldier killed two U.S. soldiers in southern Afghanistan. The DoD OIG is currently conducting an evaluation of how U.S. Forces-Afghanistan screens Afghan personnel who interact with U.S. military personnel in Afghanistan.

In addition, the DoD must ensure rapid medical care and evacuation of dispersed U.S. forces fighting terrorism. The 2017 ambush of U.S. soldiers in Niger highlighted that medical response times for injured American personnel in West Africa are much longer than response times in other parts of the world. The DoD OIG is currently examining the readiness of mobile medical teams supporting contingency operations in the U.S. Africa Command and U.S. Indo-Pacific Command areas of responsibility to determine whether these mobile medical teams are able to provide trauma care in austere environments where there is limited access to military treatment facilities.

An increasing challenge for the DoD is to counter enemy disinformation and messaging, which seeks to shape local opinion about the violent extremist threat and to mischaracterize the actions of United States and partner activities. In Afghanistan, both the Taliban and ISIS-Khorasan aggressively transmit their messaging using multiple traditional and modern platforms, including word of mouth, religious chants, radio broadcasts, and social media. The DoD has not effectively countered this information campaign, because of limited manpower and technical resources assigned to the challenge as well as cultural and linguistic difficulties. The effort to counter these messages also require coordination with the Department of State and local counterparts, which also have messaging operations. The DoD OIG is currently evaluating DoD information operations in Iraq and Syria and plans to conduct a similar evaluation of information operations in Africa.

Moreover, as demonstrated in Iraq, Syria, Afghanistan, and other countries around the world, violent extremist organizations are constantly adapting their tactics, techniques, and procedures. When executing counterterrorism operations, the DoD faces enemies that combine conventional military tactics, guerilla warfare, and high-tech information operations. According to Lieutenant General Michael Nagata, former Strategy Director of the U.S. National Counterterrorism Center, "In only five years, ISIS's global network is today larger than al Qaeda's despite decades of effort, and all terrorist groups are mimicking ISIS' innovations. In South Asia, where we face a nexus of al Qaeda, Taliban, Haqqani, and ISIS, our search for a negotiated settlement must confront the question of whether we can 'out-innovate' the adversary."

BUILDING PARTNER CAPACITY

DoD counterterrorism operations are conducted primarily "by, with, and through" local government entities. The DoD has focused these supporting efforts on improving or building partner capacities through training and equipping, although it can be directly involved in joint counterterrorism activities with partners in an accompanying or advising role. This strategy seeks to empower local forces while reducing the risk and burden for the United States. However, it also adds challenges, including the bureaucratic and political issues of working through a foreign government, tracking equipment provided to partner forces, monitoring contractors who execute supporting efforts and programs, and measuring the success of these operations and supporting programs.

U.S. Marines and Philippine airmen compare methods on how to set up a range card during Exercise KAMANDAG 3 at Colonel Ernesto P. Ravina Air Base, Philippines, October 9, 2019. (U.S. Marine Corps photo)

As part of its capacity-building activities, the DoD often provides equipment, including lethal weapons and sensitive technologies, to local partner forces. To comply with the Foreign Assistance Act and the Arms Export Control Act, the DoD must ensure that this equipment is not misused, remains under the control of partner forces, and does not fall into the hands of extremists or individuals with human rights violations. Monitoring the use of weapons and equipment provided to partner forces has been a continual challenge in Afghanistan, where Taliban fighters often steal U.S.-provided equipment, such as tactical vehicles and night-vision goggles, from Afghan forces during raids or other combat engagements. In addition, in a February 2019 evaluation report on equipment provided to Iraqi border forces, the DoD OIG determined that the DoD did not maintain proper documentation of divested equipment in accordance with U.S. laws, and lacked assurance that equipment, including lethal weapons and explosives, was not provided to individuals who have committed gross violations of human rights, or are associated with terrorist groups.[14]

In addition, the DoD OIG has, in numerous oversight projects, identified many cases where the DoD did not provide sufficient oversight of contractors that implement these train, advise, assist, and equip programs. For example, in an August 2019 evaluation report, the DoD OIG found that a contractor training Afghan Tactical Air Controllers did not teach students how to coordinate airdrops.[15] In an August 2019 audit report, the DoD OIG determined that U.S. forces did not verify that the contractor building the Afghan Personnel and Pay System developed the system in accordance with contract requirements.[16]

Moreover, while the DoD has reported incremental progress in its efforts to build the capacity of forces in Iraq, Syria, Afghanistan, and elsewhere, the DoD often lacks concrete metrics to measure progress and make necessary adjustments to its programs. Capacity-building programs are often long-term efforts that also can be undermined by frequent rotations of military and civilian advisors. In Afghanistan, for example, the frequent rotation of DoD personnel to support the Operation Freedom's Sentinel mission often brings new assessments, new styles of advising, and new ways to measure progress. In Iraq and Syria, the Coalition acknowledged that its metrics for success are subjective. With regard to Afghanistan, a January 2018 DoD OIG evaluation report on U.S. efforts to build the Afghan Air Force found that the lack of metrics and a defined end-state for the program could result in inefficient and ineffective use of U.S. resources.[17] Ultimately, the lack of consistent metrics, along with inconsistent oversight of equipment and contractors, leaves the DoD with less insight into whether these partnered efforts are having their intended effect.

STABILIZATION AND TRANSITION

Counterterrorism challenges remain even when military operations achieve decisive effects on violent extremists. According to former Commander of U.S. Central Command General Joseph Votel, defeating ISIS is not just about conducting military operations; it also involves keeping continued pressure on them

[14] Report No. DODIG-2019-057, "Iraqi Border Guard Equipment," February 13, 2019.

[15] Report No. DODIG-2019-110, "Evaluation of U.S. and Coalition Efforts to Train, Advise, Assist, and Equip Afghan Tactical Air Coordinators, Air Liaison Officers, and Afghan Air Targeting Officers," August 8, 2019.

[16] Report No. DODIG-2019-115, "Audit of the Planning for and Implementation of the Afghan Personnel and Pay System," August 15, 2019.

[17] Report No. DODIG-2018-058, "Progress of U.S. and Coalition Efforts to Train, Advise, and Assist the Afghan Air Force," January 4, 2018.

so they cannot resurge. According to the U.S. Department of State 2018 Stabilization Assistance Review, following conflict,

> we must consolidate security gains, reduce levels of local instability, and work with local partners to peaceably manage change and provide legitimate and responsive governance. Our national experience over the past two decades has taught us that it is not enough to win the battle; we must help our local partners secure the peace by using every instrument of our national power.[18]

During these periods of stabilization and transition, the DoD must coordinate with Federal agencies and international partners to support the rebuilding efforts and shift continuing counterterrorism responsibilities to local partner forces.

Stabilization programs—efforts to rebuild infrastructure and institutions damaged by conflict—are a critical component of counterterrorism efforts, although they are not implemented exclusively by the DoD. Military operations may degrade the capacity of violent extremist organizations, but they do not address the political and economic instability that contribute to the growth of violent extremism. For example, in Syria, U.S. military leaders have reported that ISIS is active in the al Hol camp for internally displaced persons, where humanitarian conditions are dire, and where ISIS is recruiting individuals to its ideology. In the Philippines, the Philippine government has been slow to rebuild the city of Marawi, which was severely damaged in a 2017 ISIS siege and the subsequent battles to retake the city, and which left more than 70,000 people displaced. The DoD has identified the population of Marawi as vulnerable to terrorist recruitment and radicalization.

Interagency coordination in these areas remains a significant challenge for the DoD. Operation Inherent Resolve in Iraq and Syria is based on a whole-of-government strategy, in which DoD supports and relies on efforts by other U.S. Government agencies, including the Departments of State, the Treasury, Homeland Security, Justice, and Energy, and the U.S. Agency for International Development. However, a 2018 Department of State OIG report found that interagency coordination challenges between the Department of State, the DoD, and other agencies slowed decision making and impeded development of clear lines of authority for Syria stabilization planning. For example, the Department of State and the DoD had differing standards for protecting civilian personnel, incompatible communications equipment, and conflicting policies for funding, training, and medical clearances.[19]

In addition, when the DoD transitions security and rebuilding activities to local partner forces, these partner forces can suffer from poor local funding, corruption, and limited capacity to complete tasks independently. The decision to transition responsibilities creates the potential for resurgence of the terrorist threat. For example, in Afghanistan, while the DoD and partner nations may reduce their presence in the coming years, the Afghan government can fund only a portion of its armed services and lacks the capacity to perform many advanced support tasks required to combat terrorists, such as in the areas of logistics and intelligence. In Iraq,

[18] Department of State, "Stabilization Assistance Review: A Framework for Maximizing the Effectiveness of U.S.Government Efforts to Stabilize Conflict-Affected Areas," July 5, 2018.

[19] Report No. ISP-I-18-29, "Department of State Stabilization Programs in Syria Funded Under the Further Continuing and Security Assistance Appropriations Act, 2017," September 2018.

the government has made only modest progress in addressing popular demands in some parts of the country for jobs, electricity, and potable water, and in rebuilding cities and infrastructure damaged in counter-ISIS fighting, resulting in widespread civil unrest.

INFLUENCE OF EXTERNAL ACTORS

The DoD's counterterrorism efforts are also challenged by malign influence by external state actors, such as Iran. Iran provides weapons, personnel, and other support to militias in Iraq and Syria whose goals often run counter to efforts by the United States and its partner forces in the region. Iran also exerts political influence over Iraqi and Syrian institutions to undermine support for the U.S. military presence in Iraq and Syria and U.S. stabilization activities in those countries.

Under Operation Inherent Resolve, the DoD cannot counter Iran directly, but must instead rely on its Iraqi and Syrian partners, many of whom have limited capability or political inclination to confront Iran and are also targets of Iranian influence. The DoD also faces challenges from Iran's extensive network of influence throughout the military, political, and social institutions of Iraq, Syria and other countries.

The DoD's counterterrorism activities are also affected by other external actors. Russia and China continue to expand their influence in diverse international economic, security and political ways. These activities can harm the DoD's ability to counter terrorists because rival influence efforts may force international partners to choose sides when U.S. foreign policy goals run up against those of a strategic competitor. For example, Russia is supporting pro-regime forces in Syria, limiting access and complicating efforts by Coalition forces to defeat ISIS.

In summary, the DoD faces numerous challenges as it seeks to counter persistent and evolving terrorist threats. The DoD must balance the resources it provides for its counterterrorism missions with other national security priorities and efforts, including countering the threats from China, Russia, North Korea, and Iran. In addition, as the DoD conducts operations against extremist threats, it increasingly must work with local and international partners, creating risks to military personnel and coordination challenges. The DoD must also monitor equipment, contractors, its own progress, and the progress of its partners as it builds partner capacity against violent extremists. To ensure defeated terrorist groups do not resurge, the DoD must overcome resource constraints, bureaucratic concerns, and interagency problems to coordinate with partner governments and other Federal agencies as it works to stabilize conflict environments, prevent further radicalization, and transfer security responsibilities to local forces. Finally, the DoD must contend with external actors, such as Iran, China, and Russia, whose activities run counter to and often seek to undermine the DoD's counterterrorism mission.

Navy Petty Officer greets his daughter during the USS Kearsarge's homecoming in Norfolk, Va., July 18, 2019. (U.S. Navy photo)

Challenge 3. Ensuring the Welfare and Well-Being of Service Members and Their Families

One of the DoD's top priorities is ensuring that service members and their families have the support they need to successfully navigate the challenges of military life. The DoD is responsible for "promoting, improving, preserving, or restoring the mental or physical well-being of Service members."[20] In addition, DoD policy states that "the role of personal and family life shall be incorporated into organizational goals related to the recruitment, retention, morale, and operational readiness of the military force."[21]

In July 2019, when he became the Secretary of Defense, Secretary Esper stated during his DoD welcome ceremony:

> [A]s a personal priority of mine, we will place a particular focus on the wellbeing of our families. Our military spouses and civilians and children make tremendous sacrifices for this country [a]nd in return, I am committed to ensuring they are properly cared for. . . . They know that this administration, that this Congress and the American people have their back. And they know that when they are deployed far away from home, their families will be taken care of.

To fulfill this goal, the DoD must address many challenges that can affect service members and their families, including substance abuse, sexual assault, suicides, unsafe housing and installations, inadequate child care, and spouse unemployment. Those challenges can be exacerbated by frequent deployments, relocations, and the stress that those events place on the service member's family. The challenges are longstanding and difficult to address, but it is critical for the DoD to make progress in these areas to help ensure the welfare and well-being of service members and their families.

[20] Joint Publication 3-0, "Joint Operations," January 17, 2017, Incorporating Change 1, October 22, 2018.
[21] DoD Instruction 1342.22, "Military Family Readiness," July 3, 2012, Incorporating Change 2, April 11, 2017.

SUBSTANCE ABUSE PROGRAMS

Alcohol and drug misuse can impact service members' physical and mental health, as well as mission readiness and productivity. The National Institute on Drug Abuse has recognized that both active duty and retired service members are at risk of developing substance use problems. The National Institute on Drug Abuse noted that the stresses of multiple deployments, combat exposure, related injuries, and the unique culture of the military contributes to the risk of developing substance use problems. The Institute also stated that the zero-tolerance policies and stigma pose difficulties in identifying and treating substance use problems in military personnel, as does the lack of confidentiality that deters many who need treatment from seeking it.

During the DoD OIG's recent evaluation of the management of opioid use disorders for Military Health System beneficiaries, representatives from the Assistant Secretary of Defense for Health Affairs stated that the primary substance abuse problem in the military is alcohol. According to the RAND Corporation's 2015 DoD Health Related Behaviors Survey, nearly 30 percent of service members are current binge drinkers (5 or more drinks for men and four or more drinks for women on one occasion), and 21 percent reported use of opioid pain relievers. Service members who deployed in the 3 years before the survey and experienced high levels of combat were more likely to report binge drinking (34.6 percent) and prescription drug use (36.2 percent). Service members who deployed in the 3 years before the survey and experienced low to moderate exposure to combat were less likely to report binge drinking (28.2 percent) and prescription drug use (23.7 percent).

According to the 2015 DoD Health Related Behaviors Survey, one in three service members (30 percent) were current binge drinkers, 5.4 percent of personnel were heavy drinkers (binge drinking on 5 or more days in the previous month), and 35 percent met criteria indicative of hazardous drinking or possible alcohol use disorder. More than 20,000 active duty service members receive treatment for alcohol use disorders each year. In addition, according to a May 2019 Congressional Research Service report on trends in active duty military deaths, alcohol was a factor in 14 percent of all active duty military accidental deaths and 7 percent of active duty military deaths unrelated to overseas contingency operations deaths.

Drug abuse is another challenge. According to a November 2018 National Center for Health Statistics report, more than 70,000 people died of drug overdoses in the United States in 2017, equating to 192 people per day. Around two-thirds of those deaths, 47,600, involved the use of opioids, and the rate of opioid overdose deaths has doubled since 2012.[22] Opioid abuse can affect service members, as it does civilians. However, although service members are prescribed opioid medications at a higher rate than the general population, prescription drug misuse in the military is lower than the civilian population and is declining, according to the 2017 DoD report to Congress. Additionally, the 2017 DoD report to Congress stated that the number of service members diagnosed with opioid drug dependence or opioid abuse decreased by 38 percent between 2012 and 2016, and opiate-positive drug tests among service members declined over 60 percent between FY 2013 and FY 2016. To assess an

[22] National Center for Health Statistics Data Brief No. 329, "Drug Overdose Deaths in the United States, 1999–2017," November 2018.

aspect of the opioid challenge, the DoD OIG is conducting an audit to determine whether beneficiaries were overprescribed opioids at selected military medical treatment facilities. Additionally, the DoD OIG plans to conduct an evaluation of the DoD's opioid abuse prevention efforts.

In a 2018 report to Congress on the prevention and reduction of underage drinking, the Department of Health and Human Services stated that the DoD has implemented a series of substance use disorder prevention efforts, Service-level prevention programs, the establishment of the Addictive Substances Misuse Advisory Committee, and the alcohol abuse countermarketing campaign called "That Guy."

In addition to treatment provided through the Military Health System, Service members may receive treatment by referral to TRICARE-approved agencies such as Military OneSource. Military OneSource connects service members with the resources they may need to overcome substance abuse or assist those they know with finding help. For example, Military OneSource provides information to the Military Crisis Line and Military Crisis Line Chat. The DoD's Drug Demand Reduction Program provides education, outreach, and awareness programs regarding illicit drugs and misuse of prescription drugs.

To further address prescription drug abuse, the DoD established the Prescription Monitoring Program to attempt to identify DoD patients who are potentially at risk for misuse of prescription drugs. The program identifies patients who show signs of misuse of controlled substances and other high-risk medications. Under the program, the TRICARE Pharmacy contractor determines which patients are at high risk of substance abuse and sends the results to the appropriate TRICARE managed care support contractor based on the patient's location. Each of the two managed care support contractors are required to conduct medical reviews on at least 20 patients per quarter to determine whether to take action to restrict access to medications, require further monitoring, or to take no action. For example, the contractor could recommend restricting a patient to receive prescriptions from only one provider and one pharmacy. This would limit the ability of patients trying to obtain controlled substance prescriptions from multiple doctors and pharmacies, helping to ensure that patients receive only those prescriptions that are truly needed for their diagnoses. The DoD OIG plans to review the Prescription Monitoring Program to determine whether the program is effectively identifying patients at risk for substance abuse.

However, reliable data is crucial for the DoD to accurately identify those patients that are potentially misusing prescription drugs. During an ongoing audit, the DoD OIG determined that opioid quantities in the Military Health System Data Repository were not reliable for calculating and tracking patients' true use of opioids per day. The DoD's challenge in identifying and treating opioid misuse and accuracy of opioid data is discussed further in Management Challenge 10, "Providing Comprehensive and Cost-Effective Health Care."

SEXUAL ASSAULT PREVENTION AND RESPONSE PROGRAMS

Sexual assault within the DoD remains a persistent and serious challenge. The number of reported sexual assaults in the DoD has risen in the past several years. According to the "Department of Defense Annual Report on Sexual Assault in the Military, Fiscal Year 2018," published in April 2019, service members and civilians reported 7,623 incidents of sexual

assault in FY 2018, compared to 6,769 reports in FY 2017, and 6,172 reports in FY 2016. Over 6 percent of active duty women reported that they were sexually assaulted in the year before being surveyed, compared to 4.3 percent in FY 2016. The estimated rate for active duty men remained statistically unchanged at 0.7 percent.

Sexual assault takes a toll mentally and physically on victims. The Department of Veterans Affairs' National Center for Post-Traumatic Stress Disorder stated on its website that sexual assault may be more likely to lead to post-traumatic stress disorder than other types of traumatic events, based on data from a study comparing the effects of different types of traumatic events. In this study, 45 percent of the women who reported having experienced a rape met criteria for post-traumatic stress disorder. This was significantly higher than the 38.8 percent rate of post-traumatic stress disorder among men who had experienced combat. The study also stated that 65 percent of men who had been raped met the criteria for post-traumatic stress disorder.[23] Although post-traumatic stress disorder is treatable and does not always result in medical separation, it can lead to permanent disability and loss of the ability to remain in the service for some. The DoD Office of People Analytics reported that, in 2016, 28 percent of women and 23 percent of men who reported being sexually assaulted also reported that "they took steps to leave or separate from the military" as a result of sexual assault.[24]

DoD and Military Service policies require the Military Services to consult victims who report sexual assault regarding their preference for prosecuting offenses by courts-martial or in a civilian court with jurisdiction over the offense before the referral of charges. In 2018, the DoD OIG performed an audit to determine whether victims of sexual assault were consulted on their preference for prosecuting offenses by courts-martial or in a civilian court with jurisdiction over the offense.[25] The DoD OIG determined that the DoD did not establish a DoD-wide process to ensure that victims of alleged sexual assaults were asked about their preference for prosecution or to ensure that their preference was documented. The DoD OIG also determined that the policies issued by the Military Services did not require that the victim's preference be documented. The DoD OIG recommended the DoD implement guidance requiring the Military Services "to

A Soldier wears a Sexual Harassment/Assault Response and Prevention program pin at Joint Base Langley-Eustis, Va., April 25, 2018. (U.S. Air Force photo)

[23] National Center for PTSD; Sexual Trauma: Information for Women's Medical Providers.

[24] Office of People Analytics Report No. 2016-050, "2016 Workplace and Gender Relations Survey of Active Duty Members, Overview Report," May 2017.

[25] Report No. DODIG-2019-064, "Audit of DoD Efforts to Consult with Victims of Sexual Assault Committed by Military Personnel in the United States Regarding the Victim's Preference for Prosecution," March 20, 2019.

document that the victim was asked about the preference for prosecution and when and what the victim's preference was."

The DoD OIG recently evaluated the DoD's handling of incidents of sexual assault at the United States Air Force Academy. The evaluation found that victim advocates provided services to cadet-victims of sexual assault, as required by DoD and Air Force policy. However, the DoD OIG also determined that the Air Force Academy did not have a process to document contacts and consultations with cadet-victims who chose not to make an official report of sexual assault, or a means to document any resulting referrals to victim support services. Furthermore, the DoD OIG determined that the number of reports of sexual assaults were not accurately reported to Congress in the "Annual Report on Sexual Harassment and Violence at the Military Service Academies," as required by law.

The DoD OIG is currently conducting an evaluation of the United States Military Academy West Point handling of sexual assaults and plans to conduct a similar evaluation of the United States Naval Academy. Additionally, the DoD OIG plans to conduct an evaluation of the military criminal investigative organizations' response to special victim investigation and prosecution capability requirements, which will focus on the collaboration between agencies that provide victim advocacy to victims of sexual assault, investigate the victim's report of sexual assault, and prosecute the offenders of sexual assault.

When service members are found to have committed sexual assault, the DoD must hold them accountable. Concerns have been raised regarding the investigation and prosecution of sexual assault in the military. For example, in a May 2019 press release, the co-chair of the Board of Directors at the Service Women's Action Network, a national organization advocating for the rights of service women and women veterans, stated:

> Despite the increase in reporting, prosecutions and convictions of sexual assaults have decreased over the last five years albeit for a variety of reasons—from lack of evidence to jurisdictional issues. The fact that the military encourages victims to report offenses is a positive step; however, the military must do more to alleviate the prevalent culture of sexual harassment and sexual assault.

According to the DoD Sexual Assault Prevention and Response Office, there were 4,002 case dispositions (the investigation or adjudication process was complete) that started with an unrestricted report of sexual assaults made in FY 2018 and prior fiscal years.[26] The office also reported that the DoD could not take action in 1,148 cases because 1,110 cases were outside of the DoD's legal authority and 38 cases involved service members prosecuted by a U.S. civilian or a foreign authority. For the remaining 2,854 cases, 1,845 (65 percent) resulted in disciplinary action and 935 cases (33 percent) resulted in no action taken by the command. According to the report, the reasons action was not taken included the death of the subject, the victim declining to participate in the judicial proceedings, insufficient evidence, or expired statute of limitations.

The following table provides statistics on the number of unrestricted sexual assault cases for FY 2018 and their disposition. The DoD uses the term "sexual assault" to refer to a range of crimes, including rape, sexual assault, forcible

[26] "Department of Defense Annual Report on Sexual Assault in the Military Fiscal Year 2018," April 27, 2019, Appendix B, "Statistical Data on Sexual Assault."

sodomy, aggravated sexual contact, abusive sexual contact, and attempts to commit these offenses, as defined by the Uniform Code of Military Justice.

Sexual assault investigations may not find sufficient evidence to support disciplinary action against the subject on a sexual assault charge but may find evidence of other forms of chargeable misconduct. In FY 2018, commanders took action in 634 cases that the military criminal investigative organizations originally investigated for sexual assault allegations, but for which evidence only supported action on non-sexual assault misconduct, such as making a false official statement, adultery, assault, or other crimes.

During an April 2019 press briefing for the issuance of the Annual Report on Sexual Assault in the Military, the Director of the DoD Sexual Assault Prevention and Response Office stated, "Every sexual assault in the military is a failure to protect the men and women who have entrusted us with their lives." She also stated, "We will not rest until we eliminate this crime from our ranks."

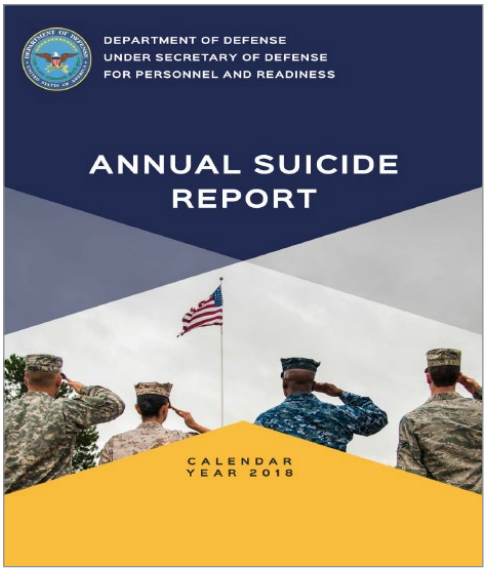
Table 1. Case Dispositions Reported in FY 2018

Case Disposition Category	Count of Case Dispositions
Sexual Assault Investigation That Can Be Considered for Possible Action by DoD Commanders	2,854
Evidence Supported Commander Action	1,845
Sexual Assault Offense Action	1,211
Court-Martial Charge Preferred (Initiated)	668
Nonjudicial Punishment (Article 15, UCMJ)	267
Administrative Discharge	118
Other Adverse Administrative Action	158
Non-Sexual Assault Offense Action	634
Court-Martial Charge Preferred (Initiated)	72
Nonjudicial Punishment (Article 15, UCMJ)	339
Administrative Discharge	96
Other Adverse Administrative Action	127
Unfounded by Command/Legal Review	74
Commander Action Precluded	935
Victim Died	0
Victim Declined to Participate in the Military Justice Action	173
Insufficient Evidence to Prosecute	735
Statute of Limitations Expired	27

Notes: Victims who were assaulted by multiple subjects are counted only once to correspond with the subject who received the most serious disposition.

Data Source: "Department of Defense Annual Report on Sexual Assault in the Military Fiscal Year 2018," April 27, 2019, Appendix B, "Statistical Data on Sexual Assault."

In addition to accountability for committing sexual assault, the DoD must focus on prevention of sexual assault. In April 2019, the Under Secretary of Defense for Personnel and Readiness issued the Prevention Plan of Action, which established expectations for a comprehensive prevention process and prevention system, as well as specific actions that the DoD, the Military Services, and the National Guard Bureau must take for effective prevention. Phase I requires the Military Services and the National Guard Bureau to conduct a self-assessment by December 31, 2019, of the status of their prevention systems to identify strengths, opportunities for improvement, and actionable starting points for the development of Phase II (Plan of Action and Milestones). Phase II requires the Military Services and the National Guard Bureau to prepare a plan of action and milestones for each of the 29 objectives in the overall Prevention Plan of Action by June 30, 2020. Phase III (Execution) requires the Military Services and the National Guard Bureau to execute activities to meet the 29 objectives of the Prevention Plan of Action. Phase IV (Evaluation) requires a report on the assessment efforts and outcomes produced by the Prevention Plan of Action by June 30, 2023.



SUICIDE PREVENTION PROGRAMS

The DoD is focusing attention on preventing suicides by DoD military personnel, which remains a significant challenge.

In testimony before the House Armed Services Subcommittee on Military Personnel and House Veterans Affairs Subcommittee on Health in May 2019, the Executive Director, Force Resiliency, Office of the Under Secretary for Personnel and Readiness, stated that suicide prevention is a complex issue for the DoD; but, DoD leaders "cannot rest until [they] have pursued every opportunity" to prevent suicide. Each Service is seeking to address suicide prevention with measures such as training, data collection and analysis, and strategic communications about suicide-related behaviors.

The Defense Suicide Prevention Office works with the Military Services to implement suicide prevention programs, to publish related policies, and to ensure that certain populations at high risk, such as transitioning service members, have access to quality mental health care and suicide prevention resources. In November 2017, the DoD issued DoD Instruction 6490.16, "Defense Suicide Prevention Program," outlining processes for planning, directing, guiding, and resourcing to effectively develop and integrate the Suicide Prevention Program within the DoD.

Despite these efforts, the findings of the calendar year (CY) 2018 DoD Annual Suicide Report show an increase in suicide rates among the active duty military members, as well as higher than expected rates in the National Guard, compared to the U.S. population.[27] In October 2018, the DoD established a requirement for a DoD Annual Suicide Report to serve as the official source of annual suicide counts and unadjusted

[27] Under Secretary of Defense for Personnel and Management, "Annual Suicide Report: Calendar Year 2018," September 2019.

rates for the DoD and a means by which to increase transparency and accountability for DoD efforts towards the prevention of suicide. The DoD also required the reporting of data on suicide deaths among military family members. The DoD intends to continue to publish the annual DoD Suicide Event Report, which provides interpretations of the risk factors, such as substance abuse or anxiety, associated with military suicide and suicide-related behavior.

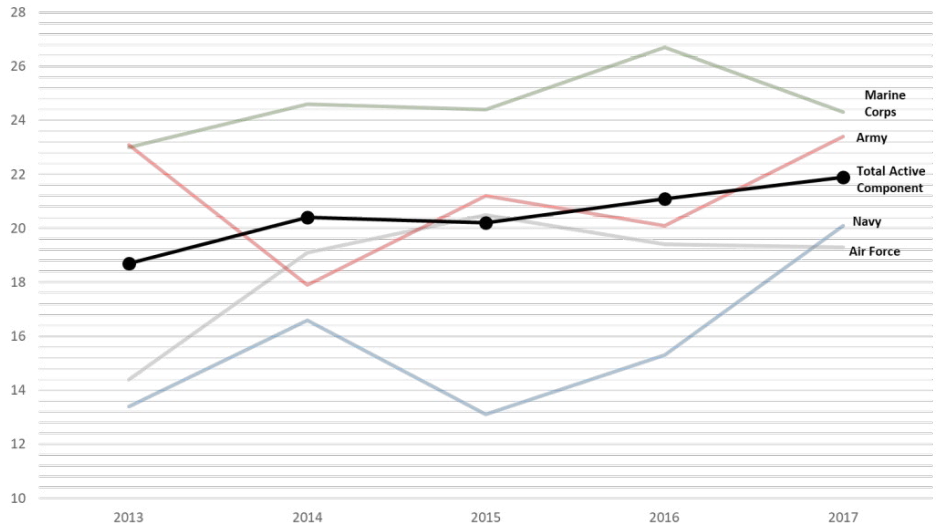
The Defense Suicide Prevention Office issued its first Annual Suicide Report in September 2019. According to the report, the 2018 unadjusted suicide rate was 24.8 deaths per every 100,000 active duty service members. The 2018 unadjusted suicide rate for the Reserves, combined across all Military Services and regardless of duty status, was 22.9 deaths per 100,000 reservists. The 2018 unadjusted suicide rate for the National Guard, combined across the Air and Army Guard and regardless of duty status, was 30.6 deaths per 100,000 members of the Guard population. These data include all known or suspected suicides (both confirmed and pending) as of March 31, 2019.

Figure 2 below depicts adjusted annual suicide rates (per 100,000 population) for the Active Component, for CY 2013 through CY 2017.

According to the National Defense Authorization Act for FY 2015, the DoD is required to collect, report, and assess data regarding military family suicide. The 2018 report shows there were 186 reported suicide deaths among military spouses and dependents in CY 2017, the most recent data available on military family members. However, the information reported was based on voluntary disclosures by service members, which likely resulted in incomplete counts of military family suicide deaths.

The 2018 DoD Annual Suicide Report also noted that approximately half (51.5 percent) of military members who died by suicide in 2018 made contact with the Military Health System in the 90 days before death. The prevalence of various risk factors, protective factors, and

Figure 2. Annual Suicide Rates per 100,000 Service Members by DoD Component and Service From CY 2013 Through CY 2017



Sources: CY 2103 through CY 2014 data obtained from the Psychological Health Center of Excellence 2014 DoD Suicide Event Report. CY 2015 through CY 2017 data obtained from the Psychological Health Center of Excellence 2017 DoD Suicide Event Report.

other event characteristics among suicides in 2018 was consistent with those observed over previous years.

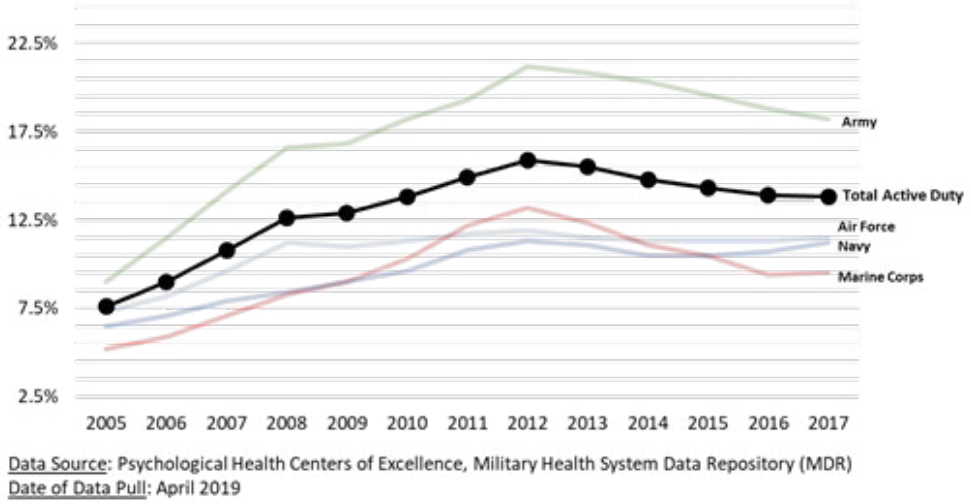
According to the report, suicide in the enlisted population occurs at a higher rate than in the officer ranks. Although younger service members, aged 17 to 19, do not tend to have a high number or rate of suicide; 20 to 30-year old service members make up roughly two-thirds of the population who died by suicide.

Identifying and providing care for behavioral health conditions that can lead to suicide is a critical challenge for the DoD. As shown in Figure 3, diagnosed mental health disorders in the total population of active duty personnel increased by 6 percent from CY 2005 to CY 2017.

In testimony before the House Armed Services Subcommittee on Military Personnel and House Veterans Affairs Subcommittee on Health in May 2019, the Director of Mental Health Policy and Oversight, Office of the Assistant Secretary of Defense (Health Affairs), stated that part of the DoD prevention efforts include behavioral and mental health specialists and military family life counselors who provide support to units. He also stated that psychiatrists are deployed with units to provide additional division-level support. The DoD also offers training to help leaders recognize situational factors related to increased risk for suicide.

The DoD Suicide Prevention Office reported that service members transitioning from military service have in an increased risk for suicide. While the DoD maintains medical records for service members while serving, not all service members who separate from the military seek medical care within the Department of Veterans Affairs health care system. In January 2018, a Presidential Executive Order required the DoD, Department of Veterans Affairs, and Department of Homeland Security to submit a Joint Action Plan to the White House describing actions to provide seamless access to mental health care and suicide prevention resources for transitioning service members. This order

Figure 3. Percentage of Patients with Any Mental Health Condition, 2005 Through 2017



Sources: Psychological Health Centers of Excellence, Military Health System Data Repository (MDR)

emphasizes access to services during the critical first year period following discharge, separation, or retirement from military service.

Both the DoD and the Department of Veterans Affairs have independent campaigns on suicide prevention. The Department of Veterans Affairs Office of Mental Health and Suicide Prevention addresses suicide using a community-based suicide prevention effort guided by the National Strategy for Preventing Veteran Suicide. The DoD Suicide Prevention Office addresses suicide through five initiatives: (1) data surveillance and analysis, (2) research and program evaluation (3) plans and policy oversight, (4) outreach campaigns, and (5) training.

The DoD and Department of Veterans Affairs efforts to prevent suicide overlap in the service member's transition phase. Service member medical records are transferred from the DoD to the Department of Veterans Affairs as the service member transitions from active duty to veteran status so that their medical information is shared. However, it is difficult for the DoD and the Department of Veterans Affairs to share medical information about service members with heightened risk for suicide, because the DoD and the Department of Veterans Affairs systems are not interoperable. The DoD OIG is conducting an audit to determine whether the DoD is developing standards and implementing controls to provide interoperability between the health care systems of the DoD. Interoperability of the DoD and Department of Veterans Affairs electronic health records systems is discussed in further detail in Management Challenge 10, "Providing Comprehensive and Cost-Effective Health Care."

On August 27, 2019, the DoD Suicide Prevention Office Director discussed at the DoD/Department of Veterans Affairs Suicide Prevention Conference the new focus areas for the DoD's suicide prevention efforts. In addition to the DoD Annual Suicide Report, another focus area is program evaluation. The DoD Suicide Prevention Office intends to use the data on suicide risk factors to evaluate suicide prevention program outcomes. The third focus area is collaboration. The DoD Suicide Prevention Office intends to cultivate active partnerships with the Department of Veterans Affairs, Defense Health Agency, and the National Action Alliance for Suicide Prevention.

The DoD and the Department of Veterans Affairs have a joint working panel called the "Lived Experience Panel," which surveys parents of individuals who died by suicide and survivors of suicide attempts to understand underlying suicide risk factors. In addition, the #BeThere outreach campaign is a joint DoD and Department of Veterans Affairs effort to use social media to increase awareness of suicide risk factors and warning signs.

However, gaps in understanding the causes of suicide in service members who died by suicide remain. In November 2014, the DoD OIG recommended that the Under Secretary of Defense for Personnel and Readiness publish guidance requiring suicide event boards to establish a multidisciplinary approach for obtaining the data necessary to make comprehensive DoD Suicide Event Report submissions. Additionally, the DoD OIG recommended that the Under Secretary of Defense for Personnel and Readiness create systems to enable military leaders to develop installation-level command suicide event tracking reports.[28] However, both recommendations remain open and are

[28] Report No. DODIG-2015-016, "Department of Defense Suicide Event Report (DoDSER) Data Quality Assessment," November 14, 2014.

Privatized military base housing at Peterson Air Force Base (U.S. Air Force photo)

awaiting final Under Secretary of Defense for Personnel and Readiness coordination of Service responses.

DoD Suicide Event Report accuracy and completeness continues to include a high number of "don't know/data unavailable" responses because DoD Suicide Event Report submissions do not reflect information obtained during Service suicide prevention lessons-learned processes. Without a comprehensive and complete DoD Suicide Event Report submission, the DoD will continue have difficulty conducting accurate trend or causal analysis necessary for developing more effective suicide prevention policy and programs to reduce suicide rates across the force.

INSTALLATIONS AND HOUSING

The adequacy of installations and housing for service members and their families is a troubling challenge for the DoD that can undermine morale, welfare, and readiness of service members.

Properly built and maintained installations and housing are essential for service members and their families.

The DoD is one of the U.S. Government's largest holders of real estate, managing a global portfolio that consists more than 585,000 facilities, located on 4,775 sites worldwide, and covering approximately 26.9 million acres, an area around the size of Tennessee. However, the DoD privatized 99 percent of its military family housing in the continental United States under the Military Housing Privatization Initiative, which

resulted in private sector developers owning, operating, maintaining, improving, and assuming responsibility for military family housing.

During FYs 2017 and 2018, the DoD, the Government Accountability Office, and the DoD OIG all reported that the DoD needs to improve its oversight of installations and housing. For installations, the reports highlighted that the Services were unable to maintain facility records, conduct facility assessment reviews, and assess risks of climate-change effects in military construction projects. For housing, the reports detailed the inability of the Services to fully mitigate health and safety hazards, such as mold, lead-based paint, and pest infestation in privatized housing. Despite years of reporting on these issues, the DoD continues to experience challenges with installations and housing, ranging from an inaccurate inventory of DoD facilities to inadequate housing provided to service members and their families.

For example, in September 2013, the DoD directed the Military Departments to record a facility condition for each asset on their installation in their respective data systems and to inspect all facilities using a standard process by September 2018.[29] However, in FY 2019, the Government Accountability Office reported that the Military Services had not consistently recorded acquisition of, changes to, and disposal of facilities. The Government Accountability Office also found that the Military Services had not corrected identified discrepancies in their data systems, such as facility condition and overdue asset reviews.[30] The Government Accountability Office noted that military installations had not consistently assessed risks from extreme weather and climate change effects and integrated that information into their master plans.[31]

The DoD continues to struggle with issues related to health and safety hazards in both Government-owned Government-controlled and privatized housing. Between FYs 2015 and 2017, the DoD OIG issued seven reports that detailed electrical system, fire protection system, and environmental health and safety hazards in military and privatized housing.[32] While the Military Departments agreed to the recommendations in the reports and acknowledged that improvements needed to be made, issues related to mold, water quality, lead-based paint, and carbon monoxide continue to be raised by military members and their families.

[29] Under Secretary of Defense for Acquisition, Technology, and Logistics Policy Memorandum, "Standardizing Facility Condition Assessments," September 10, 2013.

[30] Report No. GAO-19-73, "Defense Real Property: DOD Needs to Take Additional Actions to Improve Management of Its Inventory Data," November 13, 2018.

[31] 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.

[32] Report No. DODIG-2017-118, "Followup Evaluation on DoD Office of Inspector General Report No. DODIG- 2014-121, "Military Housing Inspection-Japan," September 30, 2014," September 14, 2017.

Report No. DODIG-2017-104, "Followup on DoD OIG Report No. DODIG-2015-013, "Military Housing Inspections – Republic of Korea," October 28, 2014," July 20, 2017.

Report No. DODIG-2017-004, "Summary Report – Inspections of DoD Facilities and Military Housing and Audits of Base Operations and Support Services Contracts," October 14, 2016.

Report No. DODIG-2016-139, "Military Housing Inspection – Camp Buehring, Kuwait," September 30, 2016.

Report No. DODIG-2015-181, "Continental United States Military Housing Inspections – Southeast," September 24, 2015.

Report No. DODIG-2015-162, "Continental United States Military Housing Inspections – National Capital Region," August 31, 2015.

Report No. DODIG-2015-013, "Military Housing Inspections – Republic of Korea," October 28, 2014.

A U.S. Army Staff Sergeant assigned to the 78th Signal Battalion reads "Goodnight, Goodnight, Construction Site," by Sherri Duskey Rinker during the Stuffed Animal Sleepover at a Library event at the Sagamihara Family Housing Area Library September 27, 2019. (U.S. Army photo)

Throughout 2018 and 2019, media reports highlighted continued issues with improper construction techniques, rampant water damage, improper electrical wiring, missing smoke alarms, chronic leaking that led to pervasive mold growth, and pest infestations in privatized military housing. Additionally, media reports indicated that privatized partners failed to respond to complaints, performed substandard maintenance and repairs, and falsified records.

For example, according to a Reuters report, military families moved off base to escape unsafe housing conditions. In February 2019, testimony before the Senate Armed Services Committee, Subcommittee on Personnel, military families living in privatized housing described conditions such as mold, poor water quality, contamination from lead-based paint, carbon monoxide, radon, faulty construction, and infestations, which have affected the health, safety, and well-being of service members and their families.

In response, military leaders acknowledged that the DoD's failure to provide oversight of housing affected safe living conditions for service members and their families. As a result of the complaints and recent attention focused on privatized housing, the DoD and Military Services have conducted internal reviews of privatized partner management actions, initiated feedback opportunities to hear resident concerns, focused more on addressing previous recommendations from the DoD OIG, and developed the pending Military Housing Privatization Initiative Bill of Rights. Once established, the Military

Housing Privatization Initiative Bill of Rights will affirm the rights for families residing in privatized housing to safe and healthy homes and communities; a housing advocate to provide advice and support; professional property management services; responsive communications with the landlord and maintenance staff; prompt and professional repairs; and dispute resolutions, mediation, and arbitration to resolve disputes concerning repairs, damage claims, and rental payments. The bill of rights will also affirm that families in privatized housing have the right to have their rental payments withheld from the property owner or manager until a dispute is resolved; the right to opportunities and sufficient time for move-in and move-out inspections, procedures, and paperwork; and the right to privacy. Finally, the bill of rights will affirm that families in privatized housing have the right to clearly defined rental terms and predictable rent; the right to not pay non-refundable fees and not have rent payment arbitrarily withheld; and the right to engage with DoD or command staff to address housing issues without fear of reprisal.

Additionally, Congress directed the DoD OIG and the Government Accountability Office to evaluate whether service members and their families were exposed to health and safety hazards in on-base military housing.[33] Both are conducting assessments of health and safety hazards management in military housing. The Government Accountability Office will report on privatized housing, and the DoD OIG will report on Government-owned and -controlled housing.

CHILD CARE SERVICES

Service members must deploy frequently, work long hours when not deployed, change duty stations often, and travel frequently, all of which can place strain on military families. One of these strains is the need for adequate child care. In addition, service members move roughly every 3 years, which requires them to find child care at their new installation.

The DoD has the largest employer-sponsored child care system in the United States, but the need for child care is growing as the size of the military increases. According to the 2017 Demographic Report published by the DoD, there were about 2.1 million service members with about 2.7 million family members, including spouses, children, and adult dependents, across the active duty and Selected Reserve population, which includes members in the Army National Guard, the Army Reserve, the Navy Reserve, the Air National Guard, the Air Force Reserve, the Marine Corps Reserve, and the Department of Homeland Security's Coast Guard Reserve.[34] Of the 2.7 million family members, about two-thirds (62.9 percent or 1.7 million) are children. Of those 1.7 million children, 633,954 (37.8 percent) are younger than 6 years old. Child care for these children includes hourly care, full-day care, part-day care, school-year care, summer camp, and extended care, including 24/7 care.

In May 2019 testimony before the House Armed Services Subcommittee on Military Personnel, the Under Secretary of Defense for Personnel and Readiness stated that the DoD recognizes the need for military families to have access to high-quality, affordable child care. In FY 2018,

[33] House Report 115-929, "Energy and Water Development and Related Agencies for the Fiscal Year Ending September 30, 2019, and For Other Purposes," September 10, 2018.

House Report 115-952, "Department of Defense for the Fiscal Year Ending September 30, 2019, and For Other Purposes," September 13, 2018.

[34] DoD Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy, "2017 Demographics: Profile of the Military Community."

the DoD system of care provided about 160,000 child care spaces through child development centers (child care services for infants through preschool-age children), school-age care programs (facility-based program that provides child care services to children in full-day kindergarten through grade 7 during the school year), family child care (providers are certified child care professionals who provide child care for infants through school-age children in their homes, located either on or off of an installation), and community-based care.[35]

However, this level of capacity is not sufficient to meet the DoD's current child care needs. For example, the Chief of Naval Personnel testified in May 2019 that the Navy had the capacity to provide child care for 35,000 children within Navy-provided sources. He also stated that the Navy is outsourcing the rest of the capacity (about 8,000), some to Family Child Care and some to community-based commercial providers. During May 2019 testimony, DoD officials stated that they needed at least an additional 14,500 child care slots.

The DoD has developed a single website, MilitaryChildCare.com, to provide information about on-base, military-operated, and military-subsidized child care options. It is designed to enable parents to seek space for their child in advance of a permanent change of station move or before the addition of a new child to the family.

However, in May 2019 testimony before the House Armed Services Subcommittee on Military Personnel, the Acting Under Secretary of Defense for Personnel and Readiness; the Army Deputy Chief of Staff; the Chief of Naval Personnel; the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services; and the Marine Corps Deputy Commandant for Manpower and Reserve Affairs reported that several installations experience an average wait time for on-installation child care in excess of 180 days. For example, Fort Bragg has a waitlist that exceeds a year. Marine Corps Base Camp Pendleton, California, bases in Hawaii, and Marine Corps Base Quantico, Virginia, have an average waitlist of 6 months. In addition, some locations, such as Wallops Island, Virginia, do not have any DoD-provided child care options available.

In addition, overnight child care options are limited. For example, service members assigned to Naval Station Norfolk are required to stand duty overnight, but, as of May 2019, only 24 spots were available for overnight child care, which are fewer than needed. Some of the factors that contribute to the growing waitlists for child care include lack of child care facilities, staff shortages contributing to closed rooms, and untimely background check completions for child care staff.

The DoD is seeking to address inadequate child care services. Through the Military Child Care in Your Neighborhood program, the DoD provides fee assistance to active duty service members (including Reservists on active duty orders) who are unable to obtain on-installation care because there are no vacancies, the available on-installation programs do not meet the family's needs, or the family lives more than 15 miles from an installation.

SPOUSAL EMPLOYMENT

Requiring families to relocate every few years can also disrupt a military spouse's career. This disruption and financial stress may cause

[35] Under Secretary of Defense for Personnel and Readiness, "Report to the Secretary of Defense and the Congressional Defense Committees: Military Family Readiness Council Fiscal Year 2018 Annual Report," July 2018.

the service member to either not reenlist or to retire if he or she is eligible. In his May 2019 testimony before the House Armed Services Subcommittee on Military Personnel, the Acting Under Secretary of Defense for Personnel and Readiness stated that 24 percent of military spouses are unemployed or underemployed, and that supporting military spouses and their employment can lead to family readiness and financial stability.

In July 2018, the Military Family Advisory Network conducted an online survey to examine the experiences of military families during the permanent change of station season. The survey asked about the effect moving had on spousal employment. The responses described the negative effect on stalled careers and unemployment, leading some to give up entirely on finding employment. Some of the challenges discussed in the responses included no job availability in their fields at the location they moved to, perceived hiring biases (not wanting to hire someone who will be moving in 1 to 3 years), and licensing delays (moving to a state that requires a person to have a license issued by that state in order to work). According to the survey, the moving process alone is a highly stressful and mentally exhausting experience, and the delays spouses experience finding work can cause increased financial strain.

In addition, many military spouses work in fields that require licenses or credentials. States may not accept military spouse licenses and credentials issued by other states, which would allow military spouses the opportunity to maintain employment during geographic relocations to mitigate the financial stress on military families. According to the Military OneSource website, the Defense State Liaison Office has successfully worked with some states to streamline license transfer processing and continues to work with interagency and state partners to expedite or exempt professional licensing requirements for military spouses. For example, the Defense State Liaison Office worked with 15 states on legislation to remove certification impediments for military spouse teachers. The Defense State Liaison Office is working with the other 35 states to pass similar legislation to remove certification impediments for military spouse teachers. In addition, the Defense State Liaison Office worked with 17 states that passed legislation enabling military spouses to transfer occupational licenses to other states and allowing transitioning service members to use their military record to obtain a license. The Defense State Liaison Office is working with the other 33 states to pass similar legislation.

To further address this challenge, in September 2019, the Secretary of Defense asked the Council of Governors "to assist with ensuring that military spouses have access to special provisions from the states to support military spouse licensure." In addition, the National Defense Authorization Act for FY 2018 authorizes the DoD to reimburse up to $500 for military spouse relicensing and recertification each time they relocate with their service member. The Military Services issued implementing policies in May and June 2019.

The DoD has also established the My Career Advancement Account program to help military spouses improve their employment opportunities. The program provides up to $4,000 in tuition assistance for education or training for eligible spouses of service members. However, the use of My Career Advancement Account program funds is restricted to the attainment of certificates, licenses, or associate's degrees in a portable career field such as auto mechanic, court reporter, firefighter, and teacher. In an April 2019 audit, the Government Accountability Office reported that, according

to DoD data, only about 21,000 military spouses (about 7 percent of eligible spouses) received tuition assistance through the My Career Advancement Account program in FY 2017. The Government Accountability Office identified various reasons why military spouses may not be participating in the program, including that the program does not cover bachelor's degrees.[36]

In addition to disrupting the military spouse's career, requiring families to relocate every few years can have an adverse effect on the service member's finances. The July 2018 Military Family Advisory Network survey found that participants said the amount of money they paid out of pocket to relocate was often more than what could be reimbursed. Some respondents said they go into debt every time they move. Others said they try to mitigate the costs of a permanent change of station move by saving for months ahead.

Added to the financial strain is the worry about the move itself, including loss and breakage of personal property during the move. The DoD OIG is performing an audit to determine whether service members received personal property shipments in a timely manner and whether actions were taken on household goods that were damaged or lost during permanent change of station moves.

CONCLUSION

In summary, the DoD must ensure the welfare and well-being of service members and their families. To ensure readiness and that military members can perform their critical missions, the DoD must provide service members and their families with, among other things, adequate housing, access to suicide prevention programs, affordable and quality child care, and help for spousal employment.

[36] Report No. GAO-19-320R, "Military Spouse Employment: Participation in and Efforts to Promote the My Career Advancement Account Program," April 9, 2019.

Gunnery Sergeant evaluates officer candidates during close order drill at Marine Corps Officer Candidates School aboard Marine Corps Base Quantico, Virginia, June 21, 2019. (U.S. Marine Corps photo)

Challenge 4. Ensuring Ethical Conduct

Maintaining high ethical standards and ensuring appropriate accountability for any misconduct is critical to the mission of the DoD. Ethical misconduct can undermine the American public's trust in the DoD, the DoD's ability to secure congressional support and funding, and the DoD's ability to execute its mission. Ensuring ethical conduct throughout all levels of the DoD is a constant challenge that requires continuous and comprehensive approaches to training and educating, conducting timely and fair investigations, and timely actions to hold DoD personnel accountable when appropriate.

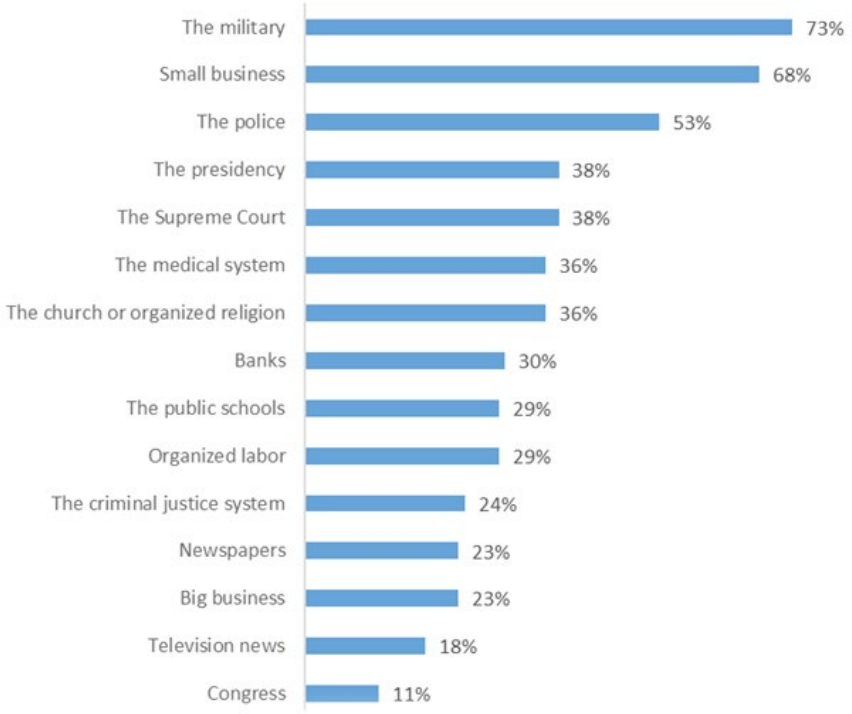
Surveys of public opinion show that the military is the most highly trusted public institution in the United States. As shown in Figure 4, a June 2019 Gallup poll on confidence in institutions found that more than 70 percent of Americans have a great deal of trust in the military, which is higher than most other institutions.

Chairman of the Joint Chiefs of Staff and former Army Chief of Staff, General Mark Milley recently spoke to the DoD OIG staff regarding the importance of ethical conduct in maintaining trust in the military, stating, "It is incumbent upon us, the military . . . to have the trust and confidence of the American people. It is so critical. If we lose that trust and confidence, then we have lost everything."

Similarly, in an August 19, 2019 memorandum on "Reaffirming Our Commitment to Ethical Conduct," Secretary Esper stated:

> [E]thics is integral to our three lines of effort. Ethical leadership that builds principled, self-disciplined teams, strengthens readiness, and improves lethality. Our shared ethical values strengthen alliances and attract new partners. Ethicsbased standards and accountability are fundamental to business reforms, and to keeping faith with our Service Members and their families.

Figure 4. Percentage of Respondents With a Great Deal or Quite a Lot of Confidence by Institution in 2019



Source: Gallup.

ETHICAL CONDUCT IN THE DOD

Federal law, the Uniform Code of Military Justice, and other policies describe standards of ethical conduct for the military, civil servants, and contractors supporting the DoD. The DoD OIG generally groups ethical misconduct by DoD personnel into the following five broad subcategories.

- **Personal Misconduct or Ethical Violations.** Inappropriate relationships, matters of dignity and respect, inappropriate gifts, misuse of position, misuse of a subordinate's time, and endorsement of a non-Federal entity. In this category, sexual assault is a persistent problem within the DoD.
- **Misuse of Government Resources.** Misuse of Government supplies, facilities, equipment, or Morale Welfare and Recreation services; and misuse of Government vehicles.
- **Travel Violations.** Unauthorized use of military aircraft for primarily personal reasons or for family or friends; improper upgrades on commercial flights or rental cars at the Government's expense; hotels in excess of per diem without adequate justification; and official travel for primarily personal reasons.
- **Personnel Matters.** Improper hiring, prohibited personnel practices, harassment, and discrimination.
- **Other Matters.** Misconduct not covered in the four principal categories above, such as improper procurement or contracting and security violations.

ONGOING EFFORTS TO ENSURE ETHICAL CONDUCT

DoD service members, employees, and contractors are advised of DoD ethical standards upon application for employment, whether civilian, contractor, or military. Ethics counselors are available to assist employees in understanding their ethical obligations and any gray areas related to ethical guidelines, laws, and regulations.

Chairman of the Joint Chiefs of Staff and former Army Chief of Staff, General Milley, while discussing the importance of ethical conduct with the DoD OIG, noted the role of Inspectors General in ensuring ethical conduct. He stated,

> Domestically, we [the military] are the most trusted institution in U.S. society. That is, in large part, because we maintain discipline and accountability within ourselves, but also because we have a watchdog group built in–it's called the Inspectors General—that is so important, and I can't underline that enough.

IGs receive allegations of misconduct, waste, fraud, and abuse through a variety of sources, including from whistleblowers, who must be protected from reprisal for their protected disclosures. Section 7 of the Inspector General Act of 1978 prohibits disclosure of whistleblowers' identities without their consent, except when unavoidable during the course of an investigation, and it also prohibits reprisal against employees for disclosing wrongdoing.

The Whistleblower Protection Enhancement Act of 2012 added a requirement that IGs designate a Whistleblower Protection Ombudsman, which in 2018 was converted to the Whistleblower Protection Coordinator. The full-time responsibilities of the DoD OIG's Whistleblower Protection Coordinator are to educate DoD employees and contractors on their rights, remedies, and avenues to report allegations, and also to educate management on their responsibilities to abide by the laws and regulations that protect whistleblowers from retaliation for making a protected communication.

The DoD OIG Hotline provides a confidential means for anyone to report allegations of ethical violations without fear of reprisal. The DoD Hotline receives approximately 14,000 complaints annually. The Military Service IGs and DoD Component IGs also operate hotlines as separate avenues for service members, employees, contractors, and others to report misconduct. Protecting and empowering whistleblowers who report violations can expose misconduct; demonstrate the DoD's commitment to deterring waste, fraud, and abuse; and address ethical misconduct.

The DoD OIG, Service IGs, and Component IGs also provide regular training to DoD personnel regarding ethics. For example, the DoD OIG proactively trains senior military officials and members of the Senior Executive Service (SES) about potential misconduct. The DoD IG speaks to each Advanced Professional Executive (APEX) class of new senior executives, as well as to more experienced SES leaders at the Vanguard course. The DoD IG also speaks to every CAPSTONE class of new general officers about the work of the DoD OIG, Service IGs, and Component IGs; ethical issues these new leaders will face; types of actions to avoid, including reprisal if there is a complaint against them; and other potential ethical minefields. In addition, the DoD OIG publicly releases, when appropriate, reports of investigation, particularly in substantiated cases when the matters involve issues of significant public concern.

Service IGs pursue similar education and training initiatives on ethics. For example, the Service IGs provide ethics training at various senior leader forums, such as the Army IG Senior Official Front Office Exportable Training Package and the Air Force Senior Leader Orientation Course. In addition, the Naval IG speaks to newly promoted flag officers and captains yearly to provide them with examples of unethical behavior from recent Navy cases, and the Marine Corps IG conducts ethics training at professional military education schools for all grades within the Marine Corps.

In other examples of efforts to ensure ethical conduct throughout the DoD, the Naval War College established the Naval Leadership and Ethics Center, which seeks to prepare commanders and their support teams to avoid ethical lapses. The Joint Staff IG conducts Staff Assistance Visits at combatant commands, where teams of subject matter experts review a variety of ethical issues in order to help commanders identify and avoid ethical pitfalls. Other DoD Component agencies have developed Jeopardy-style ethics training that allows employees to learn ethics in an entertaining and interactive manner. The Defense Prisoners of War/Missing in Action Accounting Agency sends monthly scenarios to all employees that depict common ethical dilemmas and provides detailed responses. The Defense Contract Audit Agency uses ethics podcasts for employees to use for annual ethics training. The Defense Finance Accounting Service meets individually with all senior executives to offer them the chance to discuss any ethics questions they may have. The Defense Logistics Agency uses a "Leader-Led, ValuesBased" ethics training where commanders train the troops. Each of these examples highlights how the DoD tailors its training to all levels of personnel and different environments throughout the DoD.

CURRENT TRENDS IN ETHICAL MISCONDUCT

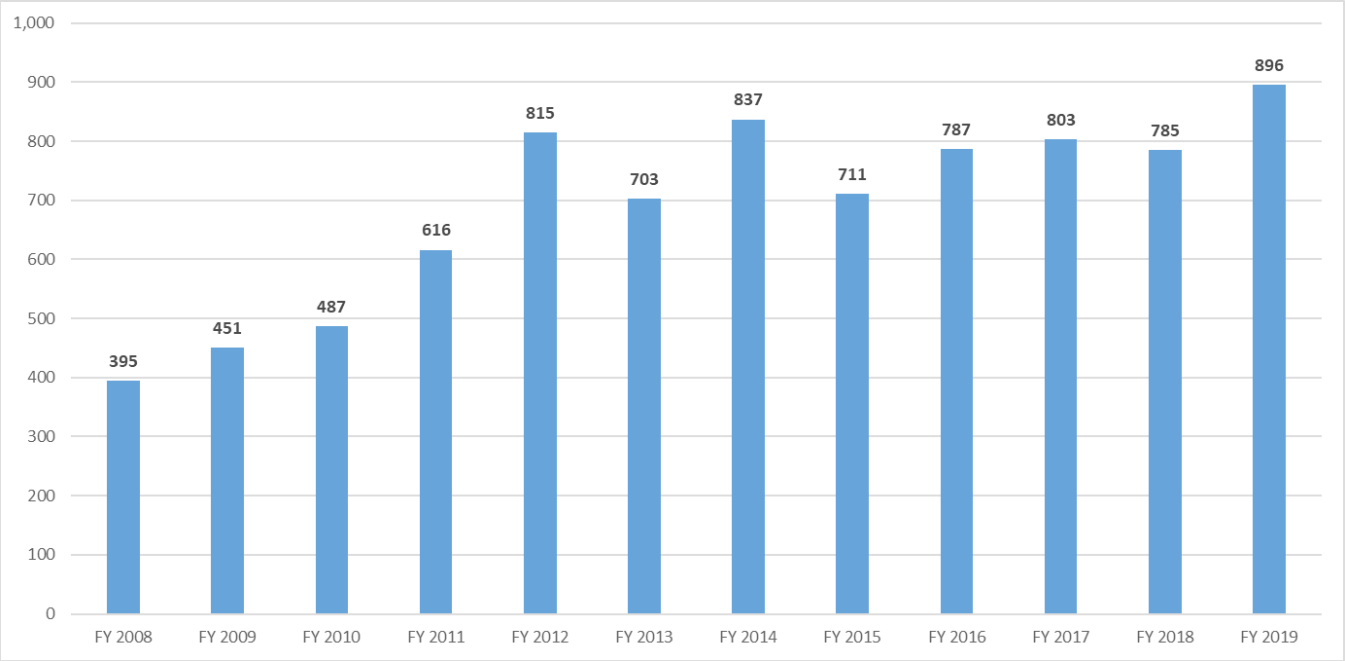
Despite the education and training and the messages from DoD leadership regarding the importance of ethical conduct, misconduct will still occur in an organization as large as the DoD. While ethical leadership starts at the top, ethical conduct is the responsibility of all personnel in the DoD. Even a few instances of misconduct can affect confidence in the integrity of the DoD and its Components.

The DoD OIG, the Service IGs, Component IGs, and commanders therefore seek to investigate allegations of misconduct thoroughly, fairly, and in a timely manner. Investigations of alleged misconduct are conducted by IG offices, Component heads, commanders or their designees, offices of general counsel, and through a wide array of formal command-directed investigators. The DoD OIG investigates, and conducts oversight reviews of, senior official investigations and reprisal investigations conducted by Service IGs and other DoD Components. In addition to these administrative investigations, the DoD investigates criminal misconduct by DoD personnel and those receiving contracts and grants from the DoD.

INVESTIGATIONS OF SENIOR OFFICIALS

Conducting timely and thorough investigations of senior official misconduct is a significant challenge and important priority within the

Figure 5. Misconduct Complaints Against Senior Officials FY 2008 Through FY 2019



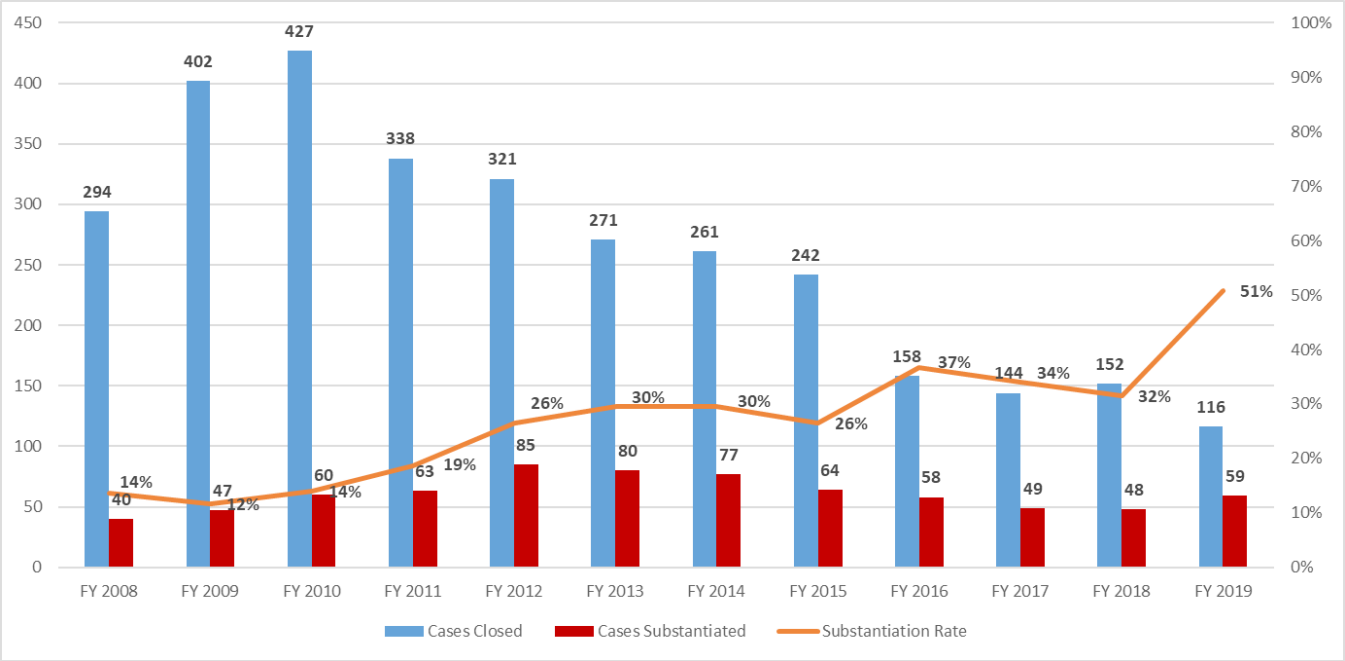
Source: The DoD OIG.

DoD. DoD senior officials include SES members, general officers, and those officers promotable to general officer. Failing to appropriately address senior official misconduct can lead to an erosion of trust in the DoD and can impact the leadership of the DoD.

As demonstrated in Figure 5, the number of senior official misconduct complaints increased significantly between FY 2008 and FY 2012 and has remained relatively constant since then. From FY 2008 to FY 2012, the overall number of complaints of senior officials increased from 395 to 815. Since FY 2012, the number of complaints has remained fairly stable, fluctuating between 700 and nearly 900 complaints per year.

To handle incoming allegations more timely and thoroughly, the DoD OIG has reallocated significant resources to its administrative investigations component to review incoming complaints. The DoD OIG has also modified the complaint intake process to include more investigative work in the complaint intake process, also known as complaint clarification, to improve the assessment of when it is necessary to conduct formal investigations. Through this complaint clarification process, the DoD OIG has resolved many allegations that were not supported by the evidence. This has resulted in an increase in the number of complaints resolved during the intake process.

Figure 6. Number of Formal Senior Official Misconduct Cases, Substantiated, and Substantiation Rates for FY 2008 Through FY 2019



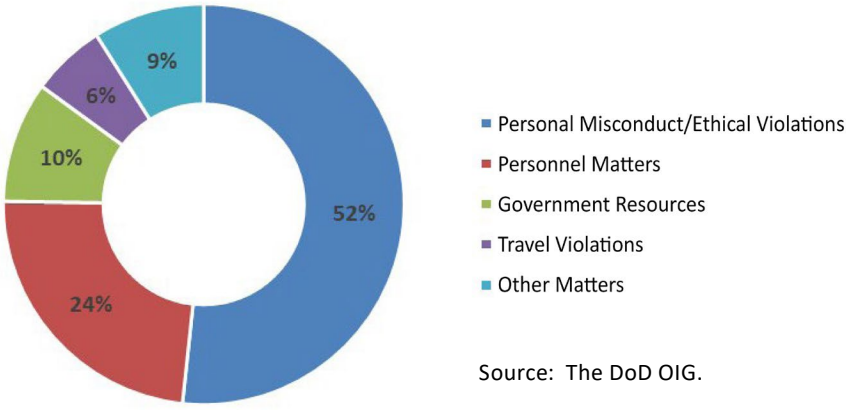
Source: The DoD OIG.

As shown in Figure 6, the number of senior official investigations decreased from 152 in FY 2018 to 116 in FY 2019, a decrease of 23.6 percent. At the same time, the substantiation rate increased from 32 percent in FY 2018 to 51 percent in FY 2019.

Overall, the number of substantiated senior official cases has declined since its peak of 85 substantiated investigations in FY 2012 to 59 in 2019. To put this number in context, there are more than 2,000 senior officials throughout the DoD.

The majority (52 percent) of substantiated misconduct cases from FY 2015 through FY 2019 were related to personal misconduct and ethical violations. These cases consisted of a variety of misconduct, including inappropriate relationships, matters of dignity and respect, inappropriate gifts, misuse of position, misuse of a subordinate's time, and endorsement of a non-Federal entity. Figure 7 shows the breakdown of the substantiated misconduct from FY 2015 through FY 2019 among five broad sub-categories of misconduct—personal

Figure 7. Substantiated Allegations of Senior Official Misconduct FY 2015 Through FY 2019



Source: The DoD OIG.

misconduct and ethical violations, personnel matters, Government resources, travel violations, and other matters.

While the trend since FY 2012 has been a decrease in substantiated allegations of misconduct, even one instance of misconduct is too many, and any substantiated case can have an impact on the DoD. Recent cases of substantiated DoD senior official misconduct include the following examples.

- The Assistant to the Secretary of Defense for Public Affairs misused subordinates' time to conduct personal services for her and accepted gifts from her subordinates.
- A Navy SES member wasted Government resources by conducting official travel for primarily personal reasons—specifically, for two family vacations in Hawaii—and conducted minimal or no official work during official travel to New Orleans, Louisiana; New York, New York; Okinawa, Japan; Key West, Florida; Rota, Spain; Iwakuni, Japan; and Saratoga Springs, New York.
- A Marine Corps brigadier general created a negative work environment through disparaging and bullying treatment of personnel, and devaluing women, which led to distrust in his impartiality and leadership.
- An Army National Guard brigadier general misused Government resources when he visited pornographic websites from his Government cell phone.
- A DoD SES member misused his public office for his friend's private gain and gave preferential treatment to that friend when he paid his friend's contracting firm to teach a writing and leadership class.
- A DoD SES member engaged in sexual relations numerous times with a subordinate during official travel and in his office during the duty day. Additionally, instead of recusing himself as required by agency standards, this member approved two favorable personnel actions benefitting the subordinate in question.

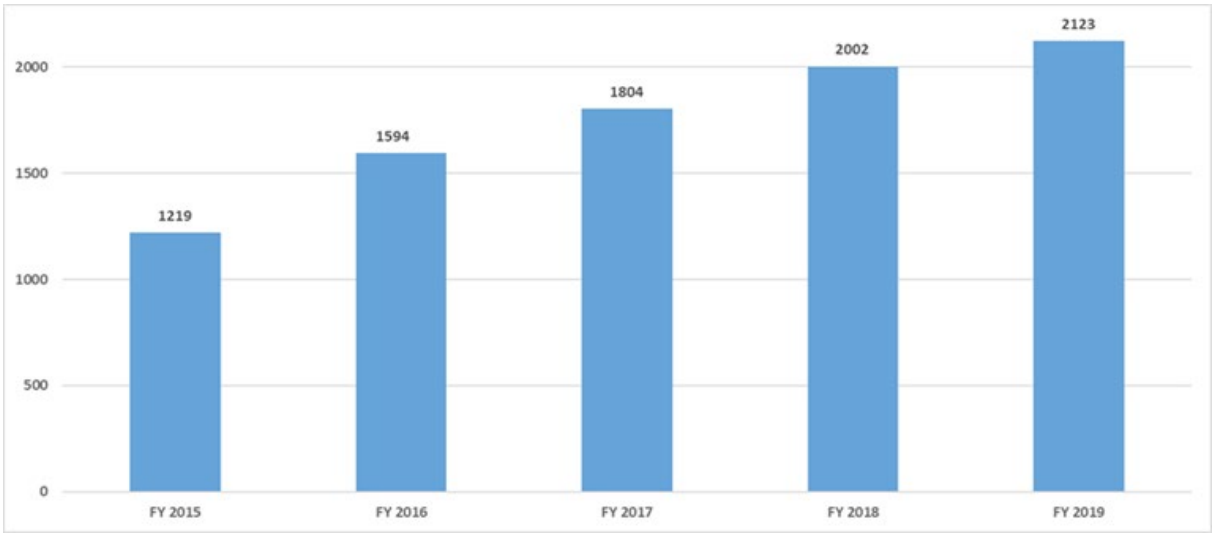
INVESTIGATIONS OF WHISTLEBLOWER REPRISAL AND RESTRICTION

Conducting whistleblower reprisal investigations is an important and challenging role for the IGs within the DoD. Whistleblower reprisal occurs when an individual or entity takes, threatens, or fails to take an action against a whistleblower in retaliation for having made a protected disclosure regarding various statutorily specified forms of wrongdoing to an authorized recipient. Whistleblower restriction occurs when someone attempts to prevent a military member from communicating with an IG or a Member of Congress.

The number of whistleblower reprisal and restriction complaints has steadily increased for several years. In FY 2019, the DoD received 2,123 complaints of reprisal and restriction, a 74-percent increase from the 1,219 complaints received in FY 2015. Figure 8 shows the number of complaints received DoD-wide from FY 2015 through FY 2019.

While the number of whistleblower reprisal and restriction complaints has steadily risen over the past 5 fiscal years, the substantiation rate has remained relatively constant. Between FY 2015 and FY 2019, the substantiation rate has remained in the range of 12 to 15 percent. Figure 9 shows the number of reprisal and restriction investigations closed within

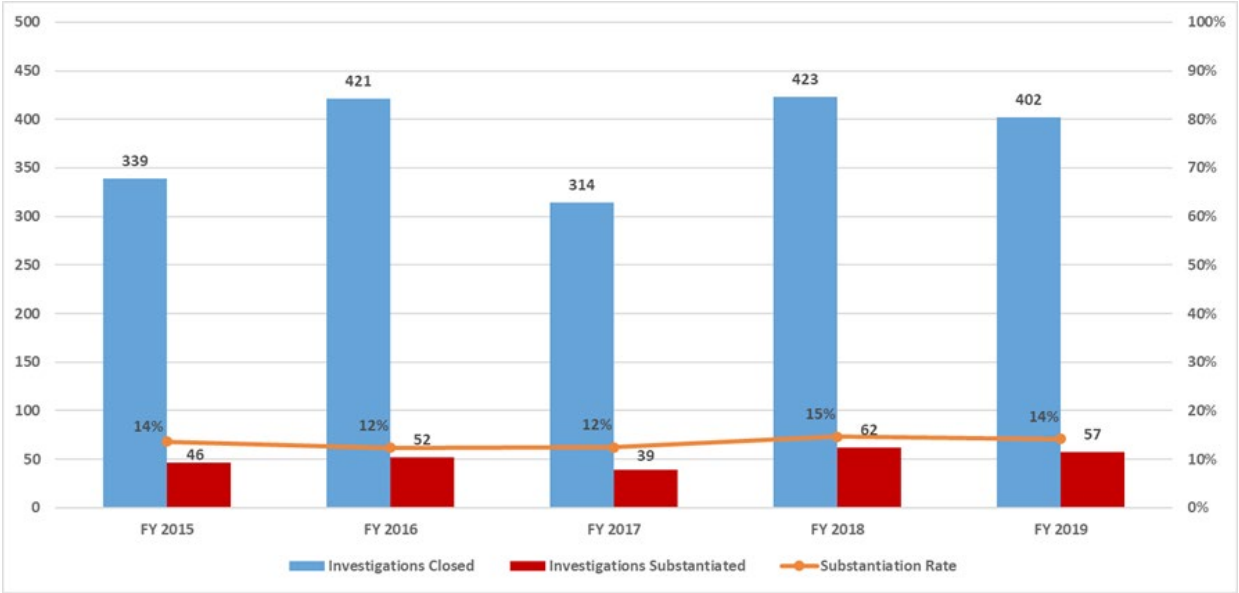
Figure 8. Number of Reprisal and Restriction Complaints Received FY 2015 Through FY 2019



Source: The DoD OIG

Note: The totals include complaints received directly by the DoD OIG and those reported by the Service and Component IGs to the DoD OIG. Source: The DoD OIG.

Figure 9. Number of DoD-Wide Reprisal and Restriction Investigations Closed and Substantiated, and Substantiation Rates FY 2015 Through FY 2019



Source: The DoD OIG.

the DoD in each fiscal year, the number of substantiated complaints, and the annual rate of substantiation.

To address the larger number of reprisal and restriction complaints, the DoD OIG increased the number of investigators conducting and oversighting these investigations. In addition, the DoD OIG has implemented an alternative dispute resolution (ADR) program, which offers complainants and their managers the opportunity to voluntarily resolve allegations of retaliation more swiftly than typically occurs in the more lengthy investigative process. Since the establishment of the DoD OIG ADR program in September 2017, over 110 cases have resulted in mutually agreed-upon resolutions, allowing investigators to focus on conducting investigations into allegations that were not resolved through the ADR program. Resolution through settlements can also result in more timely remedies. Instead of waiting for remedial action in response to recommendations made in a report of investigation, complainants are made whole upon resolution through the ADR process.

The DoD OIG Whistleblower Reprisal Investigations Directorate has also implemented process and policy changes to further enhance the efficiency and effectiveness of whistleblower reprisal investigations across the DoD. These changes include process efficiencies being implemented by the DoD OIG and service IGs during the complaint intake and investigation stages and the use of summary reports of investigation for straightforward, unsubstantiated cases. For example, summary reports are used when the evidence shows that a personnel action was taken for well-documented reasons unrelated to a protected communication. The DoD OIG is also reissuing regulations to help streamline and standardize the whistleblower reprisal investigative process.

These measures have resulted in the DoD OIG and Service IGs decreasing the time it takes to complete reprisal investigations. For example, at the close of FY 2018, the average days in investigation of open DoD OIG reprisal investigations was 356 days; at the close of FY 2019, it was 82 days. However, the Service IGs have struggled to address their increasing caseloads because, in general, resources for Service IGs have not significantly increased. As a result, the Service IGs still have a considerable backlog of aged cases, with 23 percent of their open whistleblower reprisal investigations being over 1 year old, compared to none over 1 year old for the DoD OIG.

Recent substantiated DoD whistleblower reprisal and restriction investigations include the following examples.

- An Air Force major and a first lieutenant issued a subordinate staff sergeant an adverse letter of counseling in reprisal for telling members of the chain of command about unprofessionalism and toxic leadership displayed by two detachment technical sergeants during a group counseling session.
- A Marine Corps lieutenant colonel threatened a Navy subordinate lieutenant with disciplinary action and requested a retaliatory command directed investigation in reprisal for making lawful communications to an IG and a Member of Congress regarding attitudes about sexual assault in the Service.
- Two Federal employees working for the U.S. Intelligence Community suspended a Navy lieutenant's access to classified information in reprisal for the lieutenant's complaint to a supervisor that the one of them violated Executive Order 12333, which regards U.S. intelligence agencies

and the ways in which Federal agencies are to cooperate with certain requests for information.

- A defense contractor to U.S. Army Special Operations Command placed a company employee on a temporary administrative leave of absence without pay in reprisal for reporting violations of law and abuse of authority to IGs and a contracting officer's representative.
- A civil service GS-15 told an Air Force staff sergeant and other subordinates that he had survived IG investigations in the past and implied that nothing would happen to him as a consequence of future complaints, in an attempt to restrict them from preparing or making protected communications to the IG.

When cases are substantiated, it is important for management to take prompt corrective action, particularly when whistleblowers have suffered from reprisal. Failure to take prompt and appropriate corrective action to make the whistleblower whole and to hold the reprising official accountable has the potential to deter other whistleblowers from making protected disclosures in the future.

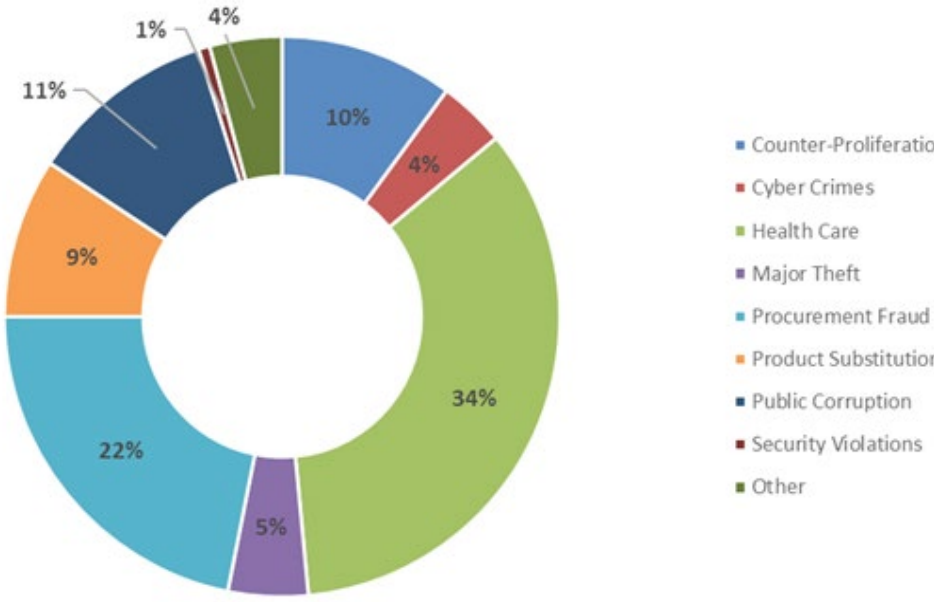
CRIMINAL INVESTIGATIONS

In addition to administrative investigations of ethical misconduct, the DoD OIG, through its criminal investigative component (the Defense Criminal Investigative Service [DCIS]), and other military criminal investigative organizations conduct criminal investigations related to DoD programs and operations. These investigations involve the full range of criminal actions, including sexual assault, procurement fraud, public corruption, product substitution, health care fraud, illegal technology transfer, and cybercrimes.

DCIS focuses its efforts on the following types of criminal investigations.

- **Procurement and Acquisition Fraud.** Defective, substituted, counterfeit, or substandard products that impact crucial DoD programs and operations or result insignificant financial losses to the DoD, with particular emphasis placed upon matters that affect the health, safety, welfare, or mission-readiness of U.S. warfighters and combat units.
- **Corruption and Financial Crimes.** Bribery, kickbacks, money laundering, conflicts of interest, gratuities, and embezzlement that undermine the integrity of the DoD enterprise, and erode public trust and confidence in DoD institutions and programs.
- **Health Care Fraud.** Allegations of patient harm to TRICARE beneficiaries or a loss to the Defense Health Agency.
- **Theft and Illegal Proliferation of Sensitive DoD Technology.** Allegations involving individuals and entities likely to use the technology to the detriment of DoD personnel, facilities, and materiel.
- **Computer Intrusions and Other Cybercrimes.** Compromise the integrity, reliability, or availability of the DoD Information Network; exfiltration, damage, or compromise of sensitive DoD operational, programmatic, or technical data; compromise of personally identifiable information or health records pertaining to civilian DoD employees or service members; or potential contractual violations on the part of a DoD contractor

Figure 10. Percentage of DCIS Cases Initiated by Type FY 2015 Through FY 2019

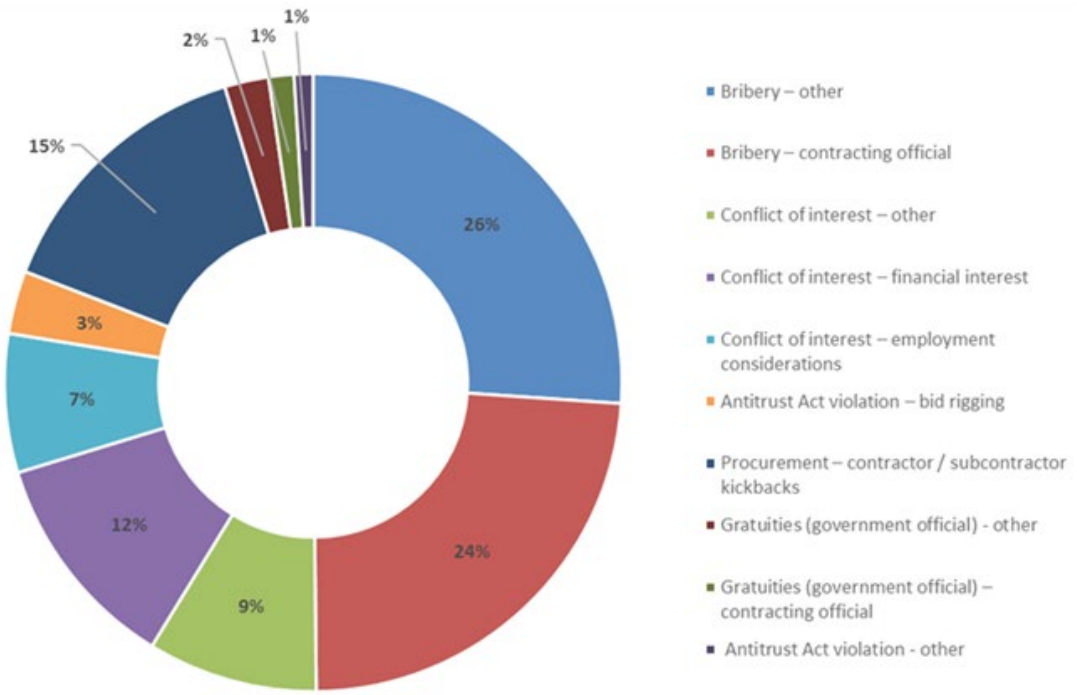


Source: The DoD OIG.

Figure 10 shows the breakdown of the criminal investigations initiated by DCIS from FY 2015 through FY 2019. Over half of the DCIS investigations were related to either health care fraud (34 percent) or procurement fraud (22 percent). Public corruption cases were an additional 11 percent of the criminal investigations opened from FY 2015 through FY 2019.

Between FY 2015 and FY 2019, DCIS closed 304 cases related to public corruption, which included criminal offenses related to bribery, kickbacks, money laundering, conflicts of interest, gratuities, and embezzlement that undermine the integrity of the DoD and erode public trust and confidence in the DoD and its programs.

Figure 11. Closed DCIS Public Corruption Cases for FY 2015 Through FY 2019



Source: The DoD OIG.

As shown in Figure 11, half of the public corruption investigations closed between FY 2015 and FY 2019 concerned bribery. In FY 2019, public corruption investigations by DCIS resulted in 26 criminal charges and 29 convictions, over $245 million in recoveries for the Government, and the debarment of 15 entities from Government contracting.

DCIS and the military criminal investigative organizations also conduct fraud awareness briefings for both Government and contractor procurement officials, legal counsels, agency heads, auditors, law enforcement officials, and other individuals in key management positions to help prevent criminal actions and also to provide information on how to report criminal activity within the DoD. The briefings also provide information on how to recognize illegal activity involving procurement fraud, public corruption, and bribery. In FY 2019, DCIS personnel briefed over 14,900 officials on these issues.

Recent DoD criminal investigations involving public corruption include the following examples.

- A DCIS joint investigation with the FBI and the General Services Administration investigated allegations that two former Aviation and Missile Command employees used their positions and Army funds to fraudulently procure power tools and other equipment through the General Services Administration Advantage program, and they sold the items, worth approximately $2.3 million. Both former employees pleaded guilty to one count of conspiracy to commit mail and wire fraud. One former employee was sentenced to 33 months in prison and 3 years of supervised release, and the other was sentenced to 6 months in prison and 3 years of supervised release.

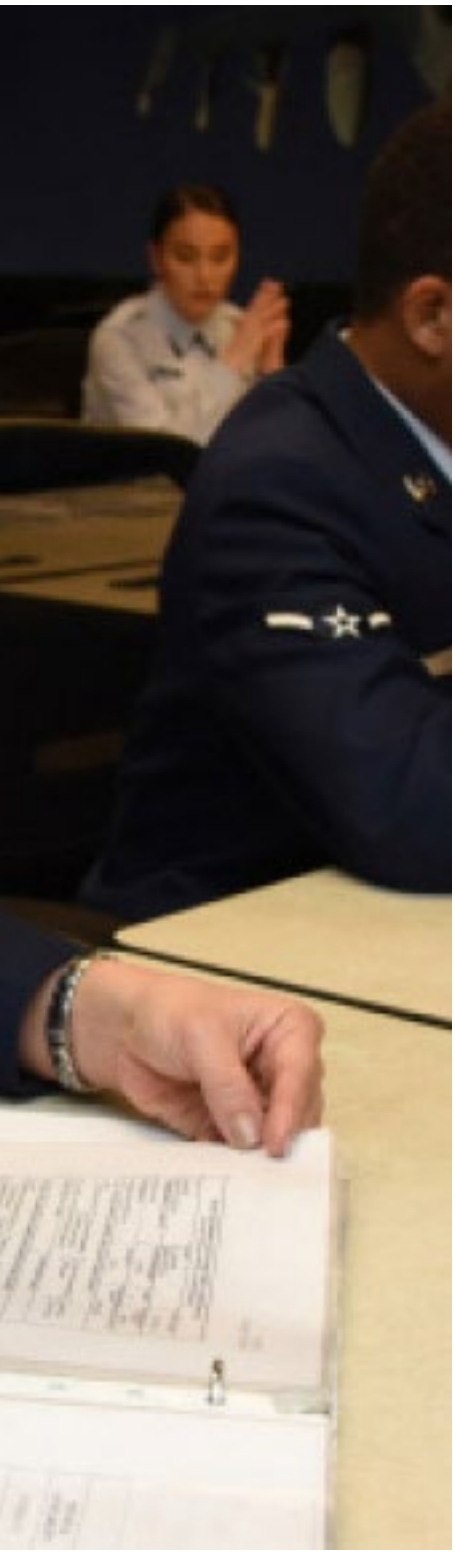
- A DCIS joint investigation with the Naval Criminal Investigative Service involved a former civilian employee of the Navy serving as a senior procurement official for Naval Base Ventura County who received $1.2 million in illegal kickbacks and was sentenced to 70 months in Federal prison. The former employee worked for 22 years as the master scheduler for the Public Works Department at the naval base where he was responsible for approving materiel purchases, service contracts, vendors, and payments to vendors.

Data analysis is a critical aspect of many criminal investigations. DCIS conducts a wide variety of investigations involving health care fraud in the DoD TRICARE system, including investigations of health care providers involved in corruption or kickback schemes, and overcharging for medical goods and services. DCIS collaborates with the DoD OIG Data Analytics Directorate and the Defense Health Agency to develop data analytic tools to identify relationships between potential criminal actors identifying health care fraud. For example, data analytics has been used to identify outliers in the opioid claims data that included the names and locations of the medical professionals and pharmacies prescribing and dispensing opioids at excessive and unjustified levels.

DCIS also coordinates with other Federal agencies and participates in Federal and state task forces. For example, DCIS partnered with the Department of Justice and the Defense Health Agency to establish a data analytical tool to identify and combat a $1.5 billion pharmaceutical scheme. Numerous DCIS health care investigations resulted in hundreds of millions of dollars being returned to the DoD, as well as the convictions of multiple pharmacists, prescribers, marketers, and Federal health program beneficiaries.

In summary, ensuring ethical conduct is essential to maintaining trust in the DoD. By deterring and detecting misconduct, the DoD is better able to justify the funding it needs to fulfill its responsibilities and perform its challenging mission both appropriately and effectively.

A U.S. Air Force Technical Sergeant, 334th Training Squadron student, reviews aviation resource management apprentice course study material inside Wolfe Hall at Keesler Air Force Base, Mississippi, February 26, 2019. (U.S. Air Force photo)



Challenge 5. Financial Management: Implementing Timely and Effective Actions to Address Financial Management Weaknesses Identified During the First DoD-Wide Financial Statement Audit

The DoD OIG oversaw and conducted the first full-scope financial statement audit of the DoD in FY 2018, as required by statute. The DoD received a disclaimer of opinion from the audit. The lack of a favorable audit opinion on the DoD financial statements is the major impediment to a successful audit of the U.S. Government. However, the critical importance of the full audit was not the ultimate opinion, but was contained in the findings and deficiencies that the auditors identified and in the DoD's commitment to addressing those deficiencies.

However, the audit reiterated that longstanding financial management challenges continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information to support reported financial statement balances. Additionally, the lack of reliable financial information impacts the DoD's operating, budgeting, and policy decisions.

In their September 2017 notification of audit readiness to the DoD Inspector General, the Secretary of Defense and the DoD Chief Financial Officer stated that they expected to receive actionable feedback on various financial areas, including existence, completeness, and valuation of certain assets, as a result of the FY 2018 financial statement audits. Even though the DoD and its Components did not receive favorable audit opinions, the auditors—from the DoD Office of Inspector General (OIG) and from independent public accountants overseen by the DoD OIG—provided actionable feedback during the FY 2018 audits through notices of findings and recommendation (NFRs). Auditors provide these notices to communicate to management the weaknesses the auditors identify, the impact of these weaknesses on the financial management processes, the reasons the weaknesses exist, and recommendations to management for correcting the weaknesses. As a result of auditor site visits, testing, and reviews of DoD documents, the auditors issued 2,578 NFRs to the DoD and its Components on the weaknesses in the DoD's accounting and business processes, financial reporting, and information technology systems.

Auditors classify weaknesses and inefficiencies in financial processes based on the severity of the weakness. A material weakness is defined as a deficiency or a combination of deficiencies in internal control over financial reporting that result in a reasonable possibility that management will not prevent, or detect and correct, a material misstatement in its financial statements before issuing the financial statements. In its FY 2018 financial statement audit opinion, the DoD OIG identified 20 DoD-wide material weaknesses, such as Financial Management Systems and Information Technology; Universe of Transactions; Inventory; Property, Plant, and Equipment (PP&E); Fund Balance With Treasury; and Financial Statement Compilation.

The DoD OIG also issued a report after the audit was completed, titled, "Understanding the Results of the Audit of the DoD FY 2018 Financial Statements." The purpose of the report was to summarize the purpose, findings, and potential benefits of the DoD's financial statement audits in terms understandable to non-auditors. In the report, the DoD OIG noted that the DoD's material weaknesses involved a complex array of issues, but that DoD management is responsible for prioritizing the findings and developing corrective action plans to address the material weaknesses. Each of the material weaknesses can hinder the DoD's efforts to improve its business processes, achieve auditable financial statements, and maintain efficient and effective operations. If DoD management takes action to address the weaknesses that auditors identified, the DoD financial information would be more accurate, and business processes and operations would become more effective and efficient.

It is critical that the DoD and its Components fix the weaknesses and deficiencies identified in the audit through the development, implementation, and monitoring of corrective action plans. In addition, the DoD must continue its commitment to the improvement of DoD business processes. While the road to a clean financial statement opinion is a long-term effort, the feedback provided through the audits and the implementation of corrective actions can help improve the DoD's operations and decision making, save money, and ensure that Congress and the public have accurate information on how the DoD's resources are being spent.

IMPORTANCE OF FINANCIAL AUDITABILITY

Audits of the financial statements of the DoD and its Components are important for a variety of reasons. They provide transparency on the DoD's use of its resources, test financial information for accuracy, evaluate information technology and cyber systems for compliance with specified requirements, and help improve DoD operations and decision making. The audits also provide Congress and the public with a transparent assessment of where the DoD spends its funds. In addition, the audit reports describe the specific weaknesses identified during the audit that need to be addressed by the DoD.

The National Defense Authorization Act for FY 2018 also requires the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, to produce a biannual Financial Improvement and Audit Remediation Plan. The Remediation Plan must describe the specific actions the DoD plans to take to address the NFRs that the auditors issue on the weaknesses in the DoD's financial reporting, business processes, and information technology systems identified in the financial statement audits.

In the most recent plan issued in June 2019, the Deputy Under Secretary of Defense (Comptroller) highlighted the audit's importance, stating:

> The audit has been a forceful catalyst for change within the department. We welcome the transparency it brings. The audit will improve our financial clarity and decision making as well as provide information that feeds modern data analytics to improve every element of how we do business.

A significant function of financial statement audits also involves reviewing information technology and cybersecurity. Many of the systems crucial to financial management and reporting are also used for operational purposes. Therefore, testing during the financial statement audits of DoD information technology systems and interfaces between information technology systems can identify vulnerabilities in those systems and result in recommendations to improve the DoD's overall cybersecurity. For example, during the FY 2018 audit, auditors issued over 1,000 information technology-related findings, and over half of the findings related to access controls. Without effective internal controls and proper cybersecurity, the systems that the DoD relies on to support military operations could be compromised, potentially undermining DoD operations. As a result, the DoD developed four DoD-wide initiatives to remediate access controls.

In addition, financial statement audits can help DoD management improve its operations. The audits provide feedback regarding the effectiveness of each reporting entity's business systems, processes, and controls. Improved business systems, processes, and controls can assist the DoD in more accurately forecasting and determining the most efficient and effective uses of its funds. On May 16, 2019, in his role as the Under Secretary of Defense (Comptroller)/ Chief Financial Officer, DoD, David L. Norquist testified before the House Armed Services Committee that the audit has become an integral tool in enabling defense personnel to identify and correct problems, and that the audits can improve operational decision making throughout the DoD.

For example, during a Navy material accountability exercise to address multiple financial statement findings from FY 2018, the Navy discovered $504 million worth of material to date, at multiple locations that were not in the system of record. As a result of finding these items, over $167 million has been added to the Navy supply system, which has been used to fill over 3,400 requisitions totaling $36.6 million.

In short, the financial statement audits can enable improvements to operations through more efficient business systems, processes, and controls, and they can result in more accurate and consistent information from the DoD Components.

RESULTS OF THE FY 2018 DOD AGENCY-WIDE AND COMPONENT FINANCIAL STATEMENT AUDITS

This section discusses the specific results of the audit of the DoD's FY 2018 financial report, which presents the consolidated financial information for 63 DoD entities. When performing a financial statement audit, auditors can express one of four potential results on the financial statements.

- **Unmodified Opinion.** Expressed when the auditor concludes that the financial statements are presented fairly and in accordance with accounting standards.
- **Qualified Opinion.** Expressed when the auditor concludes that there are material misstatements in the financial statements but are not significant to the overall presentation of the financial statements.

- **Adverse Opinion.** Expressed when the auditor concludes that misstatements in the financial statements are both material and significant to the financial statements.
- **Disclaimer of Opinion.** Expressed when the auditor is unable to obtain sufficient appropriate audit evidence on which to base an opinion.

The DoD OIG oversaw the audits of 21 DoD Component financial statements, and also performed the audit of the FY 2018 DoD Agency-Wide Basic Financial Statements. As reflected in Table 2, of the 21 Component audits, 5 Components received unmodified opinions, 1 Component received a qualified opinion, and 15 Components received disclaimers of opinion.

As a result of the DoD Component FY 2018 audits, on November 15, 2018, the DoD OIG issued a disclaimer of opinion on the FY 2018 DoD Agency-Wide Basic Financial Statements.

As noted above, in the course of performing financial statement audits within the DoD Components, the auditors issued 2,578 NFRs related to the DoD's financial statements.

Table 2. FY 2018 Financial Statement Opinions for DoD Reporting Entities

Reporting Entity	Opinion
U.S. Army Corps of Engineers-Civil Works	Unmodified
Defense Health Agency-Contract Resource Management	Unmodified
Military Retirement Fund	Unmodified
Army Sub-Allotted Funds	Unmodified
Defense Logistics Agency Sub-Allotted Funds	Unmodified
Medicare-Eligible Retiree Health Care Fund	Qualified
Department of the Army General Fund	Disclaimer
Department of the Army Working Capital Fund	Disclaimer
U.S. Navy General Fund	Disclaimer
Department of the Navy Working Capital Fund	Disclaimer
Department of the Air Force General Fund	Disclaimer
Department of the Air Force Working Capital Fund	Disclaimer
U.S. Marine Corps General Fund	Disclaimer
Defense Health Program General Fund	Disclaimer
Defense Information Systems Agency General Fund	Disclaimer
Defense Information Systems Agency Working Capital Fund	Disclaimer
Defense Logistics Agency General Fund	Disclaimer
Defense Logistics Agency Working Capital Fund	Disclaimer
Defense Logistics Agency Transaction Fund	Disclaimer
U.S. Special Operations Command General Fund	Disclaimer
U.S. Transportation Command Working Capital Fund	Disclaimer

Source: The DoD OIG

The NFRs were issued on a wide range of topics that impacted nearly every line on the Consolidated Balance Sheet and included 6,507 recommendations.

The DoD and its Components will be challenged to show continual progress in addressing the material weaknesses and NFRs identified by the auditors and obtaining favorable audit opinions on the DoD and its Components financial statements over the coming years.

To fix some of the issues identified within the NFRs, the DoD has established multiple corrective action plans. Corrective action plans summarize the condition, cause, and effect of the identified deficiency and the proposed management actions to correct the conditions and causes, with milestones for when the actions will be completed. However, completion of some of these corrective action plans is expected to take a few years and, as a result, the DoD may continue to receive a disclaimer of opinion on the DoD and DoD Components financial statements for several years.

To monitor the corrective action plans throughout the DoD, the DoD Deputy Chief Financial Officer developed a centralized database that allows DoD financial managers to track all of the NFRs and the status of the corrective action plans. DoD management plans to use the information in the NFR database to prepare its future Financial Improvement and Audit Remediation Reports, which describe the specific actions that the DoD plans to take to address the NFRs, interim milestones for completing these actions, and cost estimates for implementing these actions. For FY 2018, the DoD reported that $560 million went toward remediating audit findings in FY 2018.

The DoD has prioritized its remediation efforts based on what it believes will provide the greatest value to DoD operations and the warfighter. The DoD is currently focusing its key efforts on addressing deficiencies related to:

- information technology,
- real property,
- inventory and operating material and supplies, and
- Government property in the possession of contractors.

WEAKNESSES IN THE DOD FINANCIAL MANAGEMENT PROCESSES

As noted above, the DoD OIG identified 20 agency-wide material weaknesses during the FY 2018 audit and issued numerous findings and recommendations on a variety of areas related to the financial statements. Each material weakness can hinder the DoD's efforts to improve its business processes and achieve auditable financial statements, and are critically important to correct. A few of the most significant weaknesses were in the following areas.

- **Financial Management Systems and Information Technology.** The internal controls for information technology systems that process financial or financial-related transactions.
- **Universe of Transactions.** The entirety of underlying, individual, accounting transactions that support a balance or line item on the financial statements of each DoD Component.
- **Inventory.** Includes items, such as spare parts and ammunition, that are held for sale.

- **PP&E.** The identification and valuation of assets such as land, buildings, and military equipment.
- **Fund Balance With Treasury.** The checkbook for each of the Components and identifies the amount of funds available and spent through the Department of the Treasury.
- **Financial Statement Compilation.** The processes used to ensure that all of the DoD's transactions are accurately summarized and reported on its financial statement.

FINANCIAL MANAGEMENT AND INFORMATION TECHNOLOGY

For FY 2018, auditors issued over 1,000 NFRs on DoD information technology systems, including financial management systems. Ineffective system controls can result in significant risk to DoD operations and assets. For example, the absence of controls could cause improper payments, as well as inaccurate inventory and equipment records. The lack of information technology controls could also cause disruptions in critical operations, such as those supporting national defense activities.

The auditors found, for example, that:

- access rights and responsibilities were not appropriately restricted according to segregation of duties policy;
- user access was not terminated in a timely manner when the user left the organization;
- DoD Components were not monitoring sensitive user activities, including activities of privileged users; and
- controls had not been implemented to identify unintentional or unauthorized changes made to applications, databases, or data.

In addition, the DoD continues to struggle to confirm that controls exist to ensure that DoD data is shared completely and accurately between systems, and auditors continue to identify control weaknesses related to the processes of sharing information between financial related systems.

The DoD is pursuing several initiatives to address weaknesses related to the information technology systems. For example, personnel from the Office of the Deputy Chief Financial Officer and the Office of the Chief Information Officer are coordinating on a long-term solution to address controls at the enterprise level using automated processes. While developing the long-term process, the DoD Components are also implementing short-term solutions to correct deficiencies noted by the auditors, such as deficiencies in access controls.

UNIVERSE OF TRANSACTIONS

The DoD's inability to produce a complete, accurate, and reconcilable universe of transactions, which is the fundamental starting point for all financial statement audits, continues to be a significant roadblock to the DoD achieving a clean audit opinion on its financial statements. A universe of transactions is a central repository of financial transactions, such as transactions related to the DoD's inventory, property, and payroll, that are combined from multiple systems. The DoD Components must be able to identify a universe of transactions in order to support the information reported on their financial statements.

The DoD is experiencing significant challenges in providing an accurate universe of transactions due to the large number of transactions, systems, and owners of the financial data. For example, U.S. Special Operations Command requires the

consolidation of financial transactions from 12 systems owned by other DoD Components to support balances reported on its financial statements. In addition, most of the DoD's systems do not communicate with one another, and DoD personnel are therefore required to transfer financial transactions between systems. The lack of communication between financial systems can lead to misstatements on DoD financial statements. The Office of the Under Secretary of Defense (Comptroller)/ Chief Financial Officer, DoD, has been developing a tool that is designed to consolidate millions of transactions from 25 different DoD accounting systems in one location for over 60 DoD Components. Although the universe of transactions is nearly complete for the Defense agencies, the Military Service portion is not expected to be completed for several more years.

Once fully established, the universe of transactions will provide the auditors with one location to obtain the necessary transactions to perform a financial statement audit of the DoD Components. The benefits will extend beyond the DoD's financial management goals. For example, the same data used for audits is being used to determine medical costs to assist in allocating resources in the DoD medical facilities.

INVENTORY

DoD Components own inventory that they must report in their financial statements. Inventory is tangible property used in the production of goods for sale, items used to provide a service, finished goods, and goods held for repair and eventual sale within the DoD. Inventory can be in the custody of and managed by the Military Service or the DoD Component that owns the items, or in the custody of and managed by another organization, such as a contractor or another Federal agency.

As of October 1, 2018, the DoD reported having $276 billion in inventory and related property. However, the DoD continues to have difficulty providing assurance over the existence, completeness, and valuation of inventory recorded in the financial statements. During the FY 2018 financial statement audits, for example, auditors found that items selected for testing had been moved or used, but were still in the inventory records; were found in the warehouse but not listed in the inventory records; were recorded as in good condition but were actually unserviceable; or did not have supporting documentation to demonstrate ownership.

Inadequate controls over inventory can affect DoD operations. For example, auditors determined that the Air Force had $1.5 billion of inventory in its system of record that could not be reconciled to the supporting systems. As a result, the Air Force may not have the actual inventory it thinks it has.

Furthermore, some DoD inventory is in the custody of contractors, which can lead to inaccurate accounting. For example, the Air Force did not include inventory balances from 69 contractor locations in its accounting records, resulting in a lack of accountability of its inventory. In addition, the Air Force did not reconcile the differences between the accounting records and the inventory balances reported by the contractors, which could result in misstatements in the balances. During the second quarter of FY 2019, there was over $200 million in differences noted between the Air Force accounting records and the inventory balances reported by its contractors. Without resolving the differences, the Air Force risks

improperly accounting for its inventory, which could result in buying additional inventory that is not needed or not having enough inventory when needed.

PROPERTY, PLANT, AND EQUIPMENT (PP&E)

PP&E consists of tangible assets valued at $100,000 or more at the time of purchase or construction that are intended for use by the Component that acquired or constructed the assets, and that can be used for 2 years or more. PP&E includes land, buildings, and military equipment. PP&E is the second largest category of assets on the DoD balance sheet, with a value of $759 billion reported by the DoD on the FY 2018 balance sheet.

The DoD manages an inventory of PP&E consisting of more than a 100,000 facilities located at more than 5,000 different locations. DoD Components have made progress in verifying that the PP&E exists and that the list of PP&E is complete. However, due to the quantity of the PP&E assets, the age of the PP&E, and number of locations of the PP&E, the DoD faces challenges in verifying that all assets have been recorded in the accounting records.

In FY 2018, auditors found that DoD did not account for its real property (building and structures) sufficiently. For example, auditors found that the Air Force list of facilities in the property records was not complete or accurate. Specifically, the auditors identified instances in where facilities had been physically demolished but remained on the property records and were listed as active facilities. Auditors also identified active facilities that physically existed but were not listed in the property records. Additionally, in its FY 2019 records, the Army double counted 212 real property assets by recording them in both the Army General Fund and Army Working Capital Fund records. To help remedy these inaccuracies, the DoD is requesting a 100 percent count of real property by September 30, 2019. The DoD is also revising its policy, as discussed below, on where the real property (buildings and structures) should be reported.

In addition, the DoD struggles with obtaining evidence to support how much it paid for the PP&E. This is especially difficult with historical assets, such as radar devices, communication equipment, excavating vehicles, and Vietnam War era–aircraft, because the original documentation does not exist. As a result, the DoD could not record PP&E at acquisition or historical cost, establish or support ownership of the assets, or determine the value. For example, the Army's property system of record, the Global Combat Support System-Army, does not track the historical acquisition costs of assets. The Army has a corrective action plan. The Army has developed corrective action plans that include developing a team to identify deficiencies that prevent the Army from tracking historical acquisition costs. In addition, the Army is working to publish updated policies and procedures that will establish requirements for supporting balances and identify documentation needed to support historical costs of PP&E.

The DoD must also ensure that PP&E is reported on the correct DoD Component's financial statements. This process is not straightforward due to the interdependency of the DoD Components and the use of different funds to transform military assets into special operations force assets. For example, a U.S. Special Operations Command asset can begin as a service asset and then the Command can modify the asset to create a special operations force asset. Once the asset is modified, determining who is responsible for reporting the asset becomes a challenge. In July 2018, the DoD Deputy Chief Financial Officer issued a memorandum detailing which

Component should report construction in progress and equipment. DoD Components are currently transferring their equipment to comply with this new policy.

Similarly, inaccurate and incomplete property systems can lead to wasteful replacement costs or equipment that cannot be issued when needed because the DoD does not know what equipment it has, the equipment's condition, and what equipment it needs to effectively support the readiness of its military forces. For example, at Hill Air Force Base, $53 million worth of uninstalled missile motors were listed in "not working condition." However, the auditors found that they in fact were operational. Subsequently, the Air Force was able to put them into service.

FUND BALANCE WITH TREASURY

The Fund Balance With Treasury is an account maintained by the Department of the Treasury that reflects the cash available for the DoD to spend. In other words, Fund Balance With Treasury is the DoD cash balance reported by its bank—the Department of the Treasury. Deposits and payments by DoD Components increase or decrease the balance in the account. Each DoD Component maintains its individual Fund Balance With Treasury in its respective accounting system, similar to a personal checkbook. As of October 1, 2018, the DoD reported a Fund Balance With Treasury of $580 billion.

The size of the DoD budget, the number of information systems, the amount of deposits and expenditures, and the number of accounting transactions that must be reconciled between DoD accounts and the Treasury remain a significant challenge for the DoD to accurately reflect its Fund Balance With Treasury. In addition, the DoD Components struggle with balancing their fund balance due to a complicated business process that allows them to use each other's funds. For example, both the Defense Health Program and Defense Information Systems Agency share one checkbook, known as the Treasury Index-97 Fund Balance With Treasury account, with over 60 other DoD Components. Many of these Components do not have a complete and documented reconciliation process, which means that they cannot confirm that payments and collections are accurately recorded in the Fund Balance With Treasury account. Without an accurate checkbook balance, these Components could make spending decisions that could result in an over- or under-utilization of their funds.

Similar to balancing a personal checking account with a bank statement, a key internal control for Fund Balance With Treasury is balancing the available funds against the bank statement from the Department of the Treasury to ensure that all deposits and payments are accounted for. Each month, the DoD Components have the critical task of reconciling their available funds with statements from the Department of the Treasury. Although this may appear to be a relatively easy process, it is not due to the significant number of transactions processed by DFAS. In FY 2018, DFAS reported that it processed 135.6 million pay transactions, made 6.2 million travel payments, and paid 13.7 million commercial invoices. Auditors continue to find deficiencies in the DoD's process to routinely reconcile these accounts and resolve discrepancies. For example, a DoD OIG audit report issued in May 2018 determined that billions of dollars in collection and disbursement actions could not be assigned to a DoD Component, because these transactions were missing a limit or because the limit was invalid.[37]

[37] Report No. DODIG-2018-120, "Treasury Index 97 Cash Management Report," May 23, 2018.

As result, auditors issued over 60 findings on the Fund Balance With Treasury accounts of the DoD and its Components. Due to the continued audit findings related to Fund Balance With Treasury for the DoD Components, the auditors cannot verify the completeness and accuracy of this balance. More important, the DoD continues to make spending decisions without knowing the accurate balance of funds available with the Treasury. Without a proper accounting of its available funds, the DoD's spending decisions could result in over- or underutilization of its appropriation. For example, if a DoD Component believes that it will overspend its appropriation, it might not hire sufficient staff, make needed repairs, or maintain critical equipment. Conversely, if a DoD Component believes that it will underspend its appropriations, it could spend more funds than available, which could result in an Antideficiency Act violation.

FINANCIAL STATEMENT COMPILATION

An effective process for compiling financial statements is critical to ensuring that the DoD Components accurately summarize and report transactions on their financial statements. In addition, an accurate and complete DoD agency-wide compilation process is necessary to ensure that the financial statements of all DoD Components are completely and accurately consolidated into the DoD Agency-Wide Basic Financial Statements.

In FY 2018, the DoD and most of its Components had a material weakness related to the financial statement compilation process. The DoD had challenges in obtaining complete and accurate Component financial statements to compile the DoD Agency- Wide Basic Financial Statements. For example, to ensure that its financial statements were accurate and complete, the U.S. Army Corps of Engineers made an adjustment to its financial statements for approximately $11 billion. The adjustment was not recorded in the system used to compile the DoD financial statements, nor was it communicated to the personnel responsible for compiling the DoD financial statements. As a result, the DoD financial statements did not include the $11 billion adjustment made by the U.S. Army Corps of Engineers. Without the inclusion of the adjustment, the DoD financial statements were materially misstated.

The DoD will continue to face challenges in obtaining complete and accurate Component financial statements in sufficient time to compile the DoD financial statements. Each year, the DoD must issue its financial statements no later than November 15. To ensure accurate compilation, the DoD needs the audited Component financial statements no later than November 8. However, the DoD business processes do not provide sufficient time to compile the Component financial statements and complete audit procedures over the balances presented. For example, the Defense Information Systems Agency General Fund and Working Capital Fund FY 2018 Financial Statements were not issued until January 18, 2019, over 2 months after the Component financial data were required for complete and accurate compilation into the DoD financial statements.

Many of the issues within the financial statement compilation process result from flaws in other business processes. For example, weaknesses in the Fund Balance With Treasury process result in unsupported adjustments that prevent auditors from concluding on the accuracy and fair presentation of the consolidated DoD Fund Balance With Treasury. Therefore, as the DoD addresses other material weaknesses, the financial statement compilation process should also improve, although the DoD will continue to face challenges with the congressionally mandated deadlines.

AUDIT PERSPECTIVE ON WHAT IS LEFT TO DO

The DoD Deputy Chief Financial Officer developed a centralized database in 2017 to track the NFRs and the status of the corrective action plans to address the NFRs. The database provides financial managers with a comprehensive view of NFRs and the overarching issues that affect the DoD's financial management.

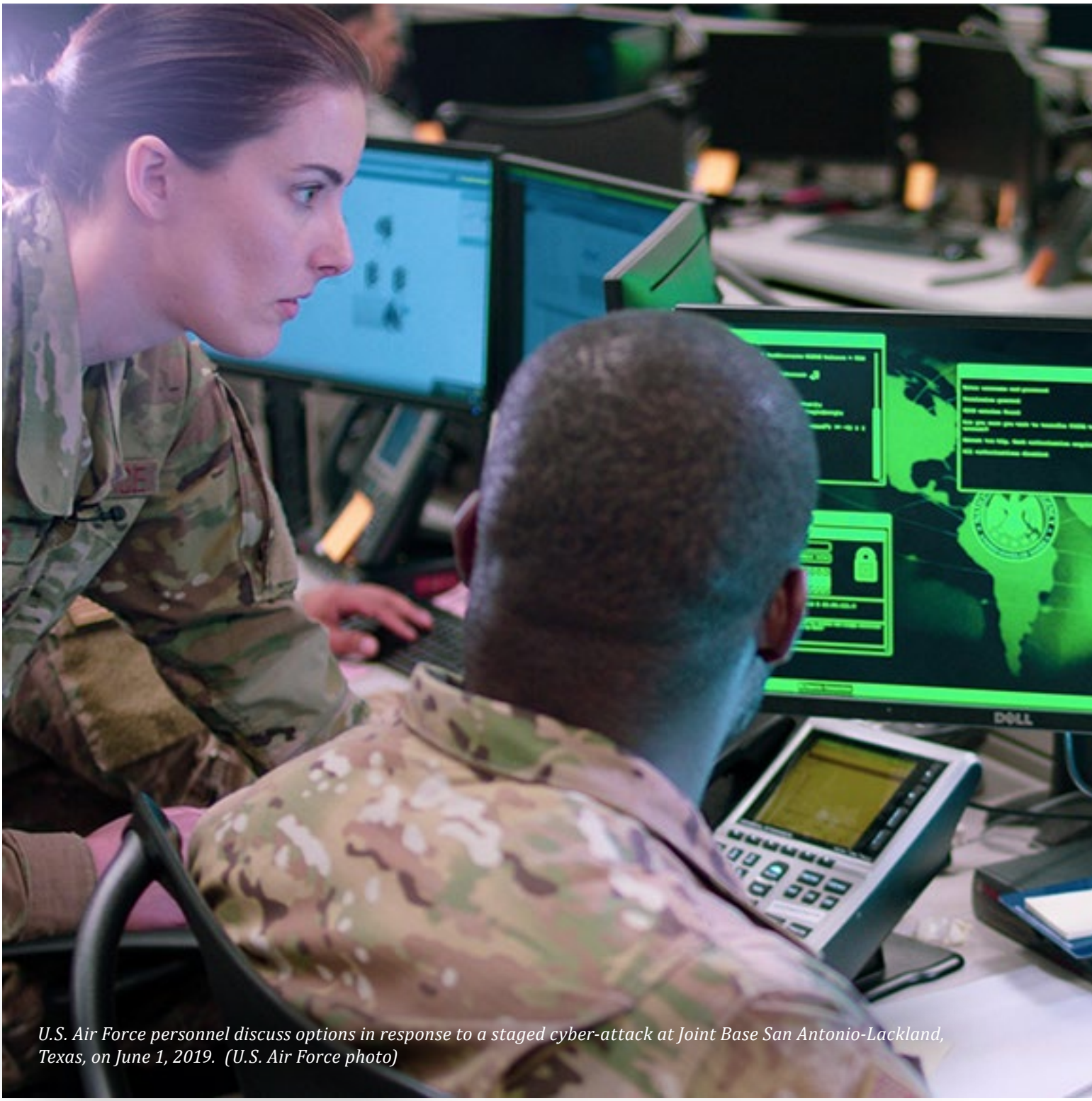
The DoD Components are now required to regularly report progress on implementing their corrective actions plans to the Deputy Secretary of Defense. This oversight of corrective actions plans sets a strong tone from the top, which is a fundamental component of an effective internal control environment. In the past, the DoD lacked corrective action plans or estimated completion dates for corrective action plans. The recent oversight provides DoD leadership with the status of NFRs and corrective action plans by DoD Components, and can measure the progress of each DoD Component. As of September 30, 2019, auditors closed 390 FY 2018 NFRs.

In addition, DoD leadership has prioritized the corrective action plans that align with the National Defense Strategy and provide the greatest potential value to the warfighter. In addition, DoD leadership established financial statement audit priorities that include such issues as access controls to information technology systems, existence and completeness of real property, inventory and operating material and supplies, and property in the possession of contractors.

DoD leadership also regularly reinforces that the financial statement audits are helping DoD business reform efforts by identifying areas that are working and those that need to be fixed. Financial statement audits are also giving DoD leadership the data it needs to prioritize improvements, allocate resources, and hold DoD Components and personnel accountable for good stewardship of taxpayer dollars.

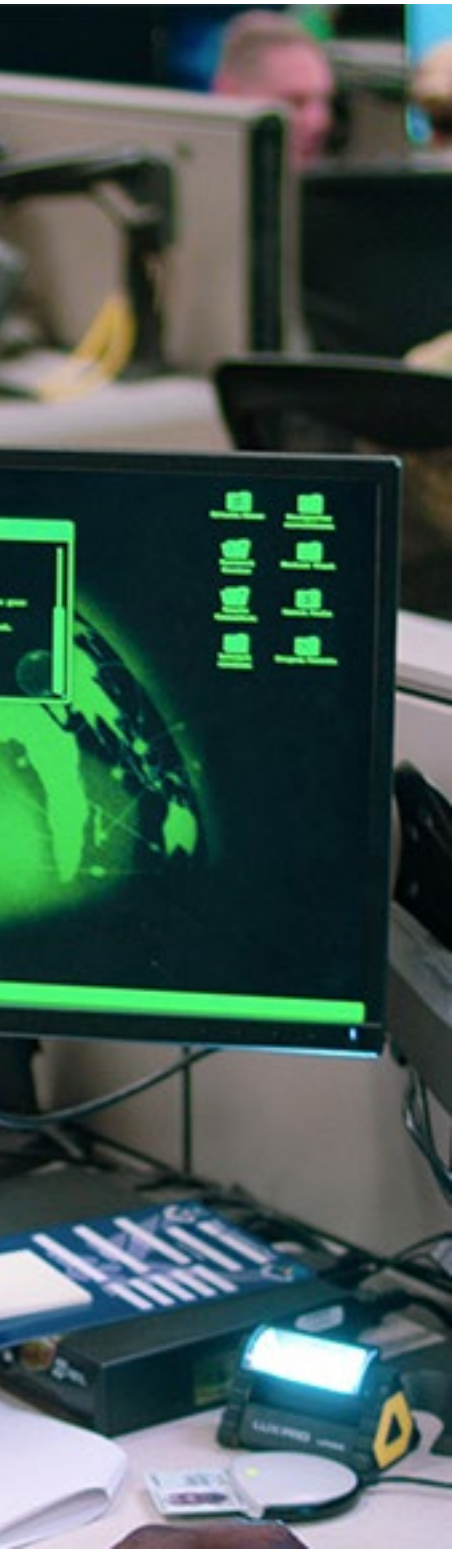
However, the road to a clean financial statement opinion is a long-term effort. It is critical that the DoD and its Components continue to fix the weaknesses and deficiencies identified in the audit through the development, implementation, and monitoring of corrective action plans. The DoD and Component leaders must also continue to regularly emphasize the importance and priority of sound financial management, the financial statement audit, and the implementation of corrective action plans. In addition, they should hold accountable other DoD leaders who are ultimately responsible for more accurate financial reporting.

In summary, the DoD will continue to face significant challenges related to financial management due to the size and complexity of the DoD and the shortcomings of its current financial management processes and systems. To obtain a clean opinion, and to improve its business processes, which go hand in hand, the DoD must implement recommendations that address a wide range of financial management and information technology issues. Financial statement audits not only determine the accuracy of financial records, but also provide actionable feedback on weaknesses and inefficiencies in the DoD financial management processes that, if corrected, can result in more efficient operations, better decision making, and better use of the significant resources provided to the DoD.



U.S. Air Force personnel discuss options in response to a staged cyber-attack at Joint Base San Antonio-Lackland, Texas, on June 1, 2019. (U.S. Air Force photo)

Challenge 6. Enhancing DoD Cyberspace Operations and Capabilities



The DoD relies on cyberspace and cyber capabilities to perform its military and intelligence missions, as well as its business operations. Cyberspace is a global domain that consists of the Internet, telecommunication networks, and computer systems. Cyberspace capabilities are devices or software used to achieve military objectives in and through cyberspace.

The DoD's cyberspace and cyber capabilities are essential to the DoD's ability to conduct operations across all domains—land, sea, air, space, and cyberspace. In addition, the 2019 National Intelligence Strategy identifies cyber as the most significant threat facing the DoD, its allies, and international partners. The 2019 National Intelligence Strategy states that cyber threats will increasingly threaten the national security of the United States and its interests as billions of devices are connected to the Internet.

Cyber attacks are becoming more sophisticated, malicious tools are more prevalent, and information technology systems, networks, and devices are more interconnected. Countries such as Russia, China, Iran, and North Korea; terrorist groups; hacktivists; and other independent malicious actors can use the Internet to exploit cyber vulnerabilities and gain unauthorized access and use of sensitive and classified information to threaten U.S. interests. In January 2019 testimony to the U.S. Senate Select Committee on Intelligence, the Director of National Intelligence stated, "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners."

The DoD's adversaries are also increasingly using cyber capabilities to collect intelligence, target DoD critical infrastructures, manipulate information, conduct cyber attacks, and disrupt or extort critical U.S. defense contractors. In addition, the DoD faces challenges in protecting its weapon systems from sophisticated cyber threats due to the DoD's frequent system upgrades that integrate emerging technologies into DoD weapons systems.

Although the Government Accountability Office (GAO) and the DoD OIG have warned of cybersecurity risks for decades, the DoD did not prioritize weapon system cybersecurity until recently. In this effort, the DoD faces many significant challenges, such as cybersecurity workforce shortages and difficulties sharing information about vulnerabilities and cyber threats with combatant commands, DoD agencies, other Federal agencies such as the Department of Homeland Security, U.S. partners, and the private sector.

To address cyber threats, the DoD must continuously assess and adapt its cyberspace capabilities to defend the DoD Information Network (DODIN) and its allies' systems. The DODIN is a global set of data, capabilities, and processes interconnected for collecting, processing, storing, disseminating, and managing real-time information for the warfighters, policy makers, and support personnel. The DODIN is vast and dispersed, composed of approximately 10,000 operational systems, thousands of data centers, tens of thousands of servers, and millions of computers and information technology devices that are mostly antiquated, which reduces the DoD's ability to secure them from cybersecurity threats.

In July 2019, the DoD released its Digital Modernization Strategy, which focuses on increasing DoD-wide technological capabilities and adopting enterprise systems through four strategic initiatives—innovation, optimization, cybersecurity resiliency, and talent cultivation—to increase capabilities for the Joint warfighter, empower new partnerships, and improve capabilities across the information enterprise. The Digital Modernization Strategy is a roadmap to implement cloud computing, artificial intelligence, and cybersecurity initiatives in support of the 2018 National Defense Strategy.

However, modernizing technology alone will not solve cybersecurity challenges. As discussed in the following sections, addressing these challenges requires the DoD to effectively conduct offensive and defensive cyberspace operations; defend against cyber attacks and insider threats; modernize and manage information technology systems; and build and maintain a skilled cyber workforce.

PLANNING AND CONDUCTING CYBERSPACE OPERATIONS

When conducting both offensive and defensive cyberspace operations, the DoD must plan, coordinate, and integrate these operations carefully considering the operations scope as well as intended and unintended outcomes. According to the Chairman of the Joint Chiefs of Staff Publication 3-12, offensive cyberspace operations are military missions intended to achieve lethal (during war-time) or non-lethal results in cyberspace through actions taken in support of DoD or national objectives. Defensive cyberspace operations are actions to defend the DODIN or any other network, system, or data that forces have been ordered to defend from cyber threats. The goal of defensive cyberspace operations is to defeat the cyber threat from an adversary and, if necessary, restore a compromised network to a secure and functional state.

As part of the 2018 National Defense Strategy, the DoD is authorized to implement an interagency process to conduct cyber operations more quickly in response to global cyber threats.

The National Defense Authorization Act for FY 2019 also expanded U.S. Cyber Command's authority to conduct cyberspace operations. U.S. Cyber Command uses 133 Cyber Mission Force teams to seek to identify and respond to evolving cyber challenges from U.S. adversaries.

Budget documents reveal plans for Unified Platform and Persistent Cyber Training Environment. (U.S. Air Force photo)

However, the GAO concluded in 2019 that U.S. Cyber Command faces difficulties retaining its Cyber Mission Force personnel and meeting the force's readiness standards.[38]

Another challenge to conducting cyberspace operations is U.S. Cyber Command's ability to acquire sufficient infrastructure, tools, and capabilities. To address this challenge, U.S. Cyber Command has taken several steps. In March 2019, the Commander testified that U.S. Cyber Command has established a new Joint Integrated Cyber Operation Center to support offensive and defensive cyberspace operations. Furthermore, the Commander stated that U.S. Cyber Command has developed the Joint Cyber Warfighting Architecture to guide capability development priorities. The Joint Cyber Warfighting Architecture is an adaptive set of cyber capabilities that constantly evolves as technology and threats change. This architecture consists of a comprehensive suite of cyber tools and shared platforms that will be used for training as well as offensive and defensive cyberspace operations.

OFFENSIVE CYBER OPERATIONS

Offensive cyber operations, which are normally classified, use intelligence collection activities to operate in and through cyberspace to affect U.S. adversaries without the use of force in the traditional military sense. Offensive cyber operations can also be used in conjunction with other military capabilities and domains to provide greater disruptive effects on an

[38] Report No. GAO-19-362, "DoD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," March 6, 2019.

adversary and gain a military advantage. Some examples of offensive cyber operations include inserting messages into adversary communications or inserting malware into systems, networks, and devices to disrupt or degrade an adversary's air defenses or command and control systems.

Offensive cyber operations face various challenges, such as the need for deconfliction. Deconfliction of cyberspace operations is the act of coordinating the use of cyberspace capabilities with DoD agencies, Federal agencies, and multinational partners to ensure that operations do not interfere, inhibit, or otherwise conflict with each other. For example, the DoD must assess whether a cyberspace mission or the use of a specific capability may impact other ongoing operations or identify the source of the action and therefore prevent the use of that capability in the future or draw the adversary's attention to a previously unknown operation by other U.S. Government agencies or U.S allies. In FY 2020, the DoD OIG plans to assess whether U.S. Cyber Command implemented processes to deconflict cyberspace operations to prevent compromise of DoD Component or interagency missions and operations.

Additionally, offensive cyber operations require proper coordination and a well-defined scope, clear rules of engagement, and measurable objectives. The laws that restrict military actions in U.S. territories also apply to cyberspace. This requires that combatant commanders, planners, and operators consult with legal counsel during planning and execution of cyberspace operations so they have a clear understanding of the applicable legal framework.

The Secretary of Defense has issued three strategies since 2011 to guide the DoD's cyberspace activities and operations, including accelerating the integration of cyber requirements into combatant command plans. However, in March 2018, the DoD OIG determined that U.S. European Command made only limited progress in integrating offensive and defensive cyberspace operations into its command plans. Since then, the DoD has combined cyber operators and planners to improve planning and integrate cyberspace operations into combatant command plans.[39]

The GAO is now conducting an examination of the DoD cyberspace authorities, strategies, policies, and procedures for military operations. In addition, the DoD OIG plans to assess whether U.S. Cyber Command planned and executed offensive cyber operations in accordance with the established rules of engagement and achieved measurable results.

DEFENSIVE CYBER OPERATIONS

The DoD also faces challenges in conducting defensive cyberspace operations, which seek to prevent, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure, the DODIN, and systems and networks used by U.S. allies. The purpose of defensive cyber operations, which also are normally classified, is to protect systems, networks, cyberspaceenabled devices, and data against malicious cyberspace activities. Defensive cyber operations missions can be conducted in response to specific cyber threats, exploitation, or other effects of malicious cyberspace activity.

On February 14, 2019, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict testified before the Senate Armed Services Committee that the DoD faces adversaries determined to erode the Nation's strategic advantages on a daily basis, and the

[39] Report No. DODIG-2018-097, "USEUCOM Efforts to Integrate Cyberspace Operations into Contingency Plans," March 30, 2018.

DoD must rapidly become more agile, more capable, and more sustainable to defend against adversarial activities.

To meet this goal, the DoD is using artificial intelligence to identify malicious cyber activities across different systems and networks. Artificial intelligence is the ability of machines to perform tasks such as recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking actions that normally require human intelligence or interaction.

To assess the DoD's efforts to effectively conduct defensive cyberspace operations, the DoD OIG is conducting an audit to determine whether the DoD planned and executed activities to implement memorandums established between the DoD and the Department of Homeland Security regarding cybersecurity and cyberspace operations. This review will assess the DoD's actions to enhance the U.S. Government's readiness to respond to cyber threats; improve protection and defense of U.S. critical infrastructure by enhancing information sharing between the DoD, the Department of Homeland Security, and the private sector; and coordinate joint planning for conducting defensive cyberspace operations and exercises in defense of the United States, the DODIN, and its partners.

DEFENDING THE DOD INFORMATION NETWORK

Increasingly sophisticated threats and the rising number of reported cyber incidents demonstrate the urgent need for strong DoD cybersecurity controls and processes within the DODIN and for its data. However, the DoD OIG and GAO have regularly identified DoD-wide problems in controlling access to systems, networks, and facilities; configuring systems and networks; and mitigating vulnerabilities associated with the use of commercial-off-the-shelf items, integrating emerging technologies, and advanced weapons system acquisitions. These deficiencies continue to hamper the DoD's ability to protect the DODIN and its sensitive and classified data from cyber attacks and unauthorized access.

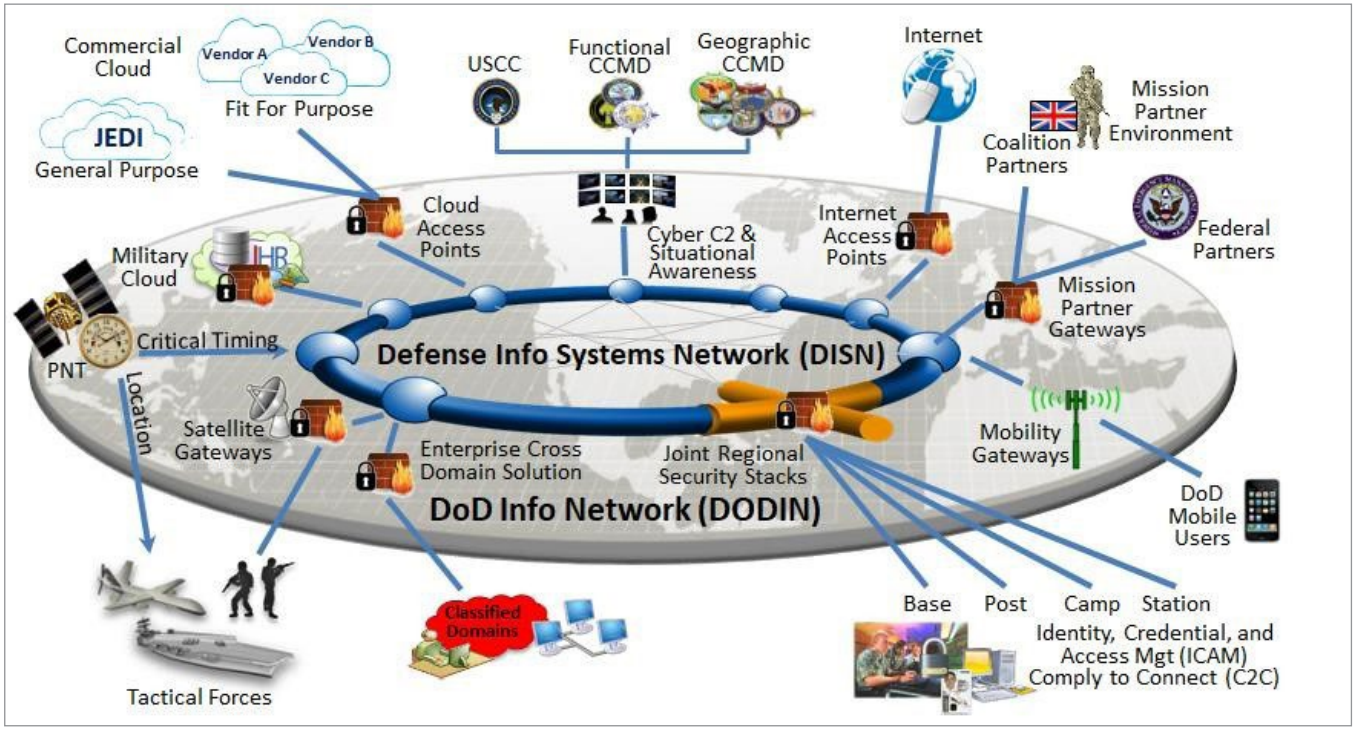
CYBER RISK MANAGEMENT

The DODIN is composed of thousands of interconnected systems, networks, and devices located worldwide, including DoD-owned and leased communications, software, security devices, data, and other associated services. The DoD cannot protect the DODIN from all cyber threats and must prioritize and protect the most critical systems, networks, and data from compromise. Figure 12 on the next page, illustrates the Joint Information Environment Framework.

In March 2014, the DoD Chief Information Officer mandated that the DoD improve the management of cybersecurity risks for its information technology by establishing and using a standard DoD-wide process—the DoD Risk Management Framework. This Framework provides DoD-wide implementation guidance that integrates activities for selecting, implementing, and monitoring system security controls based on the designated system risk level. However, this Framework unintentionally increased the cybersecurity related costs and the complexity of risk-based decisions. For example, the DoD has more than 100 authorizing officials who generally do not leverage cybersecurity reciprocity or coordinate their system approval decisions with others, thereby resulting in redundant and unnecessary system control reviews.

Reciprocity is the mutual agreement between organizations to accept each other's security assessments or security posture to share

Figure 12. Scope of the Joint Information Environment Framework



Source: 2019 DoD Digital Modernization Strategy

information. The lack of DoD-wide reciprocity and redundant system reviews has resulted in significant inefficiencies, increased costs, and reduced performance and visibility of potential cybersecurity risks for the DoD's more than 10,000 systems. In September 2018, the DoD Chief Management Officer recommended a more simplified approach that uses DoD-wide reciprocity for risk based security controls that could result in a potential overall DoD savings up to $564 million over the next 5 years (FY 2020 through FY 2024). To assess the progress that the DoD is making in this area, the DoD OIG initiated a joint audit with the Army, Navy, and Air Force audit agencies in September 2018 to determine whether DoD Components are leveraging cybersecurity reciprocity to reduce redundant test and assessment efforts when authorizing information technology to be used on DoD networks.

Additionally, the DoD faces significant risks related to protecting the information that it maintains on its systems, networks, and devices. To effectively detect data exfiltration attempts and respond to cyber incidents, the DoD must implement effective security controls and continuously monitor its networks. In May 2018, the Office of Management and Budget reported that Federal agencies, including the DoD, had agency-wide gaps in monitoring network activities and lacked standardized cybersecurity tools and capabilities.

The DoD OIG has consistently reported on problems the DoD has in protecting its systems, networks, and data. For example, in a December 2018 report, the DoD OIG determined that the Missile Defense Agency and other DoD Components did not consistently implement security controls to protect technical information related to the Ballistic Missile

Defense System.[40] Similarly, in a classified March 2019 report, the DoD OIG determined that Army, Navy, and Air Force officials did not correct problems identified in prior DoD OIG reports related to the improvement of system access controls and physical security safeguards that protect SECRET Internet Protocol Router Network access points.[41] The DoD OIG determined that the Army, Navy, and Air Force did not have a process to verify that users completed the required annual security training, ensure that approving officials maintained completed and approved user access forms, or ensure users had the required security training.

In FY 2020, the DoD OIG plans to assess additional cybersecurity controls and processes, such as whether the:

- DoD Intelligence Community agencies are implementing system security controls to protect classified enclaves from insider and external threats,
- Navy and Air Force Military Medical Treatment Facilities are implementing cybersecurity controls over medical devices that are connected to the DODIN, and
- Military Services are mitigating cybersecurity vulnerabilities for major DoD acquisition programs identified by the Office of Operational Test and Evaluation through realistic adversarial testing of the systems against cybersecurity threats.

In addition to protecting data on DoD systems and networks, the DoD must also ensure that DoD data maintained on contractor networks are secure. Cyber attacks against DoD contractor systems and networks have increased, and networks of DoD contractors remain vulnerable. For example, in July 2019, the DoD OIG issued an audit report that determined that nine DoD contractors it reviewed did not consistently implement required security controls for safeguarding sensitive DoD information.[42] In FY 2020, the DoD OIG plans to assess whether academic and research institutions that conduct military research and develop technologies in support of DoD programs and operations are implementing system security controls to protect DoD information maintained on their systems and networks and from insider and external cyber threats.

RESPONDING TO INSIDER THREATS

The number of unauthorized disclosures and data breaches by insiders working for Government agencies has increased. A DoD insider is any person with authorized access to DoD systems, networks, data, or facilities who could steal classified data, commit workplace violence, or sabotage or disclose DoD information in an unauthorized manner. For example, an Army service member leaked hundreds of thousands of classified documents in 2010. In 2013, a National Security Agency contractor disclosed classified information, which the National Security Agency Director stated resulted in the National Security Agency losing cyber capabilities.

After the 2010 unauthorized disclosures, the President issued Executive Order 13587 in October 2011 requiring that Executive Branch agencies operating or accessing classified

[40] Report No. DODIG-2019-034, "Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information," December 10, 2018.

[41] Report No. DODIG-2019-063, "Followup Audit on the Military Departments' Security Safeguards Over SECRET Internet Protocol Router Network Access Points," March 18, 2019.

[42] Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019.

systems, networks, or data implement an insider threat detection and prevention program. In December 2014, the DoD established the Defense Insider Threat Management and Analysis Center to provide the DoD with an enterprise-level capability for insider threat information integration and management. Since October 2016, the Defense Insider Threat Management and Analysis Center has been analyzing data and other indicators reported by DoD Components and agencies and recommending actions based on its analysis. This is a positive step to improve the DoD's ability to detect and proactively respond to potential insider threats.

However, the risk of insider threats remains strong. For example, as reported by the DoD OIG in December 2017, multiple data breaches by insiders have occurred at the National Security Agency since 2015.[43] In addition, a private cybersecurity firm notified the DoD in November 2017 that 100 gigabytes of data from a Top Secret Army intelligence project maintained by the National Security Agency was uploaded to an unsecured web server.

According to the DoD's 2019 Digital Modernization Strategy, the DoD plans to further address insider threats by, among other actions, deploying sensors to detect behaviors associated with insider threats and implementing analytics to improve the DoD's ability to continuously monitor those behaviors. To assess how the DoD is responding to insider threats, the DoD OIG is examining whether the Nuclear Command, Control, and Communications System has implemented controls to protect U.S. nuclear systems from insider and external threats. In FY 2020, the DoD OIG also plans to assess whether the Defense Insider Threat Management and Analysis Center is providing a DoD-wide capability for integrating, managing, and safeguarding sensitive insider threat information.

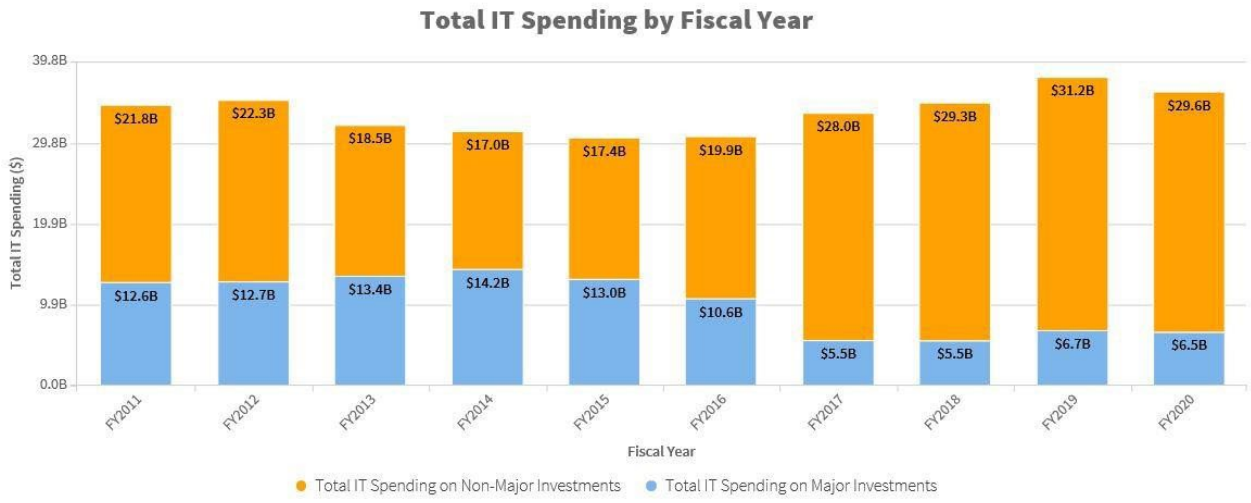
The DoD is taking steps to defend its vast architecture of systems, networks, devices, and data from insider and external threats, but longstanding challenges remain. The DoD must prioritize and protect its most critical systems, networks, and data based on the mission impact; consistently assess the risk of known and unknown threats and vulnerabilities and take timely action to mitigate those risks; and implement processes and programs to assess the sufficiency and effectiveness of contractor security. These are not easy or short-term actions, but they are critical to the DoD's ability to prevent cyber intrusions and compromise of critical information.

MODERNIZING DOD NETWORKS AND INFRASTRUCTURE

The DoD is seeking to reduce the number of Component-specific networks, platforms, and cloud computing environments that support operations and mission requirements, which will also significantly reduce the number of access points that adversaries could use to execute cyber attacks. The DoD is transitioning to enterprise-wide capabilities and services, such as an enterprise cloud environment, which the DoD believes will be more cost effective, agile, and resilient to persistent cybersecurity threats.

[43] Report No. DODIG-2018-043, "The National Security Agency Enterprise," December 19, 2017.

Figure 13. DoD Information Technology Spending by Fiscal Year



Source: IT Dashboard.

As reflected in Figure 13 below, the DoD has spent more than $30 billion annually on information technology for nearly the last decade. In FY 2019, the DoD spent $38 billion on information technology, of which, $1.2 billion was spent on modernizing its systems and networks. In addition, the DoD plans to spend another $36 billion on information technology investments in FY 2020. However, the DoD still faces key challenges with modernizing its aging information technology and ensuring the systems, networks, and devices it procures and develops are protected against cybersecurity threats.

To overcome modernization challenges, the DoD Chief Information Officer issued the 2019 Digital Modernization Strategy, which defines how the DoD will invest in information technology to modernize its architecture to meet the missions of today and support the strategic direction of tomorrow. The Digital Modernization Strategy also supports the DoD's implementation of the National Defense Strategy to provide the Joint Force with a competitive advantage in the modern battlespace through use of artificial intelligence, cloud computing, and enhanced cybersecurity capabilities.

In August 2010, the DoD began the Joint Information Environment initiatives, which required the DoD to establish a single enterprise architecture that supports the migration to cloud computing, to modernize and consolidate the DoD's information technology infrastructure and defend its systems, networks, and devices against cyber attacks. Despite some progress in meeting Joint Information Environment initiatives, the DoD continues to struggle to fully implement all Joint Information Environment initiatives. For example, in September 2014, the DoD Chief Information Officer directed the implementation of the Joint Regional Security Stacks to increase the cyber situational awareness, reduce adversary attack points, and improve the security posture of the DODIN by the end of FY 2019. The Joint Regional Security Stacks are a suite of equipment that includes assets such as network routers, firewalls, and switches that work together to provide network security capabilities, such as intrusion detection and prevention, among other things. However,

in June 2019, the DoD OIG issued an audit which determined that the Joint Regional Security Stacks are not meeting all intended Joint Information Environment initiatives and that the DoD did not ensure that all Joint Regional Security Stacks tools met users' needs to perform their cybersecurity duties, such as obtaining and reviewing log files to detect unauthorized activity.[44]

Another cyber challenge relates to developing the next generation system to manage the background investigations process. The National Defense Authorization Act for FY 2018 transferred responsibility for background investigations to the DoD from the Office of Personnel Management. In January 2018, the GAO identified a variety of problems the Defense Information Systems Agency had in connecting the DoD information technology systems with Office of Personnel Management legacy systems used for the background investigations process. In April 24, 2019, the President signed an executive order that expanded the DoD's role to conducting Government-wide suitability, credentialing, and security clearance responsibilities.

Consequently, modernizing the system that maintains security clearance background data is critical to the success of the DoD's assumption of these responsibilities. In June 2016, the Defense Information Systems Agency began developing the National Background Investigation System by awarding a 5-year, $49 million contract to develop a cloud-based security clearance information technology system prototype. In May 2019, the Defense Counterintelligence and Security Agency awarded $75 million contract to build another major component of the system. This new system is intended to allow the Defense Counterintelligence and Security Agency to use artificial intelligence to increase the timeliness of the clearance process. In FY 2020, the DoD OIG plans to assess whether the DoD identified system security requirements and is designing system security controls to protect personally identifiable information, highly sensitive information, and classified data for the National Background Investigation System.

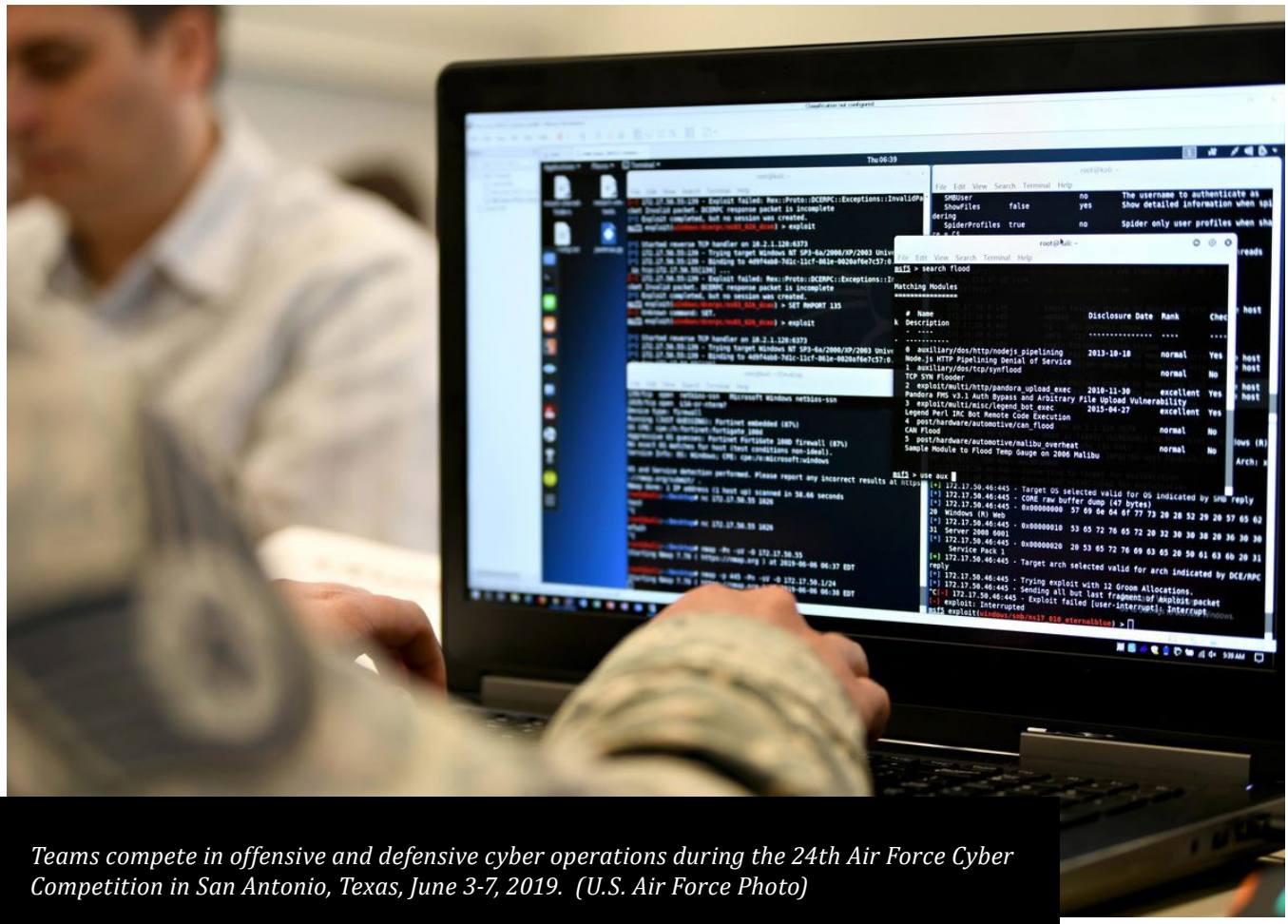
USE AND IMPLEMENTATION OF EMERGING TECHNOLOGIES

The security of new warfighting technologies is critical to maintaining the DoD's advantage in cyberspace. Other nations, particularly Russia and China, are also making significant investments in emerging technologies, such as artificial intelligence for military purposes. For FY 2020, the DoD has requested $104 million for research, development, test and evaluation, which is its largest request in 70 years. The 2019 DoD Digital Modernization Strategy includes investing in and using emerging technologies such as artificial intelligence, additive manufacturing or 3-D printing, 5G wireless networks, and cloud computing.[45]

In June 2018, the Secretary of Defense established the Joint Artificial Intelligence Center to oversee the DoD-wide integration of artificial intelligence and deliver capabilities, coordinate artificial intelligence activities, and develop governing policies, ethical guidelines, and cybersecurity requirements for the use of artificial intelligence. The 2018 DoD Artificial Intelligence Strategy provides a roadmap for using artificial intelligence to advance security and ensure a competitive military advantage

[44] Report No. DODIG-2019-089, "Audit of the DoD's Implementation of the Joint Regional Security Stacks," June 4, 2019.

[45] Report No. GAO-16-56, "Defense Additive Manufacturing," October 2015.



Teams compete in offensive and defensive cyber operations during the 24th Air Force Cyber Competition in San Antonio, Texas, June 3-7, 2019. (U.S. Air Force Photo)

against those who threaten the United States and its allies.[46] On March 12, 2019, Lieutenant General Jack Shanahan, Director of the Joint Artificial Intelligence Center, stated to the Senate Armed Services Subcommittee on Emerging Threats and Capabilities that the Center is also working with the Defense Innovation Board to collaborate on the development of DoD artificial intelligence principles and provide research and developing for optimizing artificial intelligence activities.

In an August 2019 media briefing, the Joint Artificial Intelligence Center Director stated that the DoD had invested $93 million in artificial intelligence initiatives for FY 2019 and requested $268 million for FY 2020 initiatives. For example, the DoD is using artificial intelligence for predictive maintenance of the SH-60 Seahawk helicopter; detecting cyber events; and monitoring user, system, and network activity. The DoD OIG is auditing whether the DoD has developed and implemented a governance structure and is protecting and retaining ownership rights of artificial intelligence data and technologies.

However, implementation of the DoD's artificial intelligence initiatives is limited by the pace and capabilities of its broader digital modernization efforts. To integrate artificial intelligence into DoD operations, the DoD plans to use a common platform, deploy reusable tools, establish standards, and rely on cloud computing services.

[46] The Summary of the 2018 DoD Artificial Intelligence Strategy, "Harnessing AI to Advance Our Security and Prosperity," released on February 12, 2019.

The 2018 DoD Cloud Strategy stated that the DoD should shift its focus from a physical information technology infrastructure deployed across the DoD to using an enterprise cloud computing environment that provides flexibility and greater access to its global infrastructure. The current DoD Cloud Strategy focuses on implementing the Joint Enterprise Defense Infrastructure to support the majority of DoD systems, networks, and applications. However, the contract award has been challenged in litigation since April 2019.

Additive manufacturing prints parts from a digital model using nontraditional materials, and it allows for parts to be printed wherever they are needed. Additive manufacturing can also replace the physical delivery or logistical supply chain process with digital instructions that can be transmitted instantly to machines that can print a new item that is co-located with the aircraft or vehicle. This convenience makes additive manufacturing an appealing alternative solution to the traditional acquisition, procurement, and logistics processes. However, the additive manufacturing process has inherent cybersecurity risks that could allow adversaries to manipulate the digital instructions, which could cause the printer to make a defective product. The DoD OIG is conducting an audit to determine whether DoD Components are securing additive manufacturing systems and data to prevent unauthorized changes and ensure integrity of design data. Further discussion on the DoD supply chain challenges is contained in Management Challenge 8, "Improving Supply Chain Management and Security."

BUILDING AND RETAINING A SKILLED CYBER WORKFORCE

As the DoD modernizes its information technology and adopts emerging technologies, it must ensure the DoD cyber workforce has the skills to keep pace with rapidly evolving technology. However, hiring, training, and retaining a sufficient workforce to support and defend the DODIN and handle its current and emerging cyberspace mission requirements continues to challenge the DoD.

In May 2019, the Acting Secretary of Defense stated that recruiting and retaining the DoD's cyber workforce is the greatest skill challenge that the DoD faces.[47] The DoD competes with other Federal agencies and the private sector to recruit, develop, promote, and retain a skilled military and civilian cybersecurity workforce. The DoD cyber workforce includes software developers, system administrators, network operations specialists, data analysts, systems security analysts, and system evaluators, and personnel who conduct related intelligence activities and operations in or through cyberspace. In September 2018, the DoD Principal Deputy Chief Information Officer testified that the DoD lost about 4,000 civilians performing cyber-related functions during the prior year due to attrition.

The National Defense Authorization Act for FY 2016 gave the DoD authority to establish an enterprise approach for managing civilian cyber professionals through the Cyber Excepted Service, which gives the DoD Chief Information Officer, U.S. Cyber Command, Defense Information Systems Agency, and the Service Cyber Components the ability to hire cyber professionals outside of the normal

[47] U.S. House of Representatives, Committee on Appropriations, FY 2020 Budget Hearing.

competitive service process and provide them with additional pay and bonuses. In March 2019, the Assistant Secretary of Defense for Homeland Defense and Global Security and the Principal Cyber Advisor reported that the DoD had converted 403 civilian positions from the competitive service to Cyber Excepted Service positions. The DoD plans to convert approximately 15,000 more positions to Cyber Excepted Service positions.[48] In FY 2020, the DoD OIG plans to assess the DoD's progress in recruiting and retaining its cyber professional workforce and its implementation and use of Cyber Excepted Services hiring authorities.

In March 2019, the GAO determined that although U.S. Cyber Command had taken steps to develop its Cyber Mission Force, many of the 133 teams that initially reported reaching full operational capability no longer had the full complement of trained personnel, and therefore no longer met readiness standards.[49] In addition, the July 2019 DoD OIG Compendium of Open Recommendations identified a high-priority open recommendation from a 2016 DoD OIG report, which recommended that the Commander of U.S. Cyber Command and the Commandant of the Marine Corps develop a doctrine, organization, training, material, leadership and education, personnel, facilities, and policy framework that addresses strategies to build, grow, and sustain the Cyber Mission Force.[50] As of September 2019, nearly 4 years later, these Components have yet to develop such a strategy.

In summary, the DoD must ensure that it has a skilled cyber workforce capable of using necessary tools and capabilities to conduct cyberspace operations. The DoD must also secure and monitor the DODIN and its data to prevent insiders from making unauthorized disclosures and data exfiltration that could adversely affect national security. The DoD must also continuously identify, address, and adapt to challenges affecting its ability to protect the DODIN and conduct cyberspace operations.

---

48 Statement of Mr. Kenneth Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor, "Testimony Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities," March 13, 2019.

49 Report No. GAO-19-362, "DoD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," March 6, 2019.

50 Report No. DODIG-2016-026, "Combat Mission Teams and Cyber Protection Teams Lacked Adequate Capabilities and Facilities to Perform Missions," November 24, 2015.

A Delta IV carrying the GPS III SV2 satellite lifts off from Space Launch Complex-37 at Cape Canaveral Air Force Station, Florida, August 22, 2019. The satellite will become part of a 31 satellite constellation on orbit, providing enhanced timing and navigation to civilians and the warfighter. (United Launch Alliance courtesy photo)

Challenge 7. Enhancing Space-Based Operations, Missile Detection and Response, and Nuclear Deterrence

U.S. adversaries are making significant advances in their space, missile, and nuclear capabilities. The DoD is therefore faced with the challenge of simultaneously sustaining its legacy space and nuclear systems while modernizing and replacing the systems to meet future threats.

Additionally, the DoD must develop new ballistic missile defense capabilities to keep pace with emerging threats, such as hypersonic missiles. With regard to the space challenge, the 2018 National Defense Strategy notes that new threats to commercial and military uses of space are emerging, such as Russia and China's anti-satellite weapon programs. Additionally, the 2019 Center for Strategic and International Studies Space Assessment emphasizes that Iran and North Korea continue to develop electronic capabilities to jam and spoof satellites. The United States and DoD's increased digital connectivity among business, government, consumers, and the military creates significant vulnerabilities to energy, communications, and military capabilities.

In addition, over 20 countries now possess offensive missiles. Missile capabilities, including hypersonic missiles, are becoming increasingly complex, lethal, and dangerous. According to the 2019 Missile Defense Review, Russia, China, and North Korea are investing substantially in their missile capabilities, enhancing their ground- and sea-launched missile arsenals with short-, intermediate-, and intercontinental-range systems, in addition to fielding mobile missiles to challenge the U.S. ability to detect their launch preparations. Russia, China, and North Korea have each developed and deployed dual-capable offensive missile systems able to employ conventional or nuclear warheads.

With regard to nuclear weapons, the current nuclear forces of the United States are reaching the end of their service life. According to a January 2019 Congressional Budget Office report on the projected cost of U.S. nuclear forces, "Over the next two decades, essentially all components of nuclear forces will have to be refurbished or replaced with new systems if the United States is to continue fielding those capabilities."

The Congressional Budget Office estimated that modernization of the nuclear forces would cost a total of $494 billion between 2019 and 2028.

The following sections describe in more detail the challenges facing the DoD in each of these three areas.

SPACE

The United States, as well as its allies and its adversaries, depend on space-based satellites and sensors for around-the-clock communications, weather, imagery, and many other critical functions. As of 2019, there are at least 666 intelligence satellites from 38 different countries monitoring the globe, 790 communications satellites from 45 different countries moving critical data related to all aspects of global telecommunications, 121 navigation satellites used with the Global Positioning System and 303 scientific satellites pursuing improvements in endeavors from farming to reducing pollution. The United States operates 870 of these satellites.

The DoD's space program includes launch vehicles and satellite systems for reconnaissance, early warning of missile launches and nuclear detonations, navigation, communications, and weather. Additionally, the DoD's space program includes ballistic missile defense related satellites and systems. Many of these systems are developed and operated for both national security and civilian applications. For example, the Global Positioning System is a DoD system, but the system enables civilian and commercial applications from communications to automobile navigation systems. To successfully operate these space-based systems, the DoD needs launch vehicles and launch systems. Launch vehicles are rockets that carry a payload, such as an infrared sensor, from the Earth's surface into space. Launch systems include the launch vehicle, launch pad, vehicle assembly and fueling systems, range safety, and other related infrastructure.

The United States faces rapidly growing threats to its space capabilities. China and Russia are overtly pursuing space warfighting capabilities to neutralize U.S. space capabilities during a time of conflict. Other adversaries, such as North Korea and Iran, are also continuing to develop counter-space capabilities, such as electronically jamming satellites. Jamming is an electronic attack that interferes with radio frequencies by generating noise in the same frequency as the intended target.

The Director of National Intelligence testified in January 2019 before the Senate Select Committee on Intelligence that, "Space has become the new global frontier, with competition from numerous nations" and that the Office of the Director of National Intelligence expects "foreign governments to expand their use of space-based reconnaissance, communications, and navigation systems." He further stated, "China and Russia will continue training and equipping their military space forces and fielding new antisatellite weapons to hold U.S. and allied space services at risk." The Director also stated that China has an operational antisatellite missile system, and that Russia has established a ground-based laser system that could damage spacebased optical sensors that help detect an enemy missile attack.

With regard to China's threat to space, General John "Jay" Raymond, who is the Commander of both U.S. Space Command and Air Force Space Command, stated in September 2019 during remarks at an event hosted by the Mitchell Institute for Aerospace Studies, "We're pretty comfortable [in asserting] that they are

developing directed energy weapons—probably building lasers to blind our satellites[.]" He also stated, "It's clear that China would plan to use those threats against us in conflict."

The DoD does not have a single entity responsible for space-related strategy, doctrine, and acquisition, which further complicates the management of the personnel performing space related activities which are embedded throughout the Military Services.[51] In its May 2019 report on the requirements and costs of new military space organizations, the Congressional Budget Office estimated that about 23,000 full-time positions within the DoD are dedicated to performing space activities or to supporting those who do, excluding space activities in the intelligence agencies.[52] About 93 percent of those positions are spread throughout several major commands in the Department of the Air Force.

In August 2019, U.S. Space Command was officially established as the DoD's 11th geographic combatant command. General Raymond stated that the new command will build a fighting force capable of conducting defensive and offensive operations against potential adversaries seeking to deny America's access to space. In September 2019, General Raymond stated, "The importance of standing up this [new] command and the importance of standing up a space force is to make sure that we can stay ahead of … threats."

The Administration has also proposed creating a "Space Force," which would be an independent Military Service within the Department of the Air Force, similar to the Marine Corps relationship to the Navy. In its FY 2020 budget submission, the Administration has also proposed creating a new agency that would be responsible for the development and acquisition of space systems. Furthermore, the Administration has proposed creating a civilian Under Secretary for Space who would supervise the new Service and report to the Secretary of the Air Force.

The Congressional Budget Office's May 2019 report estimated that a new Military Service would require 4,100 to 6,800 new overhead and management positions, increasing the DoD's annual personnel costs by $820 million to $1.3 billion a year. Additionally, the onetime costs for service-to-service transfer bonuses, organizational start-up costs, and new infrastructure would be $1.1 billion to $3 billion. Approximately 22,900 positions would be transferred from existing Military Services. In total, and if approved by Congress, the new Service would have 27,000 to 29,700 positions.

Highlighting the importance of space, the DoD has requested over $14 billion to modernize space capabilities. For example, the DoD has requested funds to:

- resource the initial establishment of the U.S. Space Force,
- purchase four National Security Space Launch vehicles,
- purchase an additional Global Positioning System III satellite, and
- modernize space-based missile warning satellites and sensors.

[51] Report No. GAO-19-240, "Defense Space Systems, DOD Should Collect and Maintain Data on Its Space Acquisition Workforce," March 2019.

[52] Congressional Budget Office, "The Personnel Requirements and Costs of New Military Space Organizations," 2019.

In the FY 2019 and FY 2020 budget requests, the Air Force sought funds to modernize the survivable ground component of the U.S. Nuclear Detonation Detection System, the Integrated Tactical Warning and Attack Assessment Mobile Ground System (MGS). According to the Air Force, the MGS is the DoD's only system to receive missile warning and nuclear detonation data from Global Positioning System and other satellites with the ability to survive and operate through all phases of nuclear war. The MGS receives missile warning data and nuclear detonation data from the U.S. Nuclear Detonation Detection System and other space-based sensors, and provides the data to the National Command Authority.

In 2019, the DoD OIG evaluated whether the Air Force adequately implemented previous DoD OIG recommendations to ensure that the current MGS could be sustained until the replacement system attains full operational capability. The DoD OIG evaluation determined that the Air Force had made progress in implementing the recommendations, but the Air Force had not budgeted the necessary funding to keep the replacement program on schedule.[53]

The DoD OIG is currently evaluating three other areas critical to space operations. The DoD OIG is conducting an audit to determine whether U.S. European Command and U.S. Indo-Pacific Command have integrated space operations into military deception plans to protect the United States and its allies against adversarial space capabilities. Additionally, the DoD OIG is evaluating whether the Air Force complied with the Launch Services New Entrant Certification Guide when certifying the launch system design for the Evolved Expendable Launch Vehicleclass Space X and Falcon Heavy launch vehicles. The DoD OIG is also evaluating whether the Air Force's Space and Missile Systems Center is complying with DoD and Air Force quality assurance standards for the Geosynchronous Space Situational Awareness Program and whether the program office is providing adequate oversight of the contractor. These satellites collect data to allow for more accurate tracking and characterization of man-made orbiting objects. From its orbit, the satellite has a clear, unobstructed view without the interruption of weather or the atmospheric distortion that can limit ground-based systems.

BALLISTIC MISSILE DEFENSE

With the proliferation of offensive ballistic and cruise missiles and emerging hypersonic weapons technologies that markedly raise threats to regional balances and to major U.S. allies and partners, missile defense is a key challenge for the DoD.

Missile defense involves different challenges, depending on the type of missile. Ballistic missiles are fired on a predictable trajectory, or arc, and are under power only during the launch phase. Ballistic missiles use gravity to reach their targets at high speed. Cruise missiles operate under power from launch until target and are highly maneuverable. These missiles travel at a horizontal trajectory, resulting in much lower speeds. Hypersonic weapons are more dangerous and harder to detect and intercept because they incorporate the speed of a ballistic missile with the maneuvering capabilities of a cruise missile. Hypersonic

[53] Report No. DODIG-2019-078, "Evaluation of the Air Force's Implementation of DoD OIG Recommendations Concerning Modifications of the Integrated Tactical Warning and Attack Assessment (ITW/AA) Mobile Ground System," April 17, 2019.

weapons refer to weapons that travel faster than Mach 5, approximately 3,800mph, and have the capability to maneuver during the entire flight.

The DoD's Ballistic Missile Defense System (BMDS) seeks to defend the U.S. homeland, deployed forces, and allies. The BMDS is an integrated, layered ballistic missile defense architecture that provides multiple opportunities to destroy missiles and their warheads before they can reach their targets. It includes land-, sea-, and space based elements to track, target, and destroy offensive ballistic missiles of different ranges, speeds, and sizes after their launch. The system's architecture includes:

- networked sensors (including space-based) and ground- and sea-based radars for target detection and tracking;
- ground- and sea-based interceptor missiles for destroying a ballistic missile using either the force of a direct collision, called "hit-to-kill" technology, or an explosive blast fragmentation warhead which detonates shortly before the collision of the interceptor and causes a debris field of shrapnel in its immediate flight path; and
- a command, control, battle management, and communications network providing operational commanders with the needed links between the sensors and interceptor missiles.

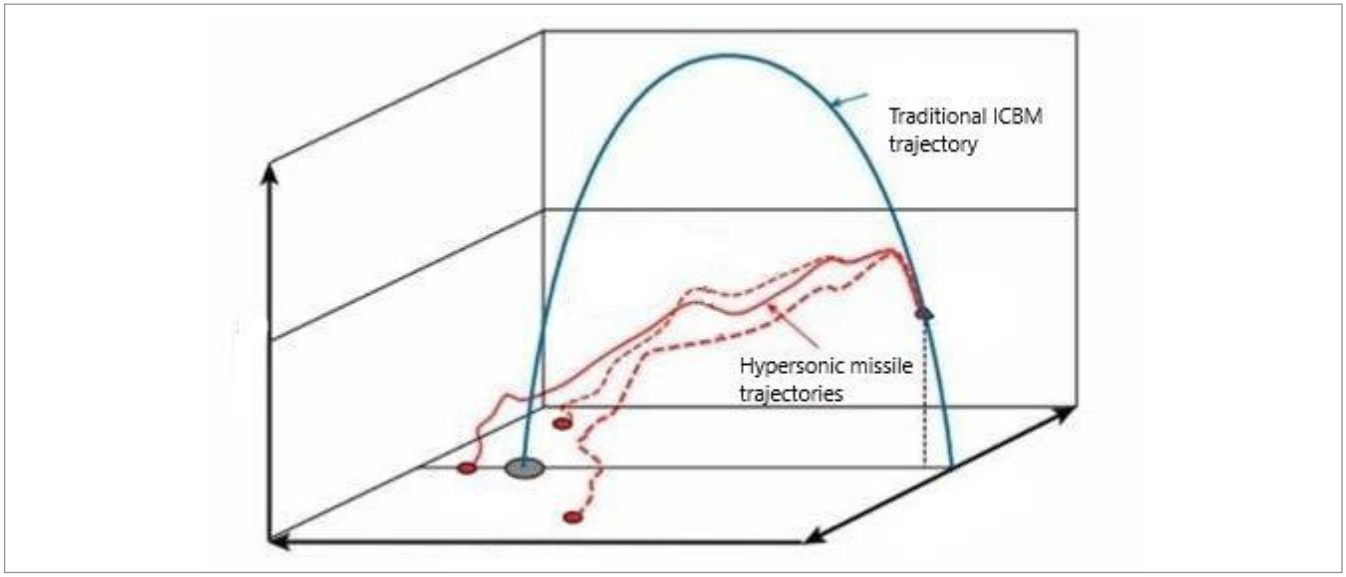
Missile defense elements are operated by military personnel from U.S. Strategic Command, U.S. Northern Command, U.S. Indo-Pacific Command, U.S. European Command, and other commands.

The United States also has missile defense cooperative programs with allies, including the United Kingdom, Japan, Australia, Israel, Denmark, Germany, the Netherlands, the Czech Republic, Poland, and Italy. The Missile Defense Agency also participates in NATO activities to develop an integrated NATO ballistic missile defense capability.

However, recent failures with new technologies and problems in missile warning indicate that the DoD has significant challenges related to identifying and communicating ballistic missile threats. For example, in 2018 a state employee in Hawaii mistakenly sent out an emergency alert declaring that a "ballistic missile threat" was "inbound." The message did not specify what kind of missile, and it created panic among some Hawaii residents until a second message, 38 minutes later, acknowledged it was an error. The error was attributed to a mistake by a single employee pressing the wrong button, which suggests a control weakness between the DoD and state emergency management.

In August 2019, the DoD canceled a multi-billion dollar contract with Boeing for a new ballistic missile interceptor. This halted the redesigned kill vehicle program after years of efforts. The redesigned kill vehicle was a $5.8 billion technology program to improve on the current exo-atmospheric kill vehicle. Both are ground-based interceptors designed to defend the continental United States against long-range ballistic missile attacks. According to an August 2019 DoD statement, the DoD canceled the contract "due to technical design problems" and "due to the failure of certain critical components to meet technical requirements as specified in the development contract." The DoD decided to move to a next-generation interceptor competition, but did not state when the interceptor will be developed or fielded.

Figure 14. Ballistic Missile and Hypersonic Missile Trajectories



Source: RAND Analysis.

At the same time, the missile programs of other countries are developing and increasing the threat to the United States. Over the past decade, North Korea has invested considerable resources in its nuclear and ballistic missile programs, and had undertaken extensive nuclear and missile testing to develop the capability to threaten the United States with a missile attack. On October 2, 2019, North Korea test fired a ballistic missile from a barge off the coast of North Korea. North Korea has been trying to develop the ability to fire ballistic missiles from submarines, giving them both a land and sea based nuclear missile capability.

Iran has the largest ballistic missile force in the Middle East and continues to develop technologies for intercontinental range missiles capable of threatening the United States.

Along with the ballistic missile threat, the United States faces a growing threat from hypersonic missiles being developed by Russia and China. As noted above, in addition to their speed, hypersonics can be maneuvered in ways that confound existing methods of defense and detection. Unlike most ballistic missiles, hypersonic missiles could strike the United States in under 15 minutes—resulting in a very short window of time for U.S. forces to react.

In March 2018, Vladimir Putin boasted that Russia had two operational hypersonic weapons—a fast, air-launched missile capable of striking targets up to 1,200 miles away, and a missile designed to be mated with an intercontinental ballistic missile before maneuvering toward its targets. However, the Congressional Research Service reported in September 2019 that U.S. intelligence reports suggest that Russia's hypersonic weapons are unlikely to be operational before 2020. The Congressional Research Service also reported that Russia successfully tested a hypersonic weapon twice in 2016 and once in December 2018, reportedly reaching speeds of Mach 20; however, an October 2017 test resulted in failure.[54]

[54] CRS Report No. R45811, "Hypersonic Weapons: Background and Issues for Congress," September 17, 2019.

Traditional ballistic missiles are powered initially by a rocket or series of rockets in stages, but then follow an unpowered trajectory that arches upwards before descending to reach its intended target. Hypersonic missiles can fly mostly horizontally with a highly advanced engine. The unusual trajectories of these missiles would allow them to approach their targets at roughly 12 to 50 miles above the Earth's surface. These heights are below the altitude at which ballistic missile interceptors—such as the American Aegis ship-based system and the terminal-phase ground-based system—are designed to typically operate, but they are above the altitude that simpler air defense missiles, like the Patriot system, can reach. Figure 14 illustrates the trajectories of ballistic and hypersonic missiles.

According to the Center for Strategic and International Studies, China is developing hypersonic missiles and could reach initial operational capability by 2020. The DoD's 2019 annual report to Congress stated that the development of hypersonic missiles by foreign entities "is something that should cause the United States concern . . . [i]f it really is a weapon that can go Mach 5 . . . and defeat U.S. missile defense systems, that puts carriers at risk." In March 2018, General John E. Hyten, Commander of U.S. Strategic Command, told the Senate Armed Services Committee, "We don't have any defense that could deny the employment of such a weapon against us."

To address these challenges, the DoD is investing in the expansion and modernization of U.S. homeland missile defense capabilities. The National Defense Authorization Act for FY 2017 stated that Congress will:

> maintain and improve an effective, robust layered missile defense system capable of defending the territory of the United States, allies, deployed forces, and capabilities against the developing and increasingly complex ballistic missile threat with funding subject to the annual authorization of appropriations and the annual appropriation of funds for National Missile Defense.

These priorities are reflected in the Administration's recent budget requests and actions. Congress appropriated approximately $15.3 billion in FY 2018 for homeland and regional missile defense, including an emergency appropriation of $4 billion to expand and enhance U.S. missile defense capabilities against North Korean missile threats to the U.S. homeland, forces abroad, allies, and partners.

The FY 2020 President's Budget request includes funds to sustain the surge in missile defense investment in FY 2018 and FY 2019. The FY 2020 budget request related to missile defense includes:

- Aegis Ballistic Missile Defense, the Naval component of missile defense including upgrades for five cruisers and 28 destroyers - $1.7 billion;
- Research for new ballistic missile defense capabilities in land-launched weapons, extended-ranged weapons, and space-based sensors - $1.5 billion;
- Ground Based Midcourse Defense, the capability to engage and destroy intermediate- and long-range ballistic missile threats in space to protect the United States - $1.7 billion;
- Terminal High Altitude Area Defense Ballistic Missile Defense, which provides the BMDS with a globally transportable, rapidly deployable capability to intercept and destroy ballistic missiles inside or

outside the atmosphere during their final, or terminal, phase of flight - $0.8 billion; and

- Patriot Advanced Capability Missile Segment Enhancements, the missile defense system that works with the Terminal High Altitude Area Defense to provide an integrated, overlapping defense against missile threats in the terminal phase of flight - $0.7 billion.

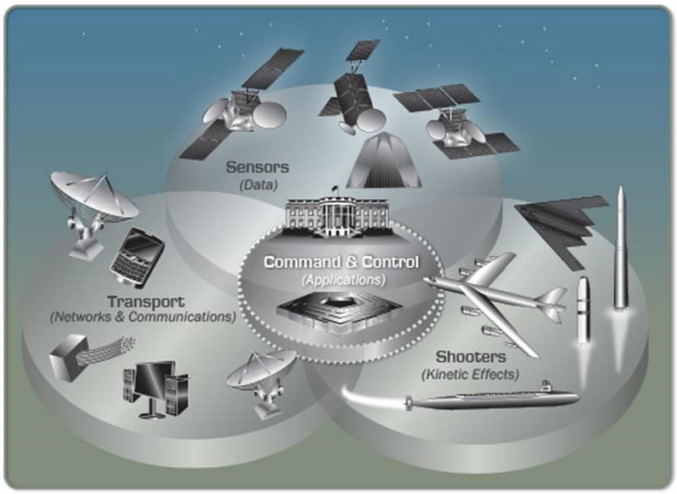
It is important that the DoD maintain effective internal controls over the expenditure of those funds and the protection of critical information in the hands of contractors. For example, the DoD OIG issued an audit in December 2018 that evaluated the DoD's progress in meeting its missile defense requirements and the controls in place to protect BMDS technical information, whether managed by cleared Defense contractors, or by the Government. Cleared contractors are entities granted clearance by the DoD to access, obtain, or store classified information, to bid on contracts, or conduct activities in support of DoD programs. The DoD OIG determined that the DoD did not consistently implement security controls and processes to protect BMDS technical information.[55]

NUCLEAR

The former Chairman of the Joint Chiefs of Staff, General Joseph Dunford, testified at a House Armed Services Committee hearing in 2019 that "Nuclear deterrence is a top priority within the U.S. military. It's our singular, most important mission." Similarly, the Deputy Under Secretary of Defense for Policy testified to the House Armed Services Committee's Strategic Forces Subcommittee in March 2019:

> Nuclear deterrence is the bedrock of U.S. national security. Our nuclear deterrent underwrites all U.S. military operations and diplomacy across the globe. It is the backstop and foundation of our national defense. A strong nuclear deterrent also contributes to U.S. non-proliferation goals by limiting the incentive for allies to have their own nuclear weapons.

Figure 15. Nuclear Command, Control, and Communications



Source: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters Handbook, 2016.

However, the components of the DoD's nuclear triad—the three-part military structure consisting of ballistic missile submarines, land-based intercontinental ballistic missiles (ICBMs), and bomber aircraft—are reaching the end of their service life.[56]

With regard to nuclear delivery systems, the DoD's nuclear command, control, and communications (NC3) system is a legacy of the Cold War. It was last comprehensively

[55] Report No. DODIG-2019-034, "Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information," December 10, 2018.

[56] Congressional Budget Office, "Projected Cost of U.S. Nuclear Forces," January 2019.

updated almost three decades ago. NC3 includes interconnected elements composed of warning satellites and radars; communications satellites, aircraft, and ground stations; fixed and mobile command posts; and the control centers for nuclear systems. Figure 15 illustrates the NC3 system.

In addition, over the next two decades, essentially all the components of nuclear forces must be refurbished or replaced with new systems if the United States is to continue fielding those capabilities.

For example, as the sea-based leg of the triad, the United States currently operates 14 *Ohio*-class ballistic missile submarines that are being replaced by the *Columbia*-class ballistic missile submarines. The *Ohio*-class submarines entered service between 1981 and 1997; each had an expected service life of 30 years. On 1998, the Navy decided to extend the original 30-year service life to 42 years. The first ballistic missile submarine is now scheduled to be retired in 2027. The *Columbia*-class program is expected to deliver a minimum of 12 ballistic missile submarines to replace the current *Ohio*-class fleet and is designed to provide required deterrence capabilities for decades. The first *Columbia*-class submarine is scheduled to be fielded in 2031, and the remaining 11 are scheduled to be fielded one-per-year until 2042. The General Accountability Office reported in April 2019 that the schedule and delivery of the first Columbia-class submarine is aggressive and leaves little room for error. The report stated, "The Navy's $115 billion procurement cost estimate is not reliable partly because it is based on overly optimistic assumptions about the labor hours needed to construct the submarines."[57]

The ICBM force, the land-based leg of the triad, consists of 400 single-warhead Minuteman III missiles deployed in underground silos dispersed across several states. The first missiles were installed in 1962, with the latest version, the Minuteman III, fielded in 1970. The DoD has initiated a program to begin the replacement of Minuteman III in 2029. The program will also modernize the 450 ICBM launch facilities that will support the fielding of 400 ICBMs. At the Air Force Association's September 2019 Air, Space, and Cyber Conference, General Timothy Ray, the Commander of Air Force Global Strike Command, stated, "We're living with a very ancient fleet."

The bomber leg of the triad consists of 46 nuclear-capable B-52H and 20 nuclear-capable B-2A "stealth" strategic bombers. At the September 2019 Air, Space, and Cyber Conference, General Ray similarly stated, "Many of these bombers are very old . . . and the planned replacement bomber, the B-21s, are years away from production."

The DoD has begun a program to develop and deploy the next-generation bomber, the B-21 Raider. It will first supplement and eventually replace elements of the conventional and nuclear-capable bomber force beginning in the mid-2020s. Along with the concerns about the age of the aircraft, General Ray cautioned, "[t]here are currently only 156 U.S. strategic

[57] Report No. GAO-19-497, "Columbia Class Submarine: Overly Optimistic Cost Estimate Will Likely Lead to Budget Increases," April 8, 2019.

bombers. But studies have shown that between 225 and 386 are needed" to deter adversaries and win in any conflict.

For the current and future nuclear-capable bombers to reach their intended targets, aerial refuelers (tankers) are required. In May 2019, the DoD OIG began an evaluation to determine whether the Air Force has mission-capable air refueling aircraft and aircrew to meet U.S. Strategic Command's nuclear deterrence requirements. This evaluation focuses on the KC-135 aircraft nuclear mission readiness, associated aircrew nuclear mission readiness, and the required installation support needed to meet U.S. Strategic Command's requirements.

Beginning in 1982, B-52H bombers were equipped with air-launched cruise missiles. The B-52H can stay outside adversary air defenses to increase its survivability against surface-to-air missiles and enemy aircraft. The AGM-86B is the only air-launched missile in the U.S. inventory with a nuclear warhead. As a result, it plays a pivotal role in the U.S. Government's strategic deterrence policies. The AGM-86B air-launched cruise missile, however, is now more than 25 years past its design life, and it was not designed to penetrate state-of-the-art air defenses in the 2020s or beyond.

According to the Air Force, the long-range standoff cruise missile replacement program is being designed to improve the capabilities of the current air-launched cruise missile, such as being able to operate in a Global Positioning System-denied environment, which requires the replacement missile to navigate toward its target if its satellite signals were jammed.

In 2015, the new long-range standoff cruise missile was delayed for 3 years for higher Air Force priorities. In 2017, the U.S. Air Force awarded contracts to begin preliminary work on the replacement cruise missile. The defense contractors were awarded agreements valued at $900 million apiece and lasting close to 5 years "to mature design concepts and prove developmental technologies." The Air Force expects to choose the winning design in 2022, and the missile is expected to become operational in 2030. Similar to the replacement of the ballistic missile submarine, however, there is little room for error in the cruise missile replacement program schedule.

The current non-strategic nuclear force consists exclusively of a relatively small number of B61 gravity bombs carried by F-15E and allied dual capable aircraft. These bombs provide a fallback option against extremely powerful conventional aggression and to deter enemy use of nuclear weapons in a previously conventional war. The United States is incorporating nuclear capability on the F-35 advance jet fighter as a replacement for the aging F-15E aircraft. In conjunction with the ongoing life extension program for the B61 bomb, the F-35 will be a key contributor to nuclear deterrence. However, the General Accountability Office has identified risks to the B61 life extension program and the F-35.[58]

Moreover, modernization and replacement of nuclear weapons and delivery systems has the inherent risk of the supply chain being compromised by malicious code or malware. For example, an August 2019 GAO report stated that according to Department of Energy and National Nuclear Security Administration documents:

[58] Report No. GAO-18-456, "B61-12 NUCLEAR BOMB: Cost Estimate for Life Extension Incorporated Best Practices, and Steps Being Taken to Manage Remaining Program Risks," May 31, 2018 and GAO19-321, "F-35 AIRCRAFT SUSTAINMENT: DOD Needs to Address Substantial Supply Chain Challenges," April 25, 2019.

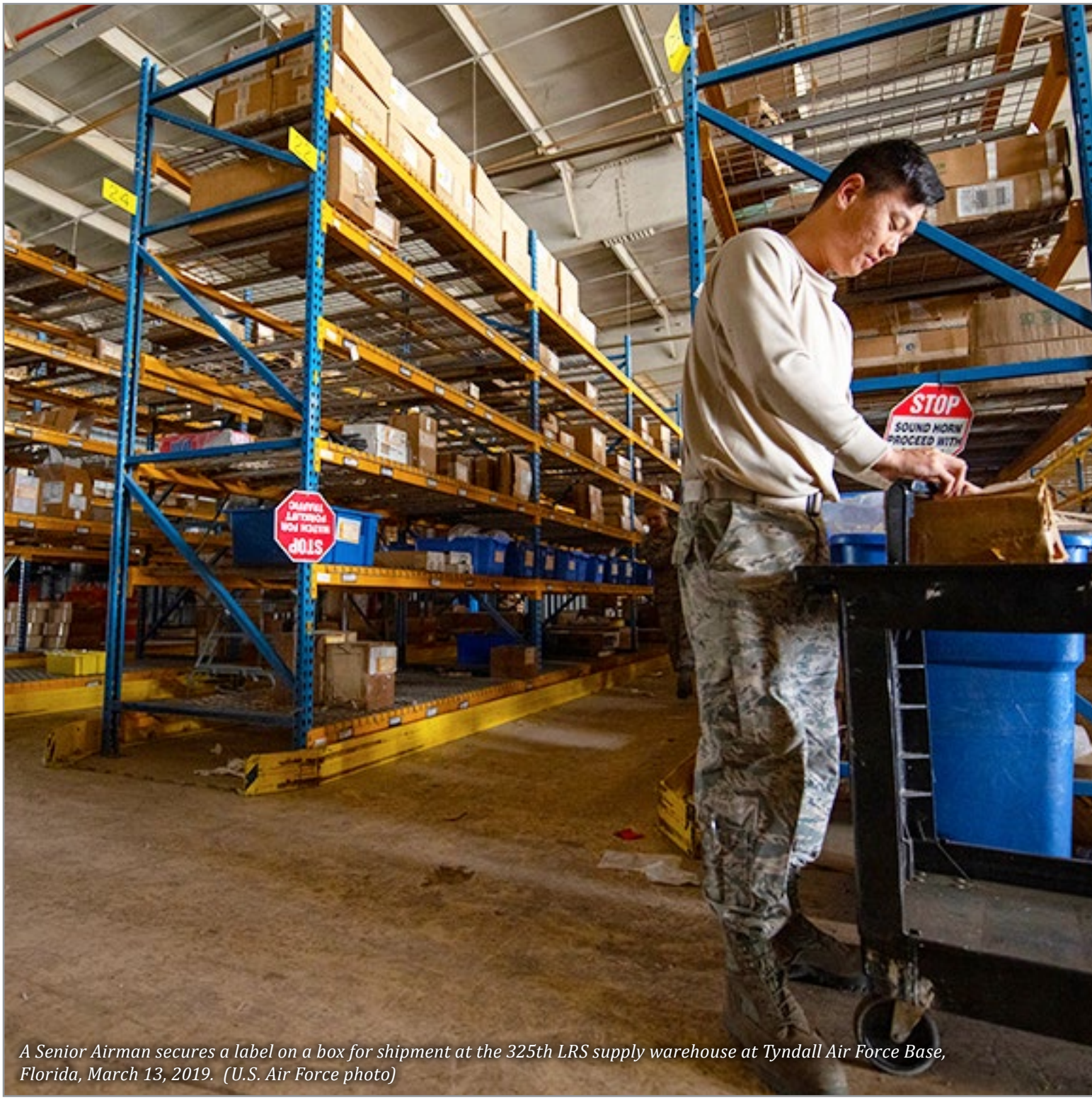
> a counterfeit or sabotaged component could cause a nuclear weapon to malfunction. Moreover, some reports have suggested that as components of nuclear weapons or delivery systems are being assembled, an adversary could introduce into the components malicious code or malware that could be activated at any time, thereby undermining confidence in the nuclear weapons systems and their operational effectiveness.[59]

The DoD OIG is now conducting an audit, in response to a congressional requirement, to determine whether the DoD has implemented supply chain risk management for a U.S. nuclear weapons delivery system in accordance with DoD requirements. The challenges related to supply chain management are highlighted in Management Challenge 8, "Improving Supply Chain Management and Security."

In summary, the United States faces rapidly growing threats in space, missile defense, and nuclear deterrence. Anti-satellite weapons and ground-based lasers threaten both the commercial and military uses of space. Adversaries are investing in their missile capabilities, enhancing their ground- and sea-launched missile arsenals with short-, intermediate-, and intercontinental-range systems, and placing the United States and its allies in significant danger.

Along with the ballistic missile threat, the United States now faces a threat from hypersonic missiles, which could strike the continental United States in under 15 minutes—less time than the United States is currently prepared to react. In addition, the DoD's nuclear submarines, land-based missiles, and bombers are reaching the end of their service life. To ensure that the United States maintains its dominance in these areas, and to protect the United States and its allies, the DoD must modernize and replace these systems to meet current and future threats.

[59] Report No. GAO-19-606R, "Nuclear Supply Chain: NNSA Should Notify Congress of Its Recommendations to Improve the Enhanced Procurement Authority," August 8, 2019.



A Senior Airman secures a label on a box for shipment at the 325th LRS supply warehouse at Tyndall Air Force Base, Florida, March 13, 2019. (U.S. Air Force photo)

Challenge 8. Improving Supply Chain Management and Security

The DoD's supply chain is essential to warfighter readiness. To support the warfighter, the DoD supply chain designs, manufactures, produces, packages, handles, stores, transports, maintains, and disposes of materials and goods that are used for DoD equipment and weapons systems that are needed to ensure readiness and accomplish DoD operations.

The DoD supply chain has faced longstanding problems, such as limited sources of supply, and challenges in distributing and transporting goods to remote locations. Ultimately, deficiencies in the DoD's supply chain can result in reduced readiness for service members because they do not have what they need, in the right place, at the right time.

The DoD supply chain requires improvements from end-to-end, beginning with the DoD obtaining the needed materials through the transportation and storage of those materials. Also, the DoD must ensure that it manages and tracks its materials throughout the supply chain.

The supply chain includes not just materials and goods, but also information technology used by the DoD. If the DoD does not adequately protect against and mitigate supply chain risks on its information technology networks, the networks risk infiltration and compromise. Recognizing these longstanding challenges, the 2018 National Defense Strategy calls for the DoD to build a more resilient and agile logistics capability, which requires a supply chain that is responsive to changes in priorities, demand, sources of supply, and distribution.

Commercial, public, and private businesses and organizations that participate in the DoD's supply chain are collectively known as the Defense Industrial Base. The DoD supply chain, which includes DoD Components and the Defense Industrial Base, is the interconnected web of people, technology, information, and resources that get a product from suppliers to the warfighter.[60] The DoD needs a Defense Industrial Base that is secure, robust, and able to meet the DoD's readiness requirements. However, a 2018 DoD report on the Defense Industrial Base and supply chain resiliency concluded that the Defense Industrial Base is challenged by

[60] GAO-18-667T Testimony, "Information Security: Supply Chain Risks Affecting Federal Agencies," July 12, 2018.

diminishing and sole sources for materials, supplies, and manufacturing, as well as a lack of cyber or physical security over products.[61] These conclusions are similar to DoD OIG and GAO findings.

Although the DoD has several ongoing initiatives that can help improve the DoD's supply chain, the DoD OIG and the GAO continue to identify shortcomings in the DoD's supply chain and logistics.

DIMINISHING SUPPLIERS AND RELIANCE ON SOLE-SOURCE SUPPLIERS

Recent reductions in the number of suppliers from which the DoD can purchase raw materials and finished goods affects the DoD's ability to obtain necessary supplies. Because of the specialized nature of DoD supplies, there are often a limited number of sources that can provide what the DoD needs and often these are sole-source manufacturers, meaning that they are the only vendor that can make a particular item. For example, the 2018 DoD report on the Defense Industrial Base and supply chain resiliency discussed a sole-source item, chaff, that is vital to aircraft defense. Chaff is composed of millions of tiny aluminum or zinc-coated fibers that are ejected behind an aircraft to confuse a missile's radar system. However, defense-unique requirements and decreasing DoD demand drove out other suppliers, leaving one company as the only source for chaff.

Diminishing sources combined with increasingly obsolete material, which occurs when materials are no longer made or available for purchase, can affect weapon systems. For example, missing a critical safety part can prevent a weapon system from being used for training or missions. In the case of obsolete materials, the DoD must find alternative sources or re-design parts with materials that are readily available. However, the DoD may not own the technical data for parts that are often associated with a sole-source manufacturer, which affects the DoD's ability to repair parts or have another vendor manufacture a part. The technical data are the information, drawings, specifications, and other relevant data that the DoD needs to enable alternative sources to manufacture or repair a specialized part.

The 2018 DoD report on Defense Industrial Base and supply chain resiliency stated that diminishing sources for supplies and the use of sole source suppliers are single points of failure within the Defense Industrial Base. The report stated that specialty manufacturers critical to the production of parts for DoD weapon systems have lost contracts since FY 2010 because of budget cuts and continuing resolutions. For example, according to the report, the single domestic source for a part within rotary wing gearboxes filed for bankruptcy in 2016 because of reduced DoD contracts. Without this part supplier, programs such as the AH-64E Apache, V-22 Osprey, and CH-53K Heavy Lift Replacement Helicopter are at risk for reduced readiness once the DoD uses the on-hand stock of those parts and until the DoD identifies an alternative source.

In addition, the parts needed to maintain weapon systems are often backordered, sometimes for years, forcing the Military Services to cannibalize weapon systems—moving working parts from one system to another—to ensure each system meets the minimum readiness requirements for mission capability. Cannibalization increases the risk of damage to both the part being removed and

[61] DoD, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," September 2018.

reinstalled and to other parts of the weapon system that are exposed during the removal and reinstallation process. For aircraft, this is a major concern in achieving readiness. According to an April 2019 GAO report, it is unlikely that the DoD will reach its September 2019 goal for 80 percent readiness of its fighter jets because of backordered parts.[62] With respect to this issue, the DoD OIG has an ongoing audit on whether the DoD identified and obtained the spare parts for the F/A-18 E/F Super Hornet, a fighter and attack jet, needed to meet readiness requirements.

The supply chain also faces risks from foreign sources. The 2018 DoD report on the Defense Industrial Base and supply chain resiliency stated that the DoD must rely on foreign sources when the domestic industry does not produce an item or cannot produce it in sufficient quantities. However, the risk to the supply chain is greater when the DoD depends on strategic competitors, such as China. For example, the report stated that China is the sole source or primary supplier of critical energetic materials used in munitions and missiles. In many cases, no alternative material can be used or the cost of using the alternative is high. The report indicated that the DoD, in an effort to address this risk, is cultivating new suppliers for these types of materials in places within the United States, as well as with allied nations. For example, according to the FY 2018 DoD report, there was only one domestic source of ammonium perchlorate, a chemical widely used in DoD propulsion systems. Foreign sources exist, but maintaining a domestic capability is critical to national security. The DoD OIG is conducting an audit to determine whether the pricing for ammonium perchlorate was fair and reasonable.

Additionally, acquisition from sole sources increases costs because there is no competition among multiple suppliers. As the DoD OIG concluded in its report on parts the DoD purchased from TransDigm, sole-source manufacturing can result in excessive costs to the DoD.[63] The DoD OIG reported that TransDigm earned $16.1 million in excess profits for 46 parts it sold to the DoD for $26.2 million between January 2015 and January 2017. The excess profits ranged from 17 percent to 4,451 percent on the 46 parts. Additional information about TransDigm and issues related to sole-source manufacturing are discussed in Management Challenge 9, "Acquisition and Contract Management."

The DoD reported that it is has begun to identify solutions to mitigate the challenges from diminished sources, obsolete material, and lack of technical data rights, through initiatives such as strategic sourcing, reverse engineering, and additive manufacturing. For example, the Office of the Chief Management Officer's FY 2019 initial plan for reforming DoD business operations identified a goal to improve the buying power of the DoD, increase transparency in the procurement process, and implement best practices in cost and contract management by strategically sourcing.[64] To accomplish this goal the DoD plans to use data analytics to make data-driven procurement decisions, identify high-priority sustainment items, and integrate best practices into the procurement process.

Another DoD initiative is reverse engineering, which is the process of examining an item, such as a spare part, with the intent of replicating its design. According to the GAO, from FY 2015

[62] Report No. GAO-19-321, "F-35 Aircraft Sustainment: DoD Needs to Address Substantial Supply Chain Challenges," April 25, 2019.

[63] Report No. DODIG-2019-060, "Review of Parts Purchased From TransDigm Group, Inc.," February 25, 2019.

[64] Office of the Chief Management Officer, "Initial Plan for Reforming the Business Operations of the Department of Defense," April 26, 2019.

through FY 2018, the Defense Logistics Agency initiated over 1,600 reverse engineering projects.[65] Although less than 10 percent of the more than 1,600 projects were successfully completed, some of those completed projects have resulted in lower prices. For example, according to Defense Logistics Agency data, the agency saved at least $22 million from the successful reverse engineering projects.

Additive manufacturing, often referred to as 3-D printing, creates an object by adding layers of material from three dimensional data, unlike traditional or subtractive manufacturing processes where the product is created by cutting away material from a larger piece. The DoD OIG is conducting an ongoing audit to determine the extent the DoD used additive manufacturing for parts to sustain equipment and weapon systems and the extent of the coordination of additive manufacturing across the DoD. Figure 16 shows the subtractive and additive manufacturing processes.

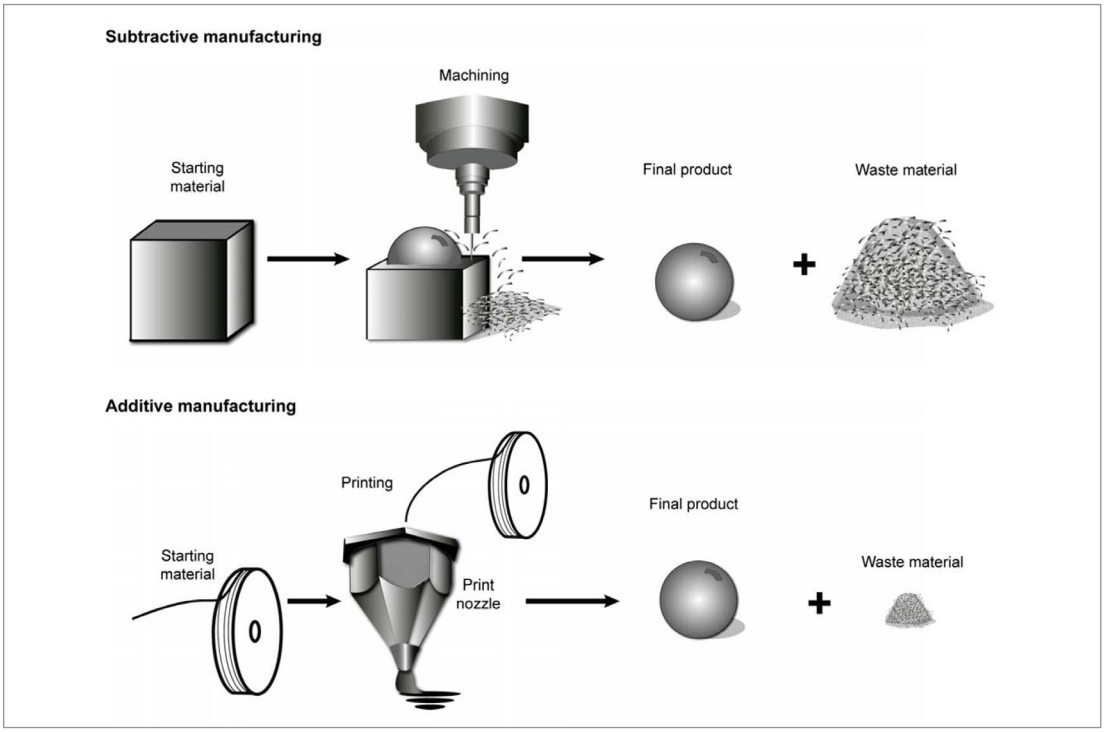
REPAIRING EXISTING PARTS ECONOMICALLY AND EFFICIENTLY

Many parts in the supply chain are either consumable (disposed of after use) or need to be repaired. Both DoD and contractor personnel repair parts at military installations, contractor facilities, or depots. Depot maintenance is generally the most involved level of maintenance, with equipment being completely overhauled, upgraded, or rebuilt.

The DoD faces challenges in controlling the cost and amount of time it takes to repair parts, regardless of whether the DoD or contractors make the repairs. For example, an April 2019 GAO report on F-35 aircraft sustainment determined that from May through November 2018, the F-35 Lightning II, a

[65] Report No. GAO-19-586, "Defense Logistics Agency: Small Businesses Participate in Reverse Engineering of Spare Parts," July 31, 2019.

Figure 16. Subtractive and Additive Manufacturing Processes



Source: The GAO.

stealth fighter jet, did not achieve its minimum readiness goals, in part because of delays in repairing spare parts.[66] During that time, there was a backlog of more than 4,000 parts waiting to be repaired and the average time to repair a part was more than twice the F-35 Program's goal for part repairs.

One of the Office of the Chief Management Officer's goals is to improve military readiness by reducing repair time at the depots.[67] The Office of the Chief Management Officer issued data calls in the first quarter of FY 2019 and intends to use the data to develop and implement metrics that measure the accuracy of maintenance planning while simultaneously measuring the costs created by a lack of parts.

The DoD OIG is conducting an ongoing audit related to another aspect of parts repair, called the beyond economical repair process, which is a process the DoD uses to decide whether to repair a part or purchase a replacement part. If it is not economical to repair a part, based on cost or time, the DoD will order a replacement part instead.

The DoD OIG also intends to conduct audits on depot-level maintenance in FY 2020 to determine the extent that the maintenance for surface ships, fixed-wing engines, heavy lift helicopters, and repairable electronics meet DoD and Service-level readiness and sustainment requirements.

To streamline the repair process and identify maintenance needs, the DoD has also attempted to use automated tools and data analytics more extensively. The results of these efforts are mixed. The F-35 Program intended to use an automated information technology system on F-35 aircraft to update the status of parts, generate supply work orders, and communicate critical data about parts to the DoD and contractor. However, in its April 2019 report on F-35 aircraft sustainment, the GAO determined that these capabilities are immature, resulting in the need for maintainers and supply personnel at military installations to perform time-consuming, manual workarounds to manage and track parts. One Air Force unit estimated that it spent the equivalent of more than 45,000 hours per year performing additional tasks and manual workarounds because the automated system did not function as intended.

A primary problem with data analytics efforts to analyze maintenance information is the lack of accurate records. For example, in March 2019, the Marine Corps reported that analysts spent 80 percent of their time reviewing and correcting maintenance data instead of analyzing the data. The time-consuming requirement for correcting data was caused by the poor quality controls over the data going into Marine Corps data collection systems. For example, the Marine Corps attempted to collect maintenance data for its 397 M1A1 Abrams tanks, which are heavily armored, highly mobile tanks designed for modern ground warfare. However, when the Marine Corps collected the data, there were 1,224 tank serial numbers, instead of 397. Without accurate basic information, such as a complete list of serial numbers, maintenance actions cannot be tied to specific tanks, and usage patterns for predictive maintenance capabilities cannot be identified.

---

[66] Report No. GAO-19-321, "F-35 Aircraft Sustainment: DoD Needs to Address Substantial Supply Chain Challenges," April 25, 2019.

[67] Office of the Chief Management Officer, "Fiscal Year (FY) 2020 Annual Performance Plan & FY 2018 Annual Performance Report," February 22, 2019.

FRAUDULENT SUPPLIERS IN THE SUPPLY CHAIN

Fraudulent suppliers also can disrupt the supply chain by intentionally failing to provide the DoD with parts or by intentionally providing the DoD with parts and materials that the DoD cannot use. When the DoD does not receive the parts it paid for or those parts are unusable, the parts must be re-ordered, which wastes time and money. Of greater concern is if one of these substandard, or even counterfeit, parts ends up on a major weapon system and fails to work properly. The results could be catastrophic.

There are generally three categories of unusable parts:

- **Counterfeit.** Identity or characteristics of the parts are deliberately misrepresented, falsified, or altered without the legal right to do so.
- **Defective.** Parts do not work as required.
- **Nonconforming.** Parts are not produced, tested, or inspected as required.

There is a high volume of parts coming into the DoD supply chain that do not undergo a robust quality control and Government acceptance procedure to ensure that incoming parts meet Government quality standards. In FY 2020, the DoD OIG plans to perform an evaluation of the Defense Logistics Agency's detection methods for identifying counterfeit parts.

The GAO and the DoD OIG both issued reports in September 2019 on weaknesses in DoD internal controls and processes that are designed to prevent fraudulent suppliers and unusable parts from entering the DoD supply chain.[68]

The DoD OIG's Defense Criminal Investigative Service (DCIS) investigations seek to deter counterfeit, defective, and nonconforming parts being provided to the DoD, and to have the perpetrators prosecuted in appropriate cases. Recently, DCIS has begun using data analytics to detect potentially fraudulent suppliers in the supply chain. In addition, DCIS partners with other Federal law enforcement agencies, DoD supply centers, and the Defense Industrial Base to investigate allegations that DoD contractors are not providing the correct parts and components to meet contract requirements.

LIMITED DISTRIBUTION NETWORKS AND TRANSPORTATION CAPABILITIES

Another challenge within the supply chain is transporting the supplies to the right place at the right time, safely and securely. Even when items arrive in a timely manner, it is necessary to ensure the safety, security, and visibility of those items in transit to prevent damage or loss. In the case of shipping arms, ammunition, and explosives, deficiencies in security procedures can result in accidents and risks to public safety. Furthermore, transit delays in the DoD's distribution networks and transportation routes can affect operations and warfighter readiness.

The Military Services, along with U.S. Transportation Command (USTRANSCOM) and its subordinate commands, transport DoD parts, supplies, and equipment around the world. The Army, Navy, and Air Force each lead subordinate commands within USTRANSCOM to ship items by ground, sea, and air. The DoD OIG has an ongoing audit of the ground transportation and secure storage of arms, ammunition, and explosives within the United States and plans to conduct an audit in FY 2020 on sea transportation and secure storage of

[68] Report No. GAO-19-549SU, "Ongoing DoD Fraud Risk Assessment Efforts Should Include Contract Ownership," September 12, 2019 and Report No. DODIG-2019-127, "Audit of Access Controls in the Defense Logistics Agency's Commercial and Government Entity Code Program," September 30, 2019. (Restricted)

Florida National Guard Soldiers and Airmen, from the CBRN Enhanced Response Force Package (CERFP), load equipment and prepare for potential missions responding to Hurricane Dorian. (U.S. Air Force photo)

arms, ammunition, and explosives. The DoD OIG also has an ongoing audit of the military ocean terminals to determine whether the physical security at the terminals meet DoD requirements.

In testimony to the Senate Armed Services Committee in April 2018, the USTRANSCOM Commander stated that in 2015 USTRANSCOM identified gaps in meeting the Joint Force's transportation requirements related to transparency, affordability, and asset visibility. To seek to ensure these requirements are met, USTRANSCOM began to develop and perform a proof-of-principle test of a transportation management system, a single platform for end-to-end shipment planning and execution, similar to those used by major manufacturers and distribution companies, such as Amazon and Walmart. According to the USTRANSCOM Commander, the proof-of-principle results, completed in FY 2018, validated that a transportation management system would improve warfighter support by streamlining transportation and financial management processes, enhancing enterprise-wide asset visibility and flexibility, and increasing readiness. With these initial results, the USTRANSCOM Commander decided to move ahead with implementation, beginning with a full-scale prototype.

Shipping supplies to remote locations that do not have accessible airports or seaports, such as locations in the U.S. Africa Command (USAFRICOM) area of responsibility, are another significant challenge in the supply chain. As stated in February 2019 testimony from the USAFRICOM Commander to the Senate Armed Services Committee, the main issue with logistics in Africa is the lack of infrastructure.

Sailors run past the foul line as a SA-330J Puma picks up pallets from the flight deck of USS Ashland. (U.S. Navy photo)

For example, in West Africa, one of USAFRICOM's newest and most important initiatives is the development of the West Africa Logistics Network. The network provides and positions aircraft throughout western and central Africa to facilitate the distribution of supplies, personnel, and equipment to support locations. Before the network, all supplies going to Africa, a continent more than three times the size of the continental United States, would fly in and out of Ramstein, Germany. In East Africa, 90 percent of all logistics and materiel for U.S. operations go through a port in Djibouti, making it imperative for USAFRICOM to maintain access to this strategic port. However, Djibouti, a nation about the size of New Jersey, is congested with forces from the United States, France, Germany, Japan, and China, who maintain bases and compete for access and airspace.

Another example of logistics challenges in the DoD are distribution networks, which are the interconnected group of storage facilities and transportation systems that receive inventories of goods and then deliver them to customers. Ineffective distribution networks can also affect readiness. For example, an April 2019 GAO report on F-35 sustainment determined that the DoD's network of manufacturers, depots, and warehouses for moving parts around the world was a factor in shortages of F-35 spare parts.

In addition to moving parts, the DoD also transports munitions through distribution networks. An FY 2019 DoD OIG audit identified issues with the availability of sealift capabilities that could negatively impact the ability of U.S. Indo-Pacific Command and the United States Forces Korea's munitions distribution network to meet customer needs.[69]

The DoD also uses preposition locations to store supplies and equipment until needed. These items must be stored appropriately

[69] Report No. DODIG-2019-099, "Audit of the Distribution of Preferred Munitions in Support of the Republic of Korea," June 24, 2019. (Classified)

so they are not damaged or destroyed before use. In a 2018 DoD OIG audit of Army and Marine Corps prepositioned stocks in the U.S. European Command area of responsibility, the DoD OIG determined that the Services did not effectively manage the storage and maintenance of prepositioned stocks.[70] For example, the Army and Marine Corps officials did not ensure proper storage facility humidity levels, weapons maintenance, or vehicle maintenance. Without adequately managed prepositioned equipment, the Army and the Marine Corps may not be ready to fully support a request to provide immediate crisis response when the need arises in Europe or Africa.

ASSET VISIBILITY AND PROPERTY ACCOUNTABILITY

It is also essential for the DoD to know what property and equipment it has available, and who is responsible for those items. However, the DoD struggles to account for its property as it moves through the supply chain, which can have harmful consequences. When the DoD does not know what supplies it already has, it may order more unnecessarily. When the DoD does not know the condition of those supplies, it may be unaware that supplies were damaged and need to be reordered.

When the DoD accurately accounts for its supplies and tracks their use, it can better forecast for its future needs and potentially eliminate or reduce backordered supplies and parts. Tracking also helps the DoD identify the useful life and maintenance requirements for parts. If useful life and maintenance requirements are not properly maintained, this can create a life and safety concern if the part is critical to a weapon system's capabilities.

When the DoD does not accurately record its property, it affects the financial statements by misstating either assets or expenses, depending on the type of property. For additional information on the DoD's financial statements, see Management Challenge 5, "Financial Management."

For example, in FY 2019 the DoD OIG performed audits that identified the DoD's failure to properly track property on Air Force Contract Augmentation Program IV and for the F-35 Program. The DoD OIG determined that officials did not record 2,081 of 2,091 pieces of property in the Air Force's system.[71] The DoD OIG also determined that the F-35 Program had no record of Government property and relied entirely on the contractor for that information. The contractor stated that it had 3.45 million pieces of F-35 property at a cost of $2.1 billion.[72] Without accurate records, F-35 Program officials had no visibility over the property and could not hold the prime contractor accountable for how it manages Government property.

To enhance property accountability, a May 2019 Under Secretary of Defense for Acquisition and Sustainment memorandum directed DoD officials to collect inventory reports to establish a baseline for Government property and appropriately record the information. In addition, the DoD established the Item Unique Identification Program to improve provide reliable accountability of property and asset visibility throughout the life cycle. Upon acceptance of Government-furnished property or new DoD acquisitions, the DoD assigns a unique, machine-readable character string or number to the item and tracks it throughout its life cycle using a central repository for item

[70] Report No. DODIG-2018-152, "Management of Army and Marine Corps Prepositioned Stocks in U.S. European Command," September 17, 2018.

[71] Report No. DODIG-2019-103, "Audit of U.S. Air Force Contract Augmentation Program IV Government Furnished Property," July 18, 2019.

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

unique identification information. The program is intended to help the DoD achieve lower life-cycle cost and improve life-cycle property management; improve operational readiness; and ensure item-level traceability throughout the life cycle to strengthen supply chain integrity, enhance cybersecurity, and combat counterfeiting. The DoD OIG plans to conduct an audit of the Item Unique Identification Program in FY 2020 to determine whether parts or subcomponents on DoD critical weapon systems have item unique identification in compliance with DoD and contract requirements.

INFORMATION TECHNOLOGY AND CYBERSECURITY IN THE SUPPLY CHAIN

In addition to accounting for its supplies, the DoD must secure and protect the information technology systems used in its supply chain. The DoD relies on many types of information technology, including classified and unclassified computer networks; cloud-based and on-premises databases and software applications; and software, hardware, and firmware on weapons systems. Cybersecurity attacks have the potential to cause major disruption in manufacturing operations. In addition, reliance on foreign suppliers and the dominance of foreign suppliers in the information technology sector put the supply chain at risk.

When DoD Components do not fully implement supply chain risk management policies for their systems, those systems face an increased risk that an adversary could infiltrate the supply chain and sabotage, introduce an unwanted function, or otherwise compromise the design or integrity of the systems' critical hardware, software, and firmware. For example, according to an October 2018 news article, China used a microchip attached to motherboards on servers that allowed China to create a back door into any network linked to the servers. These servers were used in DoD data centers and on Navy ships.

According to the USTRANSCOM Commander's April 2018 testimony to the Senate Armed Services Committee, threats in the cyber domain also pose the greatest threat to the DoD's logistics advantage. He stated that the logistics enterprise is more susceptible to malicious cyber activities than other military organizations based on the DoD's unique relationship with commercial partners. Although logistical and operational planning generally takes place on classified networks, 90 percent of military logistics and global movement operations are executed on unclassified commercial networks that do not implement DoD-level cybersecurity controls.

Information technology in both military and commercial-off-the-shelf products are also at risk. For example, a DoD OIG audit determined that the Missile Defense Agency has established several initiatives to manage supply chain risk for the Ground-Based Midcourse Defense System.[73] However, the Missile Defense Agency did not fully implement DoD supply chain risk management policy because it had incomplete supplier lists to perform its risk assessments, and its risk assessments were too limited in scope to satisfy requirements. Therefore, the system was at risk for exploitation by adversaries.

In an audit of DoD purchases of commercial-off-the-shelf information technology, the DoD OIG determined that the DoD purchased

[73] Report No. DODIG-2017-076, "The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System," April 27, 2017.

items with known cybersecurity risks.[74] Specifically, in FY 2018, the Army and Air Force purchased at least $32.8 million of commercial-off-the-shelf information technology items with known cybersecurity vulnerabilities. As a result, adversaries potentially could exploit known cybersecurity vulnerabilities that exist in some commercial-off-the-shelf items purchased by the DoD.

The DoD OIG is also conducting an evaluation of whether DoD Components are conducting appropriate risk assessments, implementing risk mitigation strategies, and using continuous monitoring procedures throughout U.S. Indo-Pacific Command's supply chain. The evaluation will determine whether there was foreign intrusion into U.S. Indo-Pacific Command's intelligence, surveillance, and reconnaissance supply chain and whether such intrusion was due to the lack of appropriate risk management by the DoD Components.

Recognizing cybersecurity risks, the DoD Office of the Chief Management Officer has announced a plan to implement various cyber supply chain risk management activities, which includes improving supplier threat assessment collection and analyses; implementing methods to mitigate risk, such as improved hardware and software testing; and enhancing processes for approved product and vendor lists.[75]

Despite these initiatives the DoD needs to implement further improvements. For example, the Department of State issued a warning in May 2017 against using video surveillance equipment from two Chinese companies, citing cyber-espionage concerns. Despite the inherent risks associated with their use, DoD Components continued to purchase and use surveillance equipment from the Chinese companies to monitor installation security until Congress banned the Government from using them in August 2018. Congress took additional action in the National Defense Authorization Act for FY 2019 by: (1) preventing the DoD from obtaining telecommunications or video surveillance equipment or services produced or provided by an entity reasonably believed to be owned or controlled by, or otherwise connected to, China; and (2) requiring the DoD to develop a process to limit foreign access to technology to protect DoD information systems and to deter strategic acquisition of industrial and technical capabilities by foreign entities to protect the Defense Industrial Base.

In summary, the supply chain is an essential part of the DoD's efforts to ensure readiness. An agile and resilient supply chain and logistics capability allow the DoD to obtain the goods and services it needs to maintain equipment, support warfighter readiness, and secure DoD networks and systems. In addition, an effective supply chain can help the DoD prevent or mitigate the risks from receiving unusable parts or having limited sources of supply because an agile supply chain can find alternatives. However, the DoD faces many challenges in achieving these goals, and needs to continue to focus on strengthening the security and effectiveness of its supply chain.

---

[74] Report No. DODIG-2019-106, "Audit of the DoD's Management of Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items," July 26, 2019.

[75] Office of the Chief Management Officer, "Fiscal Year (FY) 2020 Annual Performance Plan & FY 2018 Annual Performance Report," February 22, 2019.

The first successful air-to-air refueling of an F-35 by a KC-46A tanker. The KC-46A represents the dawn of a new era in air-to-air refueling capability for the joint force and will provide next generation aerial refueling support to F-35s. (U.S. Air Force photo)

Challenge 9. Acquisition and Contract Management: Ensuring That the DoD Gets What It Pays For On Time, at a Fair Price, and With the Right Capabilities

Acquisition and contract management have been high-risk areas for the DoD for many years, and the DoD and Congress have sought to improve the acquisitions of major weapon systems. In recent years, Congress passed legislation to reform DoD acquisitions and to allow more timely and efficient ways to acquire weapon systems. For example, the National Defense Authorization Act for FY 2016 allows the DoD to use rapid acquisition authority (intended to be completed in 2 to 5 years) and streamlined alternative acquisition processes to acquire critical national security capabilities.

Other recent reforms involved splitting the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics into two offices—the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment. These new offices have distinct responsibilities—one office focuses on technology and innovation, and the other office focuses on acquisition development, production, procurement, and sustainment. The split also resulted in the shift of responsibility for managing major Defense acquisition programs from the Under Secretary of Defense for Acquisition, Technology, and Logistics to the Military Service Acquisition Executives.

While the DoD is implementing these reforms, however, many DoD programs still fall short of cost, schedule, and performance expectations. Acquisitions remain challenging because of the complexity of developing major systems. At the same time, the DoD must address cybersecurity challenges within the acquisition system and deter contractor fraud in DoD acquisition programs.

Moreover, the DoD does not define requirements for acquisitions consistently. As a result, acquisitions of weapons systems regularly result in cost overruns and program development can span decades, which reduce the capabilities delivered to the warfighter.

In addition to acquisitions, the DoD obligates hundreds of billions of dollars annually on contracts for goods and services. The DoD has had longstanding challenges in managing its contracts, such as difficulties in clearly defining requirements and fragmented and uncoordinated approaches to acquiring services.

The DoD OIG has regularly reported on acquisition and contracting problems in the DoD, with many recommendations for improvement. As of March 31, 2019, the DoD OIG had 395 open recommendations related to acquisition and contracting.[76] These recommendations focus on the management of major and non-major defense acquisition programs and seek to improve the DoD's ability to stay within budget, on schedule with program milestones, and achieve the required performance capabilities. The DoD OIG recommendations also address issues related to the award and oversight of contracts, such as selecting the appropriate type of contract and acquiring parts at fair and reasonable prices to support the procurement of acquisition programs and automated information systems for the DoD. However, until the DoD addresses these recommendations and applies lessons learned across the DoD, it will continue to experience acquisition challenges.

ACQUISITION AND SUSTAINMENT

DoD acquisition programs range from major programs, such as Virginia-class submarines and the F-35 Joint Strike Fighter, to smaller programs, such as tactical radios and precision guided missiles, bombs, and artillery shells. In the FY 2020 budget, the DoD requested

U.S. Air Force F-35A Lightning IIs (U.S. Air Force photo)

$247.3 billion to fund acquisition programs. From FY 2018 to FY 2019, the number of programs in the DoD portfolio of major defense acquisition programs increased from 87 to 89; however, the total planned investment in these programs has decreased from $1.85 trillion to $1.8 trillion. While the total planned investment may have decreased, the DoD has a history of exceeding planned acquisition costs for individual programs.

Some of the complexities that impact acquisition improvements include urgent operational needs for a system or service; reform efforts, which can create confusion regarding procedures and processes and introduce uncertainty for risk-adverse contracting officials, and the need to continually reassess requirements, including quantities, capabilities, and cybersecurity requirements. In addition, steady turnover of senior DoD officials, including Senior Executives and General Officers, can result in changing priorities and expectations with regard to weapons systems, which can also complicate the acquisition process.

ACQUISITION REFORMS

Congress included several acquisition reforms in recent National Defense Authorization Acts (NDAAs) that seek to streamline acquisition oversight and to field capabilities

[76] DoD OIG, "Compendium of Open Office of Inspector General Recommendations to the Department of Defense as of March 31, 2019," July 22, 2019.

faster. The Senate and House Armed Services Committees have regularly expressed concerns that without improving the speed of, and increasing the amount of innovation in, the DoD acquisition process, the U.S. military could lose its technological advantage. As a result, legislative reforms have altered roles and responsibilities for oversight of major defense acquisition programs to give significantly more authority for managing acquisition programs to the Military Departments. Specifically:

- Section 804 of the FY 2016 NDAA and Section 866 of the FY 2018 NDAA—Middle Tier of Acquisition for Rapid Prototyping and Rapid Fielding—provided the DoD with the authority to rapidly prototype and rapidly field capabilities distinct from the traditional acquisition system;
- Section 809 of the FY 2016 NDAA—Advisory Panel on Streamlining and Codifying Acquisition Regulations—recommended that the DoD adapt and deliver capabilities more efficiently, while ensuring that the DoD remained true to its commitment to promote competition, provide transparency in its actions, and maintain the integrity of the defense acquisition system;
- Section 825 of the FY 2016 NDAA—Designation of the Milestone Decision Authority— directed that the milestone decision authority for a major defense acquisition program shift from the Under Secretary of Defense to the Service Acquisition Executive of the Military Department that is managing the program, unless the Secretary of Defense designates another official to serve as the milestone decision authority; and
- Section 901 of the FY 2017 NDAA—Organization of the Office of the Secretary of Defense—directed a split of the Under Secretary of Defense for Acquisition, Technology, and Logistics into two offices, a new Under Secretary of Defense for Research and Engineering, and a renamed Under Secretary of Defense for Acquisition and Sustainment.

However, these reforms remain a work in progress. A 2019 Government Accountability Office report on the DoD's efforts to implement these acquisition reforms concluded that while the DoD has made progress in implementing reforms to shift the decision making authority from the Under Secretary of Defense to the Military Departments, the DoD has not fully determined how it will:

- oversee middle-tier acquisition programs, which focus on delivering a capability in a period of 2 to 5 years; or
- resolve disagreements with the oversight roles and responsibilities between the Under Secretary of Defense for Acquisition and Sustainment and the Military Departments.[77]

In addition to the more recent initiatives, the DoD was previously given the flexibility to use other transaction authorities for research, to develop prototypes, or for follow-on production of prototyped solutions. Other transaction authorities were originally introduced in the FY 1990 NDAA; however, the authorities have been more clearly defined and refined throughout the years and are now being used more prevalently within the DoD. Other transaction authorities are legally binding instruments other than procurement contracts, grants, or cooperative agreements that are not subject to Federal laws and regulations

[77] Report No. GAO-19-439, "DoD Acquisition Reform, Leadership Attention Needed to Effectively Implement Changes to Acquisition Oversight," June 5, 2019.

that govern procurement contracts and were created to give the DoD the flexibility necessary to adopt and incorporate business practices that reflect commercial industry standards and best practices into its contract award instruments. Other transaction authorities are intended to provide the DoD with alternative ways to access state-of-the art technology solutions from traditional and non-traditional defense contractors, through different potential arrangements tailored to each particular project.

The DoD OIG is conducting an audit to determine whether the DoD planned and executed other transactions awarded through consortiums in accordance with applicable laws and regulations for other transactional authority. A consortium is an association of two or more individuals, companies, or organizations pooling their resources to establish a relationship with the Government that otherwise may not have occurred and allow for the leveraging of industry-wide capabilities to solve DoD challenges in a specific technology or mission area. The challenge the DoD faces is to incorporate the flexibilities of the streamlined acquisition process while ensuring controls are in place to protect the Government's interest and military research and prototype information.

MANAGEMENT OF ACQUISITION PROGRAMS

The ultimate objective of an acquisition program is to obtain a capability that meets the warfighters' needs and supports the DoD's objectives in the National Defense Strategy. Because of the significant amount of money and the importance of acquisition programs to the DoD, the DoD must seek to manage these programs to ensure on-time delivery, at or under the budgeted price, and with the capabilities that are needed by the end user. However, the DoD has had difficulty with acquisitions that frequently exceed program budgets and established timelines. This can happen for a variety of reasons, including inadequate requirements development, software design changes, failed developmental or operational testing, and not providing proper oversight of contractors.

For example, according to the March 2019 Selected Acquisition Report, the Air Force B-2 Defensive Management System – Modernization program costs increased 10 percent, $285 million, because of system development scope increases. The B-2 Defensive Management System – Modernization program is a system of integrated antennas, receivers, and displays that will detect, identify, and locate enemy radar systems and provide real-time threat warning, threat avoidance, and threat situational awareness information to the B-2 aircrew. The scope increase was for a new capability and for new hardware installation throughout the aircraft.

With regard to another major acquisition system, a 2019 DoD OIG audit determined that the Army may not be able to afford production and sustainment of the Integrated Air and Missile Defense program because Army officials have not properly completed an affordability analysis for unit production and sustainment costs of the Integrated Air and Missile Defense system. Assessing life-cycle affordability of systems is essential for establishing the financial achievability of the program and setting realistic program baselines to control life-cycle costs and help instill more cost-conscious management in the development of the Integrated Air and Missile Defense program.[78]

[78] Report No. DODIG-2019-114, "Army Integrated Air and Missile Defense Program," August 19, 2019.

U.S. Navy MH-60R Sea Hawk helicopters (U.S. Air Force photo)

The DoD also has problems with oversight of smaller acquisition programs, commonly referred to as acquisition category 2 and 3 programs. Acquisition category 2 programs are major systems estimated to cost between $185 and $480 million for research, development, test, and evaluation or between $835 million and $2.8 billion for procurement. Acquisition category 3 programs are those programs that fall below the acquisition category 2 minimum thresholds for research, development, test and evaluation and procurement and automated information system programs that meet select criteria. Examples of these smaller acquisition programs include the Common Sensor Payload, a sensor that provides a robust suite of sensors to collect critical information for air-ground maneuver teams, and the P-5 Combat Training System, which provides urgent, near-term training capabilities to meet Air Force and Navy air combat training needs. However, Service Acquisition Executives need to provide adequate oversight no matter the program size and cost. The DoD OIG is conducting an audit to determine whether Army, Navy, and Air Force acquisition officials have proper oversight of acquisition category 2 and 3 programs.

CHANGES TO WEAPON SYSTEM QUANTITY

The DoD continues to face challenges in validating the correct quantities of weapon systems to procure. Since 2014, the DoD OIG has published six reports that have identified various issues with planned procurement quantities for a variety of weapons systems. For example, in June 2018, the DoD OIG determined that Army officials could not justify the planned procurement quantities of 85 training, 67 float, and 15 test AH-64E Apaches. The AH-64E Apache is an Army two-pilot, four-blade attack and reconnaissance helicopter. Army officials

did not conduct the analyses required by DoD and Army guidance to determine the necessary training, float, and test quantities before the Deputy Chief of Staff of the Army, G-8, approved the Apache acquisition objective. As a result, the DoD OIG audit concluded that Army officials cannot ensure that 167 AH-64Es for training, float, and test, valued at $3.5 billion, will meet the needs of the Army.[79]

In January 2019, the DoD OIG determined that the Navy had more MH-60R and MH-60S helicopters than it required to maintain readiness. The MH-60R and MH-60S helicopters are maritime combat weapon systems that will deploy on the Littoral Combat Ship, and the number of helicopters that are required is directly related to the number of Littoral Combat Ships that the Navy is procuring. However, the Office of the Chief of Naval Operations, Director of Air Warfare, did not receive notification of the Littoral Combat Ship's quantity changes and schedule delays, which would have indicated that the Navy did not need to procure as many helicopters as originally planned. As a result, the Navy spent $1.4 billion to purchase 57 helicopters that were in storage, and the Navy will spend more than $2 million annually to store these helicopters until at least 2020 when additional Littoral Combat Ships are delivered.[80]

CYBERSECURITY CHALLENGES WITHIN ACQUISITION

The DoD must also address cybersecurity in acquisitions. The DoD has to continuously defend its systems from cyber threats throughout the entire acquisition life cycle, from development through deployment and disposal. Cyber strategies to combat potential cyber attacks from strategic competitors, such as China and Russia, need to be adjusted for legacy systems, and cybersecurity needs to be an integral part of systems that are currently in development.

For example, in 2019, the DoD OIG identified a significant cybersecurity issue with one of the performance requirements for the Air Force B61-12 tail kit program.[81] The B61-12 is a 12-foot long, 825-pound nuclear bomb that an aircraft can drop on its targets. The tail kit controls the bomb's flight path using moveable control fins.

Additionally, the DoD OIG is currently conducting an audit to determine whether the DoD Components initially define and continuously update cybersecurity requirements based on known and intelligence-based cybersecurity risks, throughout the DoD weapon systems acquisition process. The challenges facing the DoD related to cybersecurity are discussed further in Management Challenge 6, "Enhancing DoD Cyberspace Operations and Capabilities."

In summary, acquisition reform, changing weapon system requirements, and cybersecurity requirements affect the ability of the DoD to field weapons systems on time, in the right quantities, and on budget.

CONTRACT MANAGEMENT AND OVERSIGHT

The DoD spends billions—more than $274 billion through the third quarter of FY 2019—on contracts for supplies, construction and

[79] Report No. DODIG-2018-130, "Procurement Quantities of the AH-64E Apache New Build and Remanufacture Helicopter Programs," June 25, 2018.

[80] Report No. DODIG-2019-047, "Navy and Marine Corps Backup Aircraft and Depot Maintenance Float for Ground Combat and Tactical Vehicles," January 18, 2019.

[81] Report No. DODIG-2019-080, "Audit of the B61-12 Tailkit Assembly Program," April 19, 2019 (Classified)

sustainment of facilities, commercial items, information technology, support for military bases and contingency operations in Southwest Asia, as well as other support and services. In these expenditures, the DoD must implement controls to ensure contractors meet contract requirements for delivering goods and services. However, the DoD continues to face challenges with obtaining fair and reasonable prices for contracts, providing adequate contract oversight, and overseeing the use of purchase cards that are used to obtain goods and services. In 2019, the Government Accountability Office reported that DoD contract management is still a high-risk area and stated that the DoD faces challenges in how it defines, strategically manages, and budgets for its contracted services.[82]

FAIR AND REASONABLE CONTRACT PRICING

Contracting officers need accurate and current data from contractors to establish fair and reasonable pricing for contracts. The DoD OIG has identified longstanding problems with pricing of contracts for spare parts, especially sole-source parts, in large part because of the lack of adequate cost data. For example, the lack of cost data available to the DoD for sole-source spare parts resulted in contracting officers awarding contracts that allowed contractors to obtain excessive profits. In 1998, the DoD OIG first identified that DoD contracting officers failed to obtain fair and reasonable prices for spare parts.[83] Additional audit reports since then have regularly identified that the DoD continued to have problems obtaining fair and reasonable prices for spare parts. In total, the DoD OIG has issued 37 reports that identified pricing issues related to DoD contracting since 1998. Twenty-five reports identified issues related to the DoD not receiving fair and reasonable prices for spare parts. Seventeen reports identified instances when the DoD did not obtain other than certified cost and pricing data or were provided inaccurate other than certified cost and pricing data from the contractor when purchasing commercial spare parts. Eleven reports identified that when purchasing noncommercial spare parts, the DoD performed inadequate analysis of historical prices, the DoD based price analysis on incomplete cost or pricing data, or contractors had excessive pass-through costs.

DoD contracting officers' use of certified or uncertified cost data to perform cost analysis of contracts is often the most reliable way to determine whether a price is fair and reasonable. However, certified cost data is only required for contracting officers to award contracts above a certain dollar threshold, which is established by the Truth in Negotiations Act. The threshold was raised in the FY 2018 NDAA from $750,000 to $2 million. Although the intent of raising the threshold was to streamline the acquisition process, it resulted in the DoD having less information to use during negotiations with contractors to determine a fair and reasonable price. If a contract is for the acquisition of a commercial item, the Federal Acquisition Regulation does not require certified cost or pricing data, even if the acquisition is above the Truth in Negotiations Act threshold. Current statutory and regulatory requirements state that obtaining uncertified cost and pricing data from a contractor should occur when it is the only means left to determine whether a price is fair and reasonable.

---

82 Report No. GAO-19-157SP, "High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on HighRisk Areas," March 6, 2019.

83 Report No. DODIG-98-064, "Audit Report on Commercial and Noncommercial Sole-Source Items Procured on Contract N000383-93-G-M111," February 6, 1998.

Recently, in a February 2019 audit report of spare parts purchased from TransDigm Group, Inc, the DoD OIG determined that the DoD had paid $16.1 million in excess profit to TransDigm. Specifically, of the 47 parts the DoD OIG reviewed, the DoD OIG found that TransDigm earned excess profit on spare parts, ranging from 17 percent to 4,451 percent on 46 spare parts that TransDigm and its subsidiaries sold to the DoD over a 3-year period. In total, for the 46 parts, which cost the DoD $26.2 million, TransDigm earned $16.1 million in excess of 15 percent. In some instances, DoD contracting officers had attempted to obtain from TransDigm the cost of making the part, to determine whether the price TransDigm sought to charge was reasonable. However, TransDigm was not required by law to provide the data and refused to provide it to the contracting officer. The only time that TransDigm provided cost data was for one part; for that part, it received a profit of less than 15 percent. The contracting officers negotiating with TransDigm had limited options once TransDigm refused to provide the requested cost data—either buy the spare parts without receiving cost data from TransDigm, or not purchase the spare parts needed to meet mission requirements, which could potentially impact the warfighter.[84]

As a result of the DoD OIG audit of TransDigm spare parts pricing and testimony before the House Oversight and Reform Committee, TransDigm voluntarily refunded the DoD $16.1 million in excess profits. The DoD OIG is currently conducting a comprehensive audit of TransDigm, including its business model and its impact on the DoD's ability to receive fair and reasonable pricing. However, the issue of the DoD paying more than fair and reasonable prices extends beyond TransDigm, and the DoD OIG plans to perform additional audits in this area.

In addition, the provisions in the proposed FY 2020 NDAA, if enacted, would give contracting officers more authority to require contractors to disclose pricing data for sole-source parts. On June 14, 2019, the Acting Director of the DoD's Defense Pricing and Contracting issued a policy that requires contracting officers to obtain uncertified cost or pricing data to support prices proposed by TransDigm and its subsidiaries unless the prices are based on adequate price competition or set by law or regulation.

Competition, or the lack thereof, also impacts whether the Government can get a good deal on a contract. For example, currently, an $85 billion contract for a ballistic missile for the Ground Based Strategic Deterrent, an Air Force nuclear weapons program, is being considered as a potential sole-source procurement. The Government intended for the contract to be competed between two major defense contractors; however, the contract may be awarded sole-source because one of the contractors that DoD expected to compete may not bid. The DoD estimated that the long-term cost of the program could be as much as $100 billion. Without competition, the DoD may not be able to negotiate the best price.

Contracting officers need to obtain the information to ensure that the DoD gets the best price for the warfighter. Until contracting officers can be assured access to the information to be wellinformed in negotiations with contractors, the DoD will continue to pay excessive prices for spare parts.

[84] Report No. DODIG-2019-060, "Review of Parts Purchased from TransDigm Group, Inc.," February 25, 2019.

CONTRACT OVERSIGHT

Inadequate contract oversight continues to be a challenge for the DoD, potentially costing it extra millions of dollars each year, creating life and safety concerns for the warfighter, and impacting the DoD's ability to prepare for and execute its missions. The DoD must carefully monitor the contractor's performance against the contract requirements to ensure that the DoD receives what it pays for. However, for many years, the DoD OIG has reported that the DoD does not consistently ensure that it receives what it paid for.

For example, in June 2019, the DoD OIG reported that the DoD did not receive ready-for-issue spare parts for the F-35, a supersonic, low observable stealth fighter capable of executing multirole missions, in accordance with the contract requirements. The DoD joint program officials did not conduct adequate oversight of contractor performance related to receiving F-35 spare parts and aircraft availability hours. As a result, since 2015, the DoD has spent up to $303 million in DoD labor costs incurred by DoD personnel to correct non-ready-for-issue parts problems, and it will continue to pay up to $55 million annually for non-ready-for-issue spare parts until the issue is resolved.

The lack of available ready-for-issue spare parts could also result in the F-35 fleet being unable to perform required operational and training missions. Until the DoD addresses the delivery of non-ready-for-issue spare parts, the use of manual processes to mitigate non-ready-for-issue problems can also create a life and safety concern for aircrews. For example, if DoD personnel make mistakes on the number of hours the spare part was flown when manually tracking hours for limited life non-ready-for-issue spare parts, the aircraft performance may be compromised.[85]

In addition, lack of adequate contract oversight can result in wasted funds. In 2019, the DoD OIG determined that U.S. Army Corps of Engineers (USACE) Huntsville and USACE Jacksonville contracting officials did not adequately monitor contractor labor hours worked or accurately review invoices to ensure contractor invoices corresponded to actual work performed on three Puerto Rico power grid repair and restoration contracts. As a result, USACE Huntsville contracting officials did not know whether contractor labor costs paid on 11 invoices, valued at $258.9 million, were allowable in accordance with the terms of the contracts. Based on testing of a sample of labor costs, the DoD OIG identified at least $20.9 million paid by USACE that was unsupported and potentially unallowable. Additionally, USACE Jacksonville contracting officials did not know whether contractor labor costs paid on seven invoices, valued at $61.3 million, were allowable in accordance with Federal regulations or terms of the contract. Based on testing of labor costs, the DoD OIG identified at least $29.2 million paid by USACE that was unsupported and potentially unallowable.[86]

DoD contracting personnel must remain vigilant in monitoring contractor performance to ensure the DoD receives goods and services in accordance with contract requirements. To address this challenge, the DoD needs an acquisition workforce that is trained to

[85] Report No. DODIG-2019-094, "Audit of F-35 Ready-for-Issue Spare Parts and Sustainment Performance Incentive Fees," June 13, 2019.

[86] Report No. DODIG-2019-128, "Audit of U.S. Army Corps of Engineers Oversight of Contracts for Repair and Restoration of the Electronic Power Grid in Puerto Rico," September 30, 2019.

ensure the appropriate types of contract awards, understand the complexity of contract requirements, and provide the level of oversight necessary to make sure that the DoD receives the goods and services it paid for.

USE OF PURCHASE CARDS

Improper use of Government purchase cards by the DoD costs the DoD millions of dollars each year. Since 2006, the DoD OIG has consistently identified weaknesses in the DoD Government purchase card program, such as weaknesses involving split purchases, prohibited purchases, and lack of supporting documentation.[87] For example, in 2019, the DoD OIG reviewed the Air Force Nonappropriated Fund Government Purchase Card Program which is used to support Morale, Welfare, and Recreation programs for military personnel, their family members, and authorized civilians. The DoD OIG statistically projected that cardholders made up to $23.3 million in potential improper payments on 45,737 of 312,261 purchases between July 2017 and June 2018. Additionally, Air Force cardholders were responsible for inconsistencies related to supporting documentation on up to 303,125 purchases totaling $167.3 million. Air Force Nonappropriated Fund cardholders did not have proper written authority to use the purchase card, did not maintain a proof of purchase, such as in-store receipts and invoices, and paid sales tax even though the DoD is exempt from paying taxes on purchase card transactions.

PROCUREMENT FRAUD

DoD acquisitions and contracts continue to be at high risk for fraud. The Defense Criminal Investigative Service (DCIS), the DoD OIG's criminal investigative component, investigates allegations of procurement fraud by DoD contractors. In FY 2019, DCIS initiated approximately 100 investigations involving procurement fraud allegations of defective pricing, cost and labor mischarging, and false claims. DCIS also successfully resolved allegations of contractors submitting false claims, overbilling for labor hours, and submitting false documents to indicate completion of contract requirements. While each procurement fraud investigation is different in scope, they typically involve a contractor exploiting a vulnerability in the acquisition process.

For example, DCIS conducted a joint investigation with several agencies, including U.S. Army Criminal Investigation Command (CID), Air Force Office Special Investigation (AFOSI), and the Naval Criminal Investigative Service involving E.M. Photonics (EMP). EMP was awarded multiple grants and contracts under the DoD Small Business Innovation Research program and the Small Business Technology Transfer program. These two programs award Federal research funds to small businesses. EMP allegedly received funds for work the company had already performed for another Government agency and certified the work was original. Allegedly, EMP directed its employees to falsify labor hours on their timesheets submitted to the Government for payment. On December 27, 2018, EMP entered into a civil settlement agreement to pay the Government $2.75 million to resolve allegations the company violated the False Claims Act.

---

[87] Report No. D-2008-106, "U.S. European Command Headquarters Government Purchase Card Controls," August 21, 2008;

Report No. D-2011-034, "U.S. Central Command Headquarters' Use of the Government Purchase Card," January 25, 2011;

Report No. DODIG-2012-043, "Army Needs to Identify Government Purchase Card High-Risk Transactions,"January 20, 2012;

Report No. DODIG-2015-060, "U.S. Southern Command Government Purchase Card Controls Need Improvement to Prevent Improper Purchases," December 19, 2014.

In another case, DCIS, AFOSI, and the Federal Bureau of Investigation investigated allegations that Northrop Grumman violated the False Claims Act. Between July 1, 2010, and December 31, 2013, Northrop Grumman allegedly misrepresented the number of hours that its personnel in the Middle East worked on two Air Force communications contracts. On November 2, 2018, Northrop Grumman entered into a civil settlement agreement to pay the Government $25.8 million, and also agreed to administratively forfeit another $4.2 million to resolve allegations that it violated the False Claims Act.

DCIS also conducted a joint investigation with several agencies, including Army CID, involving allegations that Explo Systems conspired to defraud the Army and illegally dumped 15.6 million pounds of explosives at locations on Camp Minden, Louisiana. The Army awarded Explo an $8.6 million contract to demilitarize and dispose of explosive materials. Starting in January 2010, Explo personnel provided the Army with false documentation that indicated Explo sold the demilitarized explosive material, when in fact the material was never sold. Explo improperly dumped explosives at locations on Camp Minden and in landfills to prevent the Government from learning of the conspiracy. This was the largest illegal dumping of explosive material in U.S. history. On November 29, 2018, David Alan Smith, Co-Owner of Explo, and William Terry Wright, an Explo Vice President, were sentenced for their roles in the criminal conspiracy. Smith was sentenced to 55 months in prison and ordered to pay over $34 million in restitution. Wright was sentenced to 60 months in prison and ordered to pay over $149,000. Three other Explo employees were sentenced to prison for their participation in the conspiracy.

In summary, inadequate contract oversight has been a longstanding problem for the DoD, potentially costing millions of dollars each year, creating life and safety concerns for the warfighter, and impacting the DoD's ability to execute its mission. The reforms that were recently enacted by the DoD, such as empowering the Services with more oversight authority for their acquisition programs, can result in faster acquisitions, but the risk of unanticipated cost overruns, program development spanning decades, and reduced capability delivered to the warfighter remains a persistent challenge.

A Hospital Corpsman 1st Class cleans a patient's teeth in a dental operation room aboard the amphibious assault ship USS Boxer (LHD 4). (U.S. Navy photo)

Challenge 10. Providing Comprehensive and Cost-Effective Health Care

The Military Health System (MHS) is undergoing major changes while seeking to deliver high-quality health care for 9.6 million beneficiaries at a reasonable cost. Specifically, the DoD transferred responsibility for all military medical treatment facility in the continental United States on October 1, 2019, from the Military Services to the Defense Health Agency. The DoD is also deploying a new electronic health record system, and moving to integrate the electronic health records with the Department of Veterans Affairs.

At the same time, the DoD needs to focus on challenging behavioral health issues, such as suicide prevention and opioid and substance use disorders. It also needs to ensure that supporting data are reliable to fully assess these issues. The DoD must also reduce vulnerabilities for health care fraud within the MHS, control rising health care costs, and collect the costs for health care services from non-DoD beneficiaries, insurance companies, and other Government organizations.

These are not easy challenges. The MHS is a global, comprehensive, integrated health care system that includes a health care delivery system, combat medical services, public health activities, medical education and training, and medical research and development. The MHS provides medical care to service members, retirees, and their eligible family members. It includes direct care provided at military medical treatment facilities by military, civilian, and contracted providers, and purchased care provided at commercial locations through the TRICARE health plan. The military medical treatment facilities, usually located on DoD facilities, use a combination of military and contracted providers to treat DoD beneficiaries. TRICARE also uses civilian health care providers on a reimbursable basis to treat DoD beneficiaries. The DoD FY 2020 Budget Request contained a total request of $33.3 billion for the Defense Health Program.

The DoD OIG has performed numerous audits and evaluations and issued recommendations for improvements covering different areas of DoD health care, including reviews of quality of care, access to care, and cost control. Overall, the DoD has taken steps to address many of these recommendations, reducing the number of open recommendations related

to health care and morale issues in the past 2 years from 114 open recommendations in March 2017 to 81 as of March 31, 2019.[88]

However, while the DoD has made some progress in addressing issues that the DoD OIG has identified, there are still significant open, agreed-upon recommendations related to suicide prevention, controlling health care costs, and maximizing collections from delinquent medical services accounts. Examples include recommendations to establish a multidisciplinary approach for obtaining the data necessary to make comprehensive DoD Suicide Event Report submissions, and conducting comprehensive medical reviews on skilled nursing claims to determine whether all required documentation exists and is adequate, which would ultimately limit payments to the services provided.

DOD MILITARY HEALTH SYSTEM REFORM

The MHS transferred administration and control of all military medical treatment facilities in the continental United States from the Military Departments to the Defense Health Agency. According to the Defense Health Agency's draft transition plan, the intent of the transition is to standardize business and clinical processes, gain efficiencies, improve the medical readiness of the force, and maintain quality and accessible health care.[89]

The National Defense Authorization Act for FY 2017 mandated that by October 1, 2018, a single agency, the Defense Health Agency, would be responsible for the administration of all military medical treatment facilities. In a June 2018 report to Congress, the DoD proposed a phased approach to transition, citing the scope of the changes required by law.[90] The National Defense Authorization Act for FY 2019 amended the original deadline for full transition from October 1, 2018, through October 1, 2021, aligning with the DoD's proposed timeline. Under the phased approach, the Military Departments transferred authority, direction, and control of eight military medical treatment facilities to the Defense Health Agency on October 1, 2018. The Defense Health Agency assumed control of all military medical treatment facilities in the continental United States on October 1, 2019, but will rely on direct support from the Military Medical Departments until the Defense Health Agency's management structure is fully operational.

According to the Under Secretary of Defense for Personnel and Readiness, the optimal end state is that the MHS, under the direction of the Defense Health Agency, should be a fully integrated system of medical readiness and health care delivery. At that point, the Defense Health Agency will have direct control over military medical treatment facilities, while the Military Medical Departments will retain control over their medical uniformed personnel and non-health care delivery functions, such as medical readiness. According to the Defense Health Agency transition plan, 21 large and 16 small market offices will be established to serve as the integrating entity for geographically co-located military medical treatment facilities. In addition to ensuring access to quality health care within the military medical treatment

[88] DoD OIG, "Compendium of Open Office of Inspector General Recommendations to the Department of Defense as of March 31, 2019," July 22, 2019.

[89] Defense Health Agency Draft Implementation Plan for the Complete Transition of Military Medical Treatment Facilities to the Defense Health Agency; Version 6.0, August 12, 2019.

[90] Report to the Armed Services Committees of the Senate and House of Representatives, "Final Plan to Implement Section 1073c of Title 10, United States Code," June 30, 2018.

facilities, the market offices will be responsible for supporting medical force readiness and ensuring the clinical competency of active duty medical providers within the market.

Several Members of Congress have expressed concern about the MHS transition. In an April 2019 hearing, the Ranking Member of the House Armed Services Subcommittee on Military Personnel stated, "The military health system is undergoing the largest reform in a generation. This includes improving quality of care and increasing access to care . . . however, there are aspects of the Defense Department's reform plan that deserve greater scrutiny." Additionally, in reference to the DoD's June 2018 transition plan, Senate Report 115-262, accompanying the Senate Armed Services Committee's version of the National Defense Authorization Act for FY 2019, stated the "Department has again failed to provide a credible, detailed plan" to implement the National Defense Authorization Act for FY 2017. The report further asserted that the plan establishes "new, stove-piped service commands whose responsibilities would be to oversee medical force readiness" and "would not fully eliminate duplicative activities carried out by the Defense Health Agency and the Services' medical departments."

Establishing clear and effective authority, direction, and control over military medical treatment facility health care will be difficult and must be carefully planned to ensure beneficiaries continue to have access to high-quality and safe health care.

ELECTRONIC HEALTH RECORDS

The DoD's efforts to implement electronic health records and integrate those records with the Department of Veterans Affairs also present significant challenges. Electronic health records can contribute to improved quality of care and more efficient and convenient care. However, these records contain sensitive medical history and information about a patient's health, including symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests. The DoD must ensure that health care providers have access to millions of health care records so that providers can effectively treat the patients, but these records must be secure.

The Defense Healthcare Management System Program Executive Office began implementing the DoD's new electronic health record system, MHS GENESIS, in FY 2017. The system is intended to transform how the DoD provides medical care by replacing several legacy DoD systems and integrating inpatient and outpatient solutions that connect medical and dental information used by 205,000 MHS personnel. MHS GENESIS seeks to make electronic health records available to health care providers for the 9.6 million DoD beneficiaries worldwide. MHS facilities included 54 hospitals, 377 medical clinics, and 270 dental clinics worldwide.

According to the Defense Healthcare Management System Program Executive Office, as of July 2019, it had implemented MHS GENESIS in 53 medical and dental treatment facilities. The Program Executive Office planned to implement MHS GENESIS at 86 military medical treatment facilities by September 30, 2019, with implementation at the remaining 602 fixed medical and dental facilities worldwide and 550 Reserve Component units scheduled through FY 2024.

Implementation of MHS GENESIS has presented significant challenges. According to an April 2018, DoD Initial Operation Test and Evaluation report, published by the Office of the Secretary of

Defense (Operational Test and Evaluation), providers at three test sites could not effectively manage and document patient care. Specifically, essential capabilities were either not working properly or missing altogether, resulting in increased time for health care providers to complete daily tasks. Users reported many problems with the system including delays, insufficient training, inadequate help desk support, and accuracy of medical data exchanged between external systems and MHS GENESIS, which could jeopardize patient safety.

The Initial Operation Test and Evaluation testing was completed at the fourth site in July 2018, and although MHS GENESIS functions improved, MHS GENESIS was still not deemed operationally effective or suitable. Specifically, MHS GENESIS was not fully interoperable with other systems and users of those systems could not always view patient information, such as allergies, medications, past procedures, and immunizations data. Furthermore, users could not always determine patient dates of birth, which could be critical in determining treatment plans. Finally, in 2018, cybersecurity assessments concluded that personally identifiable information and protected health information within MHS GENESIS was not protected in accordance with DoD standards.

Maintaining the security of electronic health records is a critical responsibility for the DoD. These records contain sensitive personally identifiable information and information about a patient's past and current health, including symptoms, sensitive diagnoses, medications, lab results, and reports from diagnostic tests, and their disclosure could have serious consequences and undermine patient privacy. While electronic health records can contribute to improved quality of care, and more efficient and convenient care, if not properly protected, electronic records can leave the sensitive protected health information of millions of beneficiaries at risk. The cybersecurity of data is discussed in more detail in Management Challenge 6, "Enhancing DoD Cyberspace Operations and Capabilities."

INTEGRATION WITH THE DEPARTMENT OF VETERANS AFFAIRS

The DoD and the Department of Veterans Affairs have experienced significant problems in attempting to integrate their respective electronic health records since 1998. The National Defense Authorization Act for FY 2008 required that the DoD and Department of Veterans Affairs develop and implement electronic health record systems that allow for full interoperability of personnel health care information. The National Defense Authorization Act for FY 2014 provided additional requirements pertaining to the implementation, design, and planning for interoperability between the DoD and the Department of Veterans Affairs. The National Defense Authorization Act for FY 2017 directed the DoD and Department of Veterans Affairs to integrate their electronic health records and gave the departments 5 years to meet this requirement.

The Secretary of Veterans Affairs announced in 2017 that the Department of Veterans Affairs would acquire the same system as the DoD, and the Department of Veterans Affairs awarded a $10 billion contract in May 2018 to overhaul its electronic health record system to make it compatible with the DoD's MHS GENESIS. The Department of Veterans Affairs is using the same contractors as the DoD to develop and install the electronic health records system to potentially reduce delays and issues with implementation. According to the Secretary of Veterans Affairs, the Department of Veterans

Affairs plans initial deployment to three medical centers by April 2020. However, full implementation of the electronic health records system to all medical centers is not expected until 2028.

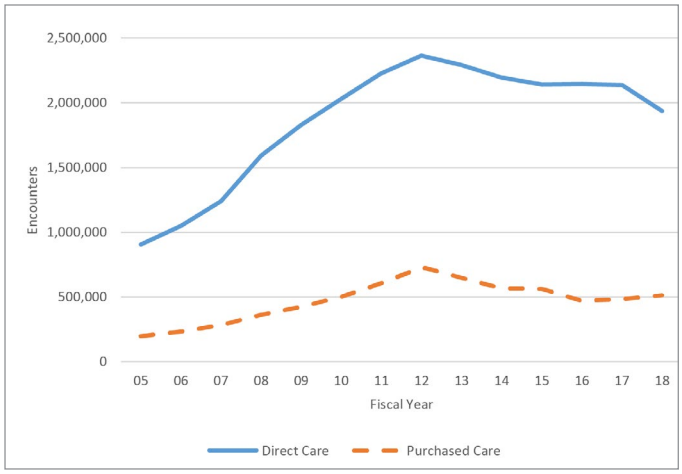
The DoD OIG and the Department of Veterans Affairs OIG both agreed to conduct complimentary audits on the status of the integration of the electronic health records of both departments. The DoD OIG announced an audit in June 2019 to determine whether the DoD is developing standards and implementing controls to provide interoperability between the health care systems of the DoD. The Department of Veterans Affairs OIG announced an audit in July 2019 to determine whether the physical and information technology infrastructure at the Department of Veterans Affairs will be able to facilitate implementation of the new electronic health record system.

BEHAVIORAL HEALTH

Behavioral health problems, such as substance abuse, depression, and suicide, continue to be a critical challenge facing the DoD. In 2018, mental health disorders were the third leading cause of outpatient medical visits and the leading cause of hospitalization for active duty Service Members. The CY 2017 DoD Suicide Event Report found that 48 percent of individuals who died by suicide and 58 percent of individuals who attempted suicide had a previous mental health diagnosis.

According to the Defense Health Agency's Psychological Health Center of Excellence, active duty service members had approximately 2.5 million outpatient mental health encounters in 2018 in both Direct Care (military medical treatment facilities) and Purchased Care (civilian medical facilities). As shown in Figure 17, although total utilization has decreased since its peak in 2012, utilization is twice as high as it was in 2005, demonstrating that there is significant patient demand for these services.

Figure 17. Outpatient Mental Health Visits Among Active Duty Service Members



Source: Psychological Health Center of Excellence.

The DoD OIG is currently evaluating how the DoD is meeting outpatient mental health access to care standards for active duty service members and their families by specifically assessing the appointment booking and referral processes. This evaluation will examine military medical treatment facility processes to determine whether they delay access to mental health care and whether there are gaps in how the MHS determines the required capacity to meet patient demand for outpatient mental health services.

DoD challenges related to suicide prevention and substance abuse are discussed in more detail in Management Challenge 3, "Ensuring the Welfare and Well-being of Service Members and Their Families."

OPIOID MISUSE AND TREATMENT

Identifying and treating those DoD beneficiaries who are misusing controlled substances, including opioids, remains a difficult challenge. The DoD must ensure that military health care providers prescribe opioids only to

those patients who need them and adhere to guidelines to avoid long-term use, if possible, to reduce the chance of addiction. Health care providers often receive pressure from patients to provide opioids to treat pain when the opioid prescriptions actually may be putting the patients at risk for addiction.

In addition, the DoD health care system must be proactive in identifying those patients who are addicted to opioids and provide treatment plans for them. The Defense Health Agency Director stated in June 2018 that the DoD is "making headway, but there is more to be done in educating our patients and providers on threats from opioid addiction and strategies to reduce abuse."

In a recent evaluation, the DoD OIG determined that the DoD did not establish and implement a standard methodology to identify the population of patients with opioid use disorder.[91] As a result, the full extent of the DoD's opioid use disorder population is unknown. The DoD OIG is now conducting an audit to determine whether beneficiaries were overprescribed opioids at selected military medical treatment facilities.

In September 2018, the Defense Health Agency implemented an opioid prescription monitoring process with multi-level oversight. According to the Defense Health Agency, this oversight process will ensure that opioid prescriptions trends are monitored on a quarterly basis at a minimum, and that providers and beneficiaries are properly educated on the use and misuse of opioids. Additionally, the Defense Health Agency entered into an agreement with the National Association of Boards of Pharmacy allowing bi-directional sharing of opioid prescription information through the Prescription Drug Monitoring Program between the DoD and the states starting in January 2019.

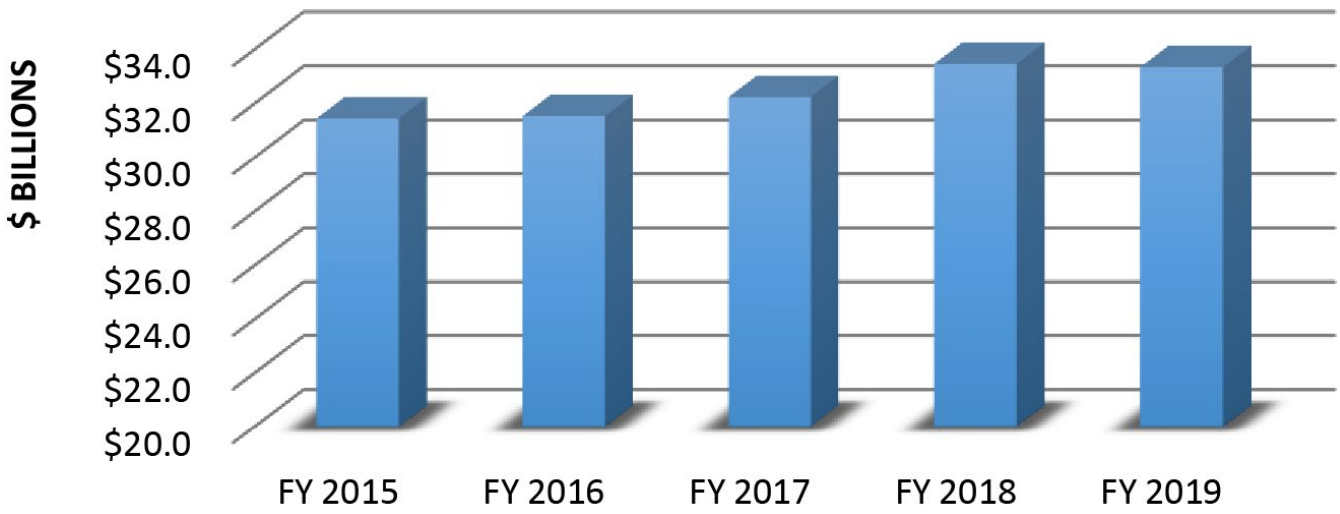
Accurate data is needed to adequately monitor patient opioid use. In an ongoing audit, the DoD OIG has determined that inaccuracy of prescription data limited the Defense Health Agency's ability to accurately track opioid use. Specifically, the audit team determined that the system did not have standardized quantity units for opioids in liquid form. Some liquid prescriptions were measured in milliliters, while some were measured as one bottle with no indication of how many milliliters were included in the bottle. As a result, attempts to calculate and track opioid use based on the quantity field would lead to errors in the amount of opioids prescribed to patients.

INCREASING HEALTH CARE COSTS

The DoD also must also confront the challenges of containing health care costs and preventing health care fraud. Health care costs in the United States have grown dramatically, and MHS costs have been no exception.

[91] Report No. DODIG-2019-091, "Evaluation of the DoD's Management of Opioid Use Disorder for Military Health System Beneficiaries," June 10, 2019.

Figure 18. Defense Health Program Appropriations From FY 2015 Through FY 2019



Source: The DoD OIG.

The FY 2020 DoD Budget Request included $33.3 billion for the Defense Health Program. Since FY 2015, the DoD appropriations for the Defense Health Program have increased from $31.4 billion in FY 2015 to $33.3 billion in FY 2019, an increase of 6.1 percent as shown in Figure 18.

At the same time, the DoD continues to struggle with combating fraudulent billing practices; implementing adequate controls to limit payments to TRICARE health care providers, and collecting from beneficiaries, insurance companies, and other Government organizations for services provided at military medical treatment facilities.

PAYMENTS FOR SERVICES WITH LIMITED OR NO COST CONTROLS

While the Defense Health Agency limits the reimbursement of many health care services, it pays for some services and products with limited or no cost containment controls. Cost containment controls include establishing maximum rates and state prevailing rates, as discussed below. However, while the Defense Health Agency has taken actions to control some costs, such as implementing a maximum rate for standard electric breast pumps, it needs to establish maximum rates for as many health care services and equipment as possible and to ensure state prevailing rates are consistent and reasonable.

Specifically, the Defense Health Agency establishes a maximum amount that the DoD pays providers for services provided to TRICARE beneficiaries. The Defense Health Agency generally sets maximum rates consistent to Medicare rates. However, if maximum or state prevailing rates do not exist, the Defense Health Agency pays the actual billed charges. For example, in an August 2019 audit, the DoD OIG determined that the Defense Health Agency did not develop maximum rates for many health care services and equipment, such as compression devices and oral appliances for the treatment of sleep apnea.[92] As a result, the Defense Health Agency paid a medical equipment supplier as much as $5,000 per month to rent a

[92] Report No. DODIG-2019-112, "Audit of TRICARE Payments for Health Care Services and Equipment That Were Paid Without Maximum Allowable Reimbursement Rates," August 20, 2019.

compression device, which helped prevent blood clots, even though research showed that other suppliers rented the same device for less than $700 per month.

The DoD OIG audit also determined that the Defense Health Agency did not apply existing maximum allowable rates for vaccines and contraceptive systems and incorrectly paid any amount that health care providers billed. For example, the Defense Health Agency paid $5,772 for a contraception system; however, the Defense Health Agency should have paid only $1,036 if it had used the existing maximum allowable rate. As a result, the Defense Health Agency overpaid $4,736 for the contraceptive system. The DoD OIG recommended that the Defense Health Agency Director identify the reasons why TRICARE region contractors did not use existing TRICARE maximum allowable reimbursement rates, and take immediate actions to confirm that TRICARE claims for vaccines and contraceptive systems are paid using the TRICARE maximum allowable reimbursement rates.

The DoD OIG audit also concluded that the Defense Health Agency could put funds to better use if the Defense Health Agency adopted some of the industry pricing benchmarks described in the report. Specifically, the Defense Health Agency could put $19.5 million to better use over the next 5 years if it adopted vaccine manufacturer and Medicaid pricing for vaccines and contraceptive systems. The Defense Health Agency implemented procedures in April 2018 to limit the amount the DoD pays for vaccines in state vaccination programs for nine states. However, the Defense Health Agency still needs to ensure it pays reasonable costs for contraceptive systems and other vaccines.

In addition, the Defense Health Agency uses state prevailing rates to control costs. The Defense Health Agency requires its TRICARE contractors, which reimburse TRICARE health care providers for health care services, to establish prevailing rates for each of the 50 states when no maximum allowable charge is available. TRICARE contractors establish state prevailing rates by selecting the most frequently billed charges from TRICARE claims data for each TRICARE service and equipment provided in each state during the previous year.

Because state prevailing rates are generated solely from using the most commonly billed charges for each TRICARE service and supply from the previous year, state prevailing rates can be greatly affected if only a limited number of providers billed for a specific TRICARE service or supply. For example, if one provider accounted for 80 percent of the claims for a specific service or supply, this methodology could result in an unreasonably high state prevailing rate if the provider billed unreasonably high prices. In 2017, news agencies reported that the Defense Health Agency paid more than $400 per can of baby formula specifically made for babies and toddlers with digestive problems; however, the same baby formula had a retail price of less than $50 per can.

Additionally, because each state has a unique prevailing rate for each TRICARE-provided service or piece of equipment and the rates can vary greatly among the 50 states, the Defense Health Agency is at risk of paying substantially higher prices for TRICARE services and supplies in some states versus other states. The DoD OIG had determined that prevailing rates for some states were thousands of dollars more than the prevailing rates for other states. The DoD OIG plans to perform an audit to review state prevailing rates in more depth.

COLLECTIONS

The DoD could also better control health care costs by proactively collecting for services provided at military medical treatment facilities. Collections from beneficiaries, insurance companies, and other Government organizations can provide additional funds to the military medical treatment facilities to be used to help improve access and quality of care.

In a December 2018 audit report, the DoD OIG summarized six OIG audit reports issued between August 2014 and January 2017, containing 47 recommendations to improve the management of DoD delinquent medical service accounts. Although some improvements were made as a result of these audits, the December 2018 followup audit noted that the Services were unable to determine the total number and dollar value of delinquent accounts, and they have not fully pursued opportunities to collect a potential $80.1 million on delinquent accounts and accounts not billed.[93]

In another audit report in September 2019, the DoD OIG identified that Defense Health Agency and military medical treatment facility personnel did not adequately manage the Third Party Collection Program to ensure collection of all available funds from delinquent medical claims for providing health care services. Without proper management of the Third Party Collection Program, the DoD did not collect up to $70.7 million of the $86.9 million that was over 120 days past due. As a result, substantial uncollected funds were not available for the medical facilities to use to improve the quality of health care.[94]

HEALTH CARE FRAUD

Fraud is a leading contributor to increasing health care costs. Health care services are susceptible to fraud partly because of how claims are paid across the health care industry. While some pre-payment reviews exist for high-risk payments in the health care industry, insurance companies, including TRICARE, pay for most services without reviewing the medical records to determine whether the bills are accurate and supported by documentation. According to the Defense Health Agency, it does not have the resources to review supporting documentation for all claims because of the high volume of health care claims received daily. As a result, health care claims are more vulnerable to fraudulent activity.

Both the Defense Health Agency Program Integrity Division and TRICARE use contractors to analyze historical claims data to identify unusual billing patterns and trends. Once potentially fraudulent activities are identified, the Program Integrity Division refers this potential fraud to the Defense Criminal Investigative Service (DCIS). Health care fraud cases are the largest source of referrals to DCIS. As of July 2019, DCIS was conducting 530 health care investigations. In FY 2017 and FY 2018 combined, DCIS health care fraud investigations resulted in 212 criminal charges and 113 convictions, the seizure of $31 million in assets, and $138 million in recoveries for TRICARE and the Defense Health Agency. Health care fraud investigations also accounted for a significant number of DCIS arrests, civil settlements, and monetary recoveries in FY 2018.

---

93 Report No. DODIG-2019-38, "Followup of Delinquent Medical Service Account Audits," December 19, 2018.

94 Report No. DODIG-2019-108, "Audit of the DoD's Management of the Third Party Collection Program for Medical Claims," September 16, 2019.

Health care fraud schemes constantly evolve, which makes combating fraud a continual challenge. When the DoD and other Federal health care programs implement measures to prevent fraud in one area, fraudsters seek other vulnerabilities. For example, in 2014 and 2015 health care providers fraudulently billed TRICARE for compound drugs (produced by combining, mixing, or altering two or more ingredients to create a customized medication), such as compound pain cream and other creams, without examining or even meeting the patient. Many of these creams were ineffective or not needed by the recipient. These schemes took advantage of a TRICARE reimbursement policy that allowed for full and immediate reimbursement of prescribed compound drugs, even though their costs were often grossly inflated. In 2015, the Defense Health Agency changed its reimbursement policy for compound drugs in response to the significant fraud that occurred and reduced monthly costs for compound drugs from $497 million in April 2015 to $10 million in June 2015.

When the Defense Health Agency took actions to combat compound drug fraud schemes, fraudsters shifted schemes to other health care services. For example, the Centers for Medicare and Medicaid Services reported that Medicare had an improper payment rate of 35.5 percent in 2018 for durable medical equipment, such as wheelchairs and braces. Other emerging areas of concern for fraudulent billings and kickback schemes within the DoD health care system include genetic testing and laboratory testing. Genetic testing fraud can occur when TRICARE or other health care programs are billed for a test or screening that was not medically necessary or was not ordered by a beneficiary's treating physician. Fraudsters offer beneficiaries "free" screenings or cheek swabs for genetic testing to obtain their TRICARE information for identity theft or fraudulent billing purposes. Fraudsters also target beneficiaries through telemarketing calls, booths at public events, health fairs, and door-to-door visits. Beneficiaries who agree to genetic testing or provide their personal or TRICARE information may receive a cheek swab, an in-person screening or a testing kit in the mail, even if it is not ordered by a physician or medically necessary.

Fraudulent laboratory testing schemes occur when laboratories collude with physicians to order unnecessary or redundant tests usually involving blood or urine specimens. Payments under these arrangements are typically made on a per-specimen or per-beneficiary-encounter basis and often are associated with expensive or specialized tests. Payment is offered on the condition that the physician order either a specified volume or type of tests or test panel, especially if the panel includes two or more tests performed using different methodologies intended to provide the same clinical information.

Durable medical equipment fraud schemes can involve equipment companies or marketers colluding with physicians, or using the stolen identities of unsuspecting physicians, to falsely certify that beneficiaries need specialized equipment. This same fraudulent durable medical equipment company may also have stolen, or otherwise purchased, beneficiary information to fraudulently bill for equipment. Typically, no actual equipment is delivered to the beneficiaries, and the beneficiaries may not know equipment is being billed in their names but not delivered. In other schemes, durable medical equipment companies offer the beneficiaries meals or vitamins and supplements in exchange for TRICARE information. Common costly durable medical equipment items that are offered include custom shoes for diabetic

patients, braces, oxygen, nebulizers, and therapeutic mattresses. Sometimes beneficiaries are aware of the fraud and are paid a "kickback" in cash for selling their TRICARE information.

The Defense Health Agency Program Integrity Division monitors claims, looking for spikes or drastic increases in the cost or volume of the claims. If fraud indicators are present, the Defense Health Agency refers the matter to DCIS or other criminal investigative agencies.

However, the DoD needs to regularly and comprehensively review billing trends to proactively address potential fraud schemes and implement effective controls to help prevent payments for fraudulent claims. In this effort, the DoD OIG also uses data analytics to identify improper payments in several categories of health care payments, including breast pumps, compression devices, oral appliances, vaccines, and services related to treatment of autism. Data analytics can identify unusual billing patterns and identify health care providers overcharging the DoD. It has allowed the DoD OIG to focus on high-risk transactions and concentrate resources on areas that need the most oversight.

In summary, the DoD faces significant challenges with providing health care to the DoD's 9.6 million beneficiaries worldwide. As of October 1, 2019, the Defense Health Agency took operational control of all military medical treatment facilities in the continental United States, which is a monumental task. The DoD must implement the new MHS GENESIS electronic health record system across all military medical treatment facilities while ensuring patient health information is secure and available to all DoD health care providers. The DoD must also integrate electronic health records with the Department of Veterans Affairs as that department implements MHS GENESIS across its facilities. At the same time, the DoD needs to proactively identify and treat behavioral health disorders, such as opioid addiction, and aggressively reduce the number of suicides within the military. The DoD must continue to implement proactive controls to fight health care fraud and reduce costs for services and equipment, which would result in more funds available to treat Military Service members, their families, and retirees.

A U.S. Army Lieutenant, optometrist, Expeditionary Medical Facility Dallas One, Ft. Worth, Texas, examines a patient at Innovative Readiness Training Appalachian Care 2019 at Wise County Fairgrounds, Wise, Virginia., August 18, 2019. (U.S. Army photo)


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Whistleblower Protection
U.S. Department of Defense

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

www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

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
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