INSPECTOR GENERAL

U.S. Department of Defense

FISCAL YEAR 2019

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, 2018

Each Inspector General (IG) is required by law, the Reports Consolidation Act of 2000, 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. The law states that the "agency head may comment on the IG's statement, but may not modify the statement." The law also requires the IG's statement to be included in the agency's Financial Report.

The following is the DoD Office of Inspector General's (OIG) statement on the top management and performance challenges facing the DoD. The DoD OIG identified these challenges based on a variety of factors, including DoD OIG oversight work, research, and judgment; oversight work done by other DoD components; oversight work conducted by the GAO; and input from DoD officials. While we reviewed DoD statements, documents, and assessments of these and other critical issues, we identified these top challenges independently.

The DoD OIG also uses this document to determine areas of risk in DoD operations and where to allocate the DoD OIG oversight resources. This document is forward looking and identifies the top challenges facing the DoD in FY 2019 and in the future.

As reflected in this document, the top 10 DoD management and performance challenges are:

1. Implementing DoD Reform Initiatives
2. Countering China, Russia, Iran, and North Korea
3. Countering Global Terrorism
4. Financial Management: Implementing Timely and Effective Actions to Address Financial Management Weaknesses Identified During the First DoD-Wide Financial Statement Audit
5. Improving Cyber Security and Cyber Capabilities
6. Ensuring Ethical Conduct
7. Enhancing Space-Based Operations, Missile Detection and Response, and Nuclear Deterrence
8. Improving Readiness Throughout the DoD
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

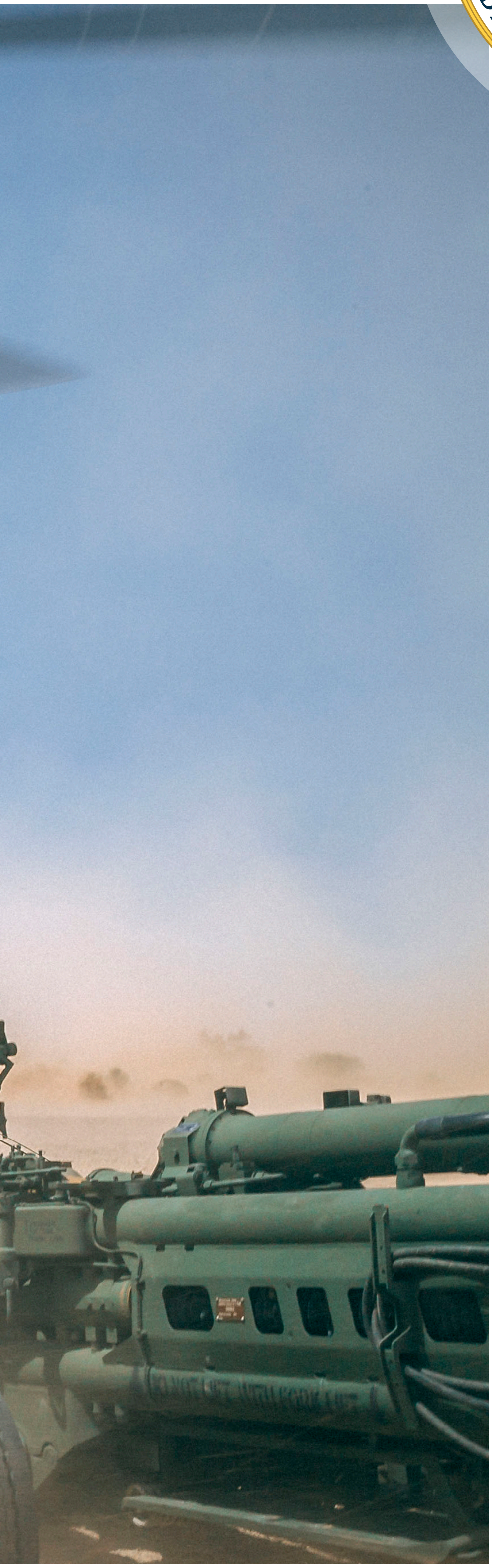
In this document, we discuss each challenge, actions taken by the DoD to address the challenge, and oversight work by the DoD OIG and others related to the challenge.

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

Glenn A Fine

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

Marines prepare to use a CH- 53E Super Stallion helicopter to move an M777 howitzer to its firing position during a training exercise at Marine Corps Air Ground Combat Center Twentynine Palms, California. (U.S. Marine photo)

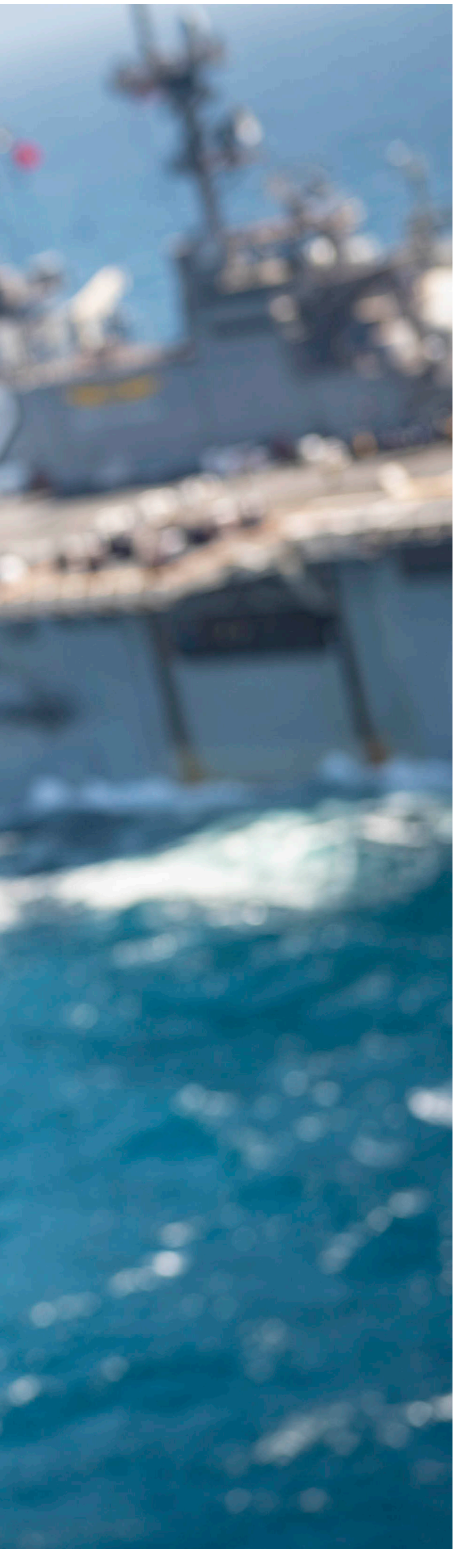


Summary of Management and Performance Challenges Facing the DoD

FISCAL YEAR 2019

A U.S. Navy Aircrewman rides in an MH-60S Seahawk helicopter during composite training unit exercise (COMPTUEX) in the Pacific Ocean. (U.S. Navy photo)

Challenge 1: Implementing DoD Reform Initiatives



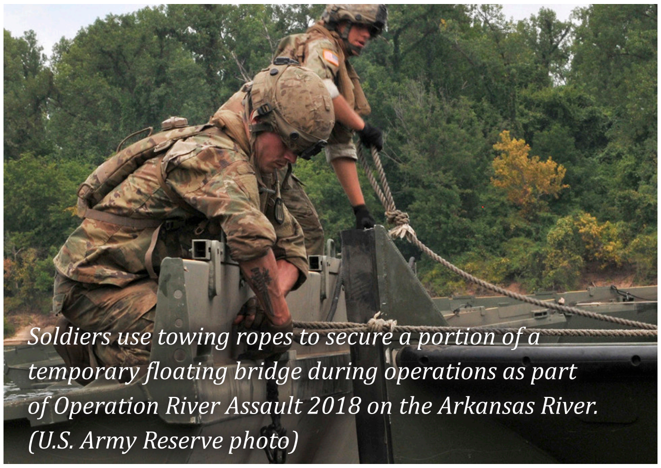
In April 2018, Secretary of Defense James Mattis stated, "The United States has a clear way forward with the 2018 National Defense Strategy to restore the military's competitive edge in an era of re-emerging long-term great power competition." In this effort, the DoD is pursuing several initiatives to reform business operations and mission support infrastructure throughout the DoD. These initiatives are intended to increase readiness, more effectively use DoD forces, and develop advanced capabilities, all of which, according to the DoD will contribute to increased lethality.

Specifically, as a supplement to the National Defense Strategy, the FY 2018 – FY 2022 National Defense Business Operations Plan, issued by the Chief Management Officer, presents three strategic reform goals: (1) rebuild military readiness to build a more lethal Joint Force, (2) strengthen alliances to attract new partners, and (3) reform the Department's business practices for greater performance and affordability. According to this report, these interrelated strategic goals contribute to increasing military capabilities by ensuring that warfighters have the best support available to prepare for their wartime missions. These reform initiatives are also intended to free up resources to enable the Military Services to rebuild readiness and acquire advanced capabilities more rapidly.

Developing and implementing these reforms, many of which address management challenges described in this report, will be especially challenging because of the size of the DoD and the complex nature of its structure. The DoD consists of 1.3 million active duty military and 862,000 personnel in the National Guard and Reserve, supported by a civilian workforce of more than 742,000. The DoD has over $2.6 trillion in assets, with installations and facilities in more than 5,000 different facilities worldwide.

The DoD is faced with the challenge of what forces it needs and how to organize its forces to be able to simultaneously undertake a wide range of potential diverse missions to address both conventional and unconventional threats. To fulfill these responsibilities, the DoD's budget is large but not unlimited.

In addition, change is not easy. Some cultural resistance to change has contributed to the difficulty of implementing past reform efforts to improve the DoD's financial, infrastructure, inventory, and acquisition systems. For example, initiatives that require the development and use of common systems and processes across Military Service and organizational boundaries are often resisted.



Soldiers use towing ropes to secure a portion of a temporary floating bridge during operations as part of Operation River Assault 2018 on the Arkansas River. (U.S. Army Reserve photo)

Additionally, DoD leadership regularly changes. Political appointments and rotating military leadership can shift goals and priorities, which can affect reform momentum.

In the face of these challenges, the DoD must set clear expectations for the reform goals so that they are well understood, and tracking against those goals should be consistent and transparent.

DOD REFORM INITIATIVES

In 2018, the Chief Management Officer position was established to improve the enterprise management of DoD business operations. The Chief Management Officer has independent authority to direct the Departments of the Army, Navy, and Air Force and the Defense agencies to implement reforms on matters such as business transformation, business planning, performance management, and information technology. The Chief Management Officer is also the principal advisor to the Secretary of Defense and Deputy Secretary of Defense regarding enterprise business operations within the DoD.

On January 19, 2018, Secretary Mattis stated: "To keep pace with our times, the Department will transition to a culture of performance and affordability that operates at the speed of relevance. Success does not go to the country that develops a new technology first, but rather, to the one that better integrates it and more swiftly adapts its way of fighting." In conjunction with that goal, the National Defense Business Operations Plan focuses on the DoD's strategy to improve performance, provide a strong foundation to rebuild readiness, work with partners in support of its priorities, and reform business operations.

The National Defense Business Operations Plan also states, "Current challenges and increased threats facing our warfighters require more financial investment than is currently available with a fixed top-line budget." The DoD appropriation for FY 2019 is $674.4 billion, which represents a $19.8 billion increase from the enacted fiscal 2018 budget.

However, the DoD cannot count on increased budgets in the future. Reforming its business practices is therefore critically important not only to increase performance but also to generate savings to invest in advanced capabilities for the future. The DoD must accomplish this at the same time is fighting two wars and pursuing other overseas contingency operations throughout the world.

REBUILDING READINESS

As part of its reform efforts, the DoD is implementing initiatives to rebuild military readiness by investing in modernization of key capabilities. According to the DoD, examples of ongoing reforms to rebuild military readiness include:

- transforming how the DoD delivers a secure, stable, and resilient information technology infrastructure to ensure protection from continuous cyber attacks. This effort includes modernizing the DoD's information transport capabilities through installation of high throughput routers and fiber optic links; deployment of enhanced network security stacks; implementation of state-of-the-art tools to better manage the network; and a comprehensive analytics capability that integrates defensive cyber operations throughout the DoD. The goal of these improvements is to enhance the DoD's ability to operate and defend its information infrastructure.

- ensuring that human capital resources are provided in the right places, at the right time, at the right levels, and with the right skills, while simultaneously being good stewards of taxpayer dollars. The DoD plans to align uniformed personnel to only military essential requirements, maintaining sufficient levels of Government civilians to perform critical enabling and readiness functions, and seeking the most cost-effective and economical solution for all other work.

STRENGTHENING ALLIANCES

The DoD has also pursued reform efforts to strengthen military alliances and attract new partnerships. These programs include foreign military sales, foreign military funding, exercises and training events, military-to-military exchanges, and partnering to develop key technological capabilities. This effort includes assessing and reforming the DoD's security cooperation organizations and structures, workforce, and processes. Reform efforts to strengthen the DoD's military alliances and attract new partnerships include:

- developing a certified DoD Security Cooperation workforce with the training, experience, and resources necessary to meet mission requirements. The DoD plans to build a certification program and enhance existing management systems to ensure that personnel with the appropriate training, skills, and experience are assigned to Security Cooperation positions, and that developmental opportunities exist to ensure smooth succession planning.
- strengthening and evolving alliances and partnerships into an extended network capable of deterring or decisively acting to meet the shared challenges. The DoD plans to provide a full-spectrum capability including defense systems, personnel, strategy, doctrine, plans, and institutional support to our partners. The intended outcome of this effort is to maximize the DoD's return on investment by applying comprehensive solutions to effectively enable partner nations to perform desired roles and sustain capabilities over the long term.

IMPROVING BUSINESS OPERATIONS

The DoD is also pursuing other reforms in information technology, health care, logistics and supply chain, service contracts, community services, real property management, human resources, and testing and evaluation. Examples of these reforms include:

- reviewing the DoD's 716 regulations, including 350 contained in the Code of Federal Regulations, to identify regulations that are no longer required or relevant for repeal, replacement, or modification with the goal to reduce the regulatory burden with the DoD. The DoD's Regulatory Reform Task Force is leading this effort and is tasked with making recommendations by December 31, 2018, to the Secretary of Defense. The goal of this review is to reduce the DoD's existing regulations by 25 percent.
- expanding resource sharing between the DoD and the Department of Veterans Affairs to enhance the services provided to Service members and Veterans. For example, the Secretary of Veterans Affairs and the Secretary of Defense have entered into agreements for the use or exchange of health care resources. While the DoD is not seeking a complete integration of both health care systems, expansion of key resource sharing initiatives may lead to improved care and significant cost savings.

OPTIMIZING ORGANIZATIONAL STRUCTURES

The DoD is also seeking to shift the structure of business operations from single-organization use to enterprise-wide use. According to the Chief Management Officer, the DoD intends to leverage benchmarked internal, external, and private sector best practices, while developing specific performance metrics and goals. In particular, the DoD has taken several actions to streamline and restructure its organizations, such as:

- reorganizing the Under Secretary of Defense for Acquisition, Technology and Logistics into two new Under Secretaries of Defense: (1) the Under Secretary of Defense for Research and Engineering, focused on research and engineering to advance technology and innovation, and (2) the Under Secretary of Defense for Acquisition and Sustainment, focused on acquisition and sustainment programs to deliver and sustain timely, cost-effective capabilities for the DoD.
- transferring the responsibility for military treatment facilities from the Military Services to the Defense Health Agency. This transfer is intended to strengthen management of medical enterprise activities; standardize policies and procedures to maximize efficiencies and eliminate duplicative activities; and assume direction and control over the military treatment facilities.

IMPROVING THE QUALITY OF BUDGETARY AND FINANCIAL INFORMATION

The DoD is also focused on improving its financial management practices on developing reliable, useful, and timely financial information to help ensure accountability over DoD budgets and assets and to help DoD leadership to make informed decisions. Sound financial management is particularly important for the DoD because its expenditures constitute nearly half of the Government’s discretionary spending and its physical assets represent more than 70 percent of the Government’s physical assets.

Soldiers receive a mission brief before conducting air assault training during Exercise Saber Junction 2018 at the Grafenwoehr Training Area, Germany, September 11, 2018. (U.S. Army photo)

For decades, auditors have reported weaknesses in DoD financial management, including financial statement reporting and financial management systems. These weaknesses affect not only the DoD's ability to attain an unmodified opinion on its financial statements, but also its ability to make sound decisions related to its mission and operations and to deter waste and abuse. The DoD is undergoing a full financial statement audit for the first time ever. This audit is discussed in more detail in Management Challenge 4, "Financial Management: Implementing Timely and Effective Actions to Address Financial Management Weaknesses Identified During the First DoD-Wide Financial Statement Audit."

DOD REFORM INITIATIVES RELATE TO DOD OIG MANAGEMENT CHALLENGES

Many of the reform initiatives that the DoD has initiated are related to the DoD's top management and performance challenges, as discussed in this report.

The following are a few examples of how these reform initiatives relate to the top management and performance challenges discussed in this report. These examples provide only a brief overview of the challenges; each of these challenges, and others, are discussed in more detail in the remainder of this report.

ACQUISITION AND CONTRACT MANAGEMENT

One of the DoD's ongoing reform initiatives is related to the acquisition of major weapons systems, as well as to contracting for goods and services. According to the DoD, the goals of these initiatives are to develop a rapid, interactive approach to capability development to reduce costs, technological obsolescence, and acquisition risk, and to ensure that the DoD receives quality services and supplies in a timely manner. Key elements of the DoD's efforts include significantly streamlining the acquisition process and assigning greater responsibility and accountability for program execution and performance to the Military Services.

However, acquisition and contract management has remained a high-risk area for the DoD for many years. While the DoD seeks to improve the acquisition of major weapon systems, the DoD struggles to ensure products and services are delivered on time and within budget. It is also essential that the DoD recruit and retain skilled personnel to effectively and efficiently perform contract management and oversight. These initiatives and the longstanding challenges related to acquisition and contract management are discussed in more detail in 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."

CYBER SECURITY AND CYBER CAPABILITIES

The DoD relies on cyberspace to perform the full spectrum of its military, intelligence, and business operations. The DoD is pursuing reform initiatives related to enhancing information technology and cybersecurity capabilities. The goal of these initiatives is ensure a worldwide, secure, and resilient information environment. Additionally, the DoD continues to seek to streamline information technology to reduce costs and improve efficiency. These initiatives are intended to modernize the DoD Information Network and improve cyber capabilities and cyber security.

One aspect of these reforms involves building, retaining, and growing the DoD's cyber workforce. The DoD also needs to maintain partnerships with U.S. allies, international partners, and other private organizations regarding technological capabilities. It also needs effective programs to monitor system and network activity. The challenges related to information technology and cybersecurity and the DoD's progress in addressing them are highlighted in Management Challenge 5, "Improving Cyber Security and Cyber Capabilities."

HEALTH CARE MANAGEMENT

Another of the DoD's reform initiatives involves determining how to provide comprehensive and cost-effective health care without sacrificing quality is an ongoing challenge for the DoD. The DoD faces additional challenges associated with Military Health System reform because the DoD is switching responsibility for the military treatment facilities from the Military Services to the Defense Health Agency. Also, the DoD faces challenges related to suicide and opioid misuse, increasing health care costs, and the security and integration of electronic health records. The challenges related to health care and the DoD's progress in addressing them are highlighted in Management Challenge 10, "Providing Comprehensive and Cost Effective Health Care."

ADDITIONAL REFORM INITIATIVES

Other DoD reform initiatives related to real property, logistics and supply chain, testing and evaluation, human resources, and community services are addressed in other challenges discussed in this report.

IMPLEMENTING OVERSIGHT RECOMMENDATIONS WILL IMPROVE DOD BUSINESS OPERATIONS

Each year, the DoD OIG issues approximately 150 audit and evaluation reports on DoD programs and operations. These reports contain recommendations to DoD management that seek to improve the efficiency and effectiveness of DoD programs and operations; ensure integrity and accountability; detect and deter waste, fraud, and abuse; reduce costs; manage risks; realize monetary benefits; and improve management processes. The DoD OIG recommendations address a wide range of topics throughout the DoD, such as procurement of weapon systems and automated information systems, maintenance and sustainment of military systems, DoD financial management and accounting systems, cybersecurity, contractor oversight, health care costs, military construction, maintenance and structural stability of dams, and identification and prioritization of critical assets.

On July 30, 2018, the DoD OIG published its second Compendium of Open Office of Inspector General Recommendations to the Department of Defense (Compendium). This Compendium identified 1,558 open OIG recommendations, which are recommendations from prior reports for which corrective action had not been completed.[1] All but 102 of these recommendations had been agreed to by DoD management. The Compendium is designed to summarize DoD OIG recommendations issued to DoD Components and to focus attention on recommendations that have not yet been implemented.

Since the first Compendium was issued in 2017, the DoD has made concerted efforts to address many of the open recommendations. DoD management has worked with the DoD OIG to provide information about the status of the DoD's efforts to implement open recommendations. In total, DoD management provided documentation that enabled the DoD OIG to close 421 open recommendations listed in the 2017 Compendium. These efforts to address open recommendations are an important benefit of the Compendium.

[1] DoD OIG, "Compendium of Open Office of Inspector General Recommendations to the Department of Defense as of March 31, 2018," July 30, 2018.

As a result of the Compendium, the Office of the Chief Management Officer has been assigned the responsibility for coordinating the DoD's efforts to implement open DoD OIG recommendations. As part of this effort, the Office of the Chief Management Officer organizes regular meetings among DoD Components and DoD OIG senior leaders. These meetings help the DoD to prioritize action on open DoD OIG recommendations and provide a forum for DoD senior leaders to discuss open recommendations, their plans for implementing agreed-upon corrective actions, and the documentation that must be provided to the DoD OIG in order to close a recommendation.

While the DoD has made progress since the first Compendium was issued, many recommendations remained open as of March 31, 2018, including 33 recommendations with associated potential monetary benefits totaling $2.3 billion, and 56 recommendations that had been open for at least 5 years.

In addition to the recommendations listed in the Compendium, the DoD OIG and its contracted independent public accounting firms issue Notifications of Findings and Recommendations throughout the financial statement audits. Auditors use these notifications to communicate to management the discovery of findings throughout the audit phases of financial statement audits. For the FY 2017 financial statement audit, the DoD OIG and independent public accounting firms issued 1,217 Notifications of Findings and Recommendations. These recommendations, if implemented, can improve the financial management process, develop efficiencies in both financial management and operations, and improve the auditability of the financial statements.

To track Notifications of Findings and Recommendations and report corrective actions, the Office of the Deputy Chief Financial Officer has developed a centralized database to track financial audit and attestation Notifications of Findings and Recommendations and corrective action plans and communicate progress to both DoD management and Congress. The database provides financial managers a comprehensive view of overarching issues that affect the DoD's financial management.

In summary, the DoD faces significant challenges related to business reform because of the size and complexity of the DoD. Successfully implementing these business reform efforts, addressing the management challenges discussed in this report, and implementing open recommendations can improve DoD programs and business operations. However, continual attention, and focus at all levels in the DoD, is critical to addressing these challenges, to rebuilding military readiness, to strengthening alliances, and to reforming the DoD's business practices.

A U.S. Navy Aircrewman rides in an MH-60S Seahawk helicopter during composite training unit exercise (COMPTUEX) in the Pacific Ocean. (U.S. Navy photo)

Challenge 2: Countering China, Russia, Iran, and North Korea

The U.S. National Security Strategy issued in December 2017 states that the United States faces three main sets of challengers—the revisionist powers of China and Russia, the rogue states of North Korea and Iran, and transnational threat organizations, particularly jihadist terrorist groups—that actively compete against the United States and our allies and partners. Although differing in nature and magnitude, these rivals compete across political, economic, and military arenas, and use technology and information to accelerate these contests in order to shift regional balances of power in their favor.

The National Defense Strategy, issued in January 2018, reemphasizes that the central challenge to U.S. prosperity and security is the reemergence of long-term, strategic competition by the revisionist powers of China and Russia. The National Defense Strategy also notes that the "rogue regimes of North Korea and Iran are destabilizing regions through their pursuit nuclear weapons or their sponsorship of terrorism."

The DoD's challenge is to maintain readiness and lethality to confront each of these diverse threats. It must maintain the flexibility to counter the evolving nature of each threat while simultaneously supporting the diplomatic, informational, and economic efforts associated with U.S. national power.

CHINA

According to the National Security Strategy, China seeks to weaken U.S. influence in the Indo-Pacific region and elsewhere, while strengthening its own influence and attempting to supersede the United States as a global leader.

CHINA'S ECONOMIC INITIATIVES SUPPORT ITS MILITARY EXPANSION

In the January 2018 U.S. National Defense Strategy, Secretary Mattis summarized China's long-term competitive strategy as a convergence of military modernization, influence operations, and predatory economics to expand its power and increase its influence. He warned that China seeks regional dominance in the Indo-Pacific region in the near term and displacement of the United States to achieve global preeminence in the future.

For example, although China has been a member of the World Trade Organization since 2001, it has not followed the organization's rules, including violating pledges not to force foreign firms in China to transfer their technologies to Chinese officials. According to media reports, China has pressured about one in five foreign companies, including companies in defense-related aerospace, semiconductors, and chemical industries, to transfer technology to China in order to continue doing business there. Additionally, China has pursued an aggressive campaign of stealing U.S. high-tech commercial and defense technology through cyber and more traditional forms of espionage.

South and East China Seas

China had also claimed, developed, and militarized seven artificial land features in the South China Sea, despite competing claims from five other Pacific nations and a 2016 ruling by the International Court of Justice against China's unilateral territorial expansion. According to the Asia Maritime Transparency Initiative at the Center for Strategic and International Studies, China has increased infrastructure construction to support air and naval bases on at least seven small islands in the South China Sea.

China has economic as well as military incentives for controlling this area. Economically, the South China Sea floor contains an estimated 11 billion barrels of oil and 190 trillion cubic feet of natural gas. The East China Sea contains similar resources.

Sailors inventory munitions on the flight deck of the aircraft carrier USS Theodore Roosevelt in the Pacific Ocean, April 25, 2018. (U.S. Navy photo)

If China achieves exclusive control of these areas, it can exploit these oil and gas fields and control fishing rights. Militarily, by occupying islands in the disputed South and East China Sea regions, China can expand its strategic defenses far from its coastline.

In addition, annual trade worth $5.3 trillion passes through these sea lanes, and China considers its national defense and economic well-being dependent on securing control of the South and East China Sea logistics routes and resources. China has also increased its presence in the Indian Ocean in 2018, developing commercial island infrastructure and increasing the People's Liberation Army's naval presence in the Maldives, southwest of India. To its east, China maintains a capability to target enemy ships as far away as Guam with high-speed ballistic missiles.

Belt and Road Initiative

In 2013 and 2014, China devised a plan to develop trade and investment along the ancient Silk Road and maritime spice routes, using infrastructure investments to link China to countries throughout Asia, the Middle East, and Europe, called the Belt and Road Initiative. According to media reports, since 2014 China has financed and constructed railroads, ports, pipelines, and highways and has underwritten an estimated $900 billion in loans in 71 countries. As a condition for its loans, China requires partner countries to contract and pay for the construction and operation of infrastructure with Chinese firms, often with the risk of ceding ultimate control to China. Through these practices, Chinese state-owned companies have assumed a controlling stake in at least 76 ports in 35 countries.

In addition, China recently completed its first year of operations in Djibouti, a strategic seaport located on the Gulf of Aden near the Strait of Bab-el-Mandeb. In 2017, China constructed its first overseas military base in Djibouti following completion of a large-scale infrastructure, airfield, and port facility project. Media reports indicate that China's Djibouti base contains aircraft hangars, a helicopter base, and housing for 10,000 troops.

Pakistan, already the beneficiary of Chinese commercial investments near the Strait of Hormuz, could be the next location for a Chinese overseas military base.[2] China also is reported to be discussing military basing with Sri Lanka and the 80-island nation of Vanuatu, less than 1,250 miles off the eastern coast of Australia. An army base in Vanuatu would be China's first military facility in the Pacific Ocean.

CHINA'S TECHNOLOGICAL ADVANCES ARE MILITARISTIC IN NATURE

China is second to the United States in military expenditures, with an FY 2018 military budget of $175 billion (compared to the 2019 U.S. military budget of $674.4 billion). However, China continues to modernize its People's Liberation Army. Admiral Harry Harris, the former Commander of U.S. Pacific Command, testified before the House Armed Services Committee on February 14, 2018, that China's force modernization was essential to its strategy of achieving military dominance over the United States in the Indo-Pacific region.

China is also transitioning its military into a modern, high-technology fighting force in all military domains. According to Admiral Harris, modernizing the People's Liberation Army includes:

- rapidly expanding the quantity and sophistication of ballistic missiles that can target Taiwan, U.S. carrier strike groups, U.S. forces in Japan and Guam, and the U.S. mainland;
- building more lethal and survivable ships, including guided missile destroyers, nuclear submarines, and Fast Combat Support Ships designed to logistically support aircraft carriers;
- producing advanced fighter jets;
- upgrading bombers, heavy-lift transport, and anti-submarine aircraft;
- increasing electronic warfare and command and control;
- re-organizing the People's Liberation Army Ground Force divisions into combined arms brigades; and
- expanding the People's Liberation Army Marine Corps from two to as many as eight Marine Brigades.

Nuclear and Missile Advances

In a 2018 National Defense University speech, General John Hyten, Commander of U.S. Strategic Command, warned that China was close to achieving a nuclear triad capability for the first time in its history. According to the DoD's "Annual Report on Military and Security Developments," released August 2018, analysts expect China to add long-range bombers to its land and sea-based nuclear capability soon. Other advanced People's Liberation Army military technologies include independently targetable missiles with multiple strike options and hypersonic glide missiles with speed and approach paths built to counter U.S. missile defense systems.

Space and Information Warfare Advances

China has also been testing counter-space weapons, such as its anti-satellite systems, by targeting unserviceable satellites in orbit. These tests have produced massive debris clouds that can linger for generations and interfere with the safe operation of other satellites. In 2015, China began testing anti-satellite missiles against satellite targets at much higher orbits than it had in the past. According to the Center for Strategic and International Studies' 2018 "Aerospace Security Project Report," China's ability to hit satellites in orbit where the United States positions some of its most sensitive assets is a serious threat to U.S. satellites.

[2] Council on Foreign Relations, Wang, Monica, "China's Strategy in Djibouti: Mixing Commercial and Military Interests," April 13, 2018.

In his March 6, 2018, "Worldwide Threat Assessment," the U.S. Director of National Intelligence stated that space-based systems are essential to Chinese modern warfare. Further, he said that China continues to build its People's Liberation Army Strategic Support Force, with the mission of developing and employing space and information warfare capabilities, as a key component of strategic deterrence.

According to a 2017 RAND Report on China's military space operations, China is quickly closing the gap with U.S. researchers in the area of military artificial intelligence. It is building a new generation of supercomputer systems that learn, accumulate, and share battlefield data, and make autonomous battlefield decisions for humans.[3] The Chinese government invested $1.3 billion in U.S.-owned artificial intelligence firms between 2010 and 2017, and additionally invested in U.S. robotics, virtual reality, and other fields where the United States currently leads in the application of technology for military purposes. For example, China is closing the gap with the United States in the use of "swarm intelligence"—the use of networked drones as an automated attack force to engage from all directions and paralyze the enemy's capability to respond.

Referring to cyber threats, the U.S. Director of National Intelligence, in a February 2018 hearing before the Senate Select Committee on Intelligence, included China as one of the primary state actors using cyber to shape societies and markets, international rules and institutions, and international areas of conflict to its advantage.

In a July 2018 interview, FBI Director Christopher Wray asserted that from a counterintelligence perspective, China represented the broadest, most challenging, and most significant threat to the United States.

The USS Dewey transits the Pacific Ocean while underway in the U.S. 3rd Fleet area of operations, July 19, 2018. (U.S. Navy photo)

U.S. RESPONSE TO MILITARY, TECHNOLOGICAL, POLITICAL, AND ECONOMIC CHALLENGES

The 2018 National Defense Strategy discussed how DoD resources would be dedicated to priorities for 2019 through 2023 that directly respond to China's military strategy. One of the top U.S. priorities relates to modernizing the nuclear triad. According to the Office of the Secretary of Defense's 2018 Nuclear Posture Review and the Council on Foreign Relations, the United States is planning and executing weapon modernization in all three nuclear weapon domains. The U.S. Air Force is building a new Stealth Bomber, the B-21 Raider. The Air Force is also designing the Ground-Based Strategic Deterrent missile system that will replace the Minuteman III Intercontinental Ballistic Missile. The Navy will begin replacing its *Ohio*-class submarines with the *Columbia*-class, and will make improvements to the submarine-launched Trident II missile to extend its life. The 2018 Nuclear Posture review stated that the nuclear triad is the Nation's number one defense priority.

The United States currently leads China in developing space warfare capability, but China is investing heavily and is closing the gap with the United States. Recently, in response to direction from the President, the DoD announced the organization of a space command intended to ensure this warfighting domain fully supports U.S. land, sea, cyberspace, and air combat capability.

[3] RAND, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations," 2017.

The United States also 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 uses, such as computer processing power and secure communications.

The DoD, in coordination with the Department of State, continues to focus on maritime security in the Indo-Pacific region, particularly the South China Sea. The United States exercises its Freedom of Navigation Operations program to contest unilateral acts of China and other states designed to restrict freedom of navigation in international waters. U.S. policy since 1983 provides that the United States will exercise and assert its navigation and overflight rights and freedoms on a worldwide basis. As a result, the U.S. Navy continues to conduct Freedom of Navigation Operations with U.S. allies in the South China Sea. The U.S. Military Services also regularly participate in bilateral and multi-lateral exercises with allied forces in the Indo-Pacific region.

In a statement before the House Armed Services Committee in February 2018, the Commander of U.S. Pacific Command stated that the People's Liberation Army continues to produce more ballistic missiles that can target Taiwan, U.S. carrier strike groups, U.S. forces in Japan and Guam, and the U.S. mainland. Improving U.S. and allied missile defense is therefore a priority for U.S. forces and allies.

RUSSIA

In an April 2018 congressional hearing, General Joseph Dunford, Chairman of the Joint Chiefs of Staff, described Russia's intent to modernize its military across the spectrum of warfighting capabilities, to include investing in new technologies with military applications such as hypersonics, artificial intelligence, and directed energy. He stated that Russia is seeking to erode the United States' competitive advantage and to challenge and, where possible, revise the European geopolitical order in its favor.

This modernization has been highlighted by Russian President Vladimir Putin who, in May 2018, stated that Russia is committed to rapidly recapitalizing military units across ground, sea, and air warfighting domains. Speaking at a meeting with top Russian military leaders in Sochi, President Putin outlined Russia's plans to procure 500 armored vehicles and artillery systems, commission 10 new warships, and purchase 160 advanced new aircraft. New Russian systems include the *Armata* main battle tank; additional *Borei*-class nuclear-powered ballistic missile submarines; and a new high-altitude air defense system scheduled to begin operational service in 2020 and which is capable of engaging 10 hypersonic targets simultaneously.

Russia also announced in July 2017 the creation of the world's most powerful quantum computer. In July 2018, Representative Will Hurd, R-Texas, discussed the national defense implications of this emerging technology: "Whoever gets to true quantum computing first will be able to negate all the encryption that we've ever done to date."

Notwithstanding the pace of its military modernization, Russia's defense budget of $66.3 billion is less than one-tenth that of the United States, and the $900 billion combined military spending of all North Atlantic Treaty Organization (NATO) countries far outstrips that of Russia. However, Russia still had the fourth highest military expenditure in the world in 2017. Military modernization, paired with indirect, cheaper means of warfare such as information operations, remains a crucial component of Russia's national security strategy.

RUSSIA REMAINS THE UNITED STATES' PRIMARY NUCLEAR OPPONENT

Russia remains the United States' primary nuclear adversary, and, according to the Commander of the U.S. Northern Command and North American Aerospace Defense Command, is the only power currently capable of mounting an air-launched nuclear attack on the U.S. homeland. The DoD's 2018 Nuclear Posture Review reported that, in addition to upgrading its existing nuclear triad, Moscow is developing a new nuclear-armed and nuclear-powered autonomous underwater vehicle with intercontinental range.

Russia has also deployed a ground-launched, nuclear-capable cruise missile in violation of the 1987 Intermediate-Range Nuclear Forces Treaty, and it has been unwilling to engage in another round of negotiations to extend the New Strategic Arms Reduction Treaty.

RUSSIA DEMONSTRATES SOPHISTICATED CYBERWARFARE CAPABILITIES

Moscow regularly engages in cyberwarfare, a warfighting domain that can range from sophisticated attacks on critical infrastructure to malign influence operations conducted through social media as an asymmetric, cost-effective complement to its strategic and conventional military capabilities. According to a summary of the DoD 2018 Cyber Strategy, "Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes."

RUSSIA CONTINUES TO SUPPORT SYRIA'S ASSAD REGIME

To achieve its strategic objectives, Russia employs diplomatic, informational (including cyberspace), military, and economic means. For example, aided by Russia's military intervention, the Syrian government has consolidated its hold on power. Russia's presence in Syria, which is continuing into its third year, aligns with Russia's strategic interests of:

- preventing the rise of the Islamic State of Iraq and Syria (ISIS), an organization which, if unchecked, could inspire terrorist attacks within Russia or on its periphery;
- counterbalancing U.S. and coalition forces in the region to prevent a reoccurrence of the North Atlantic Treaty Organization-led 2014 intervention in Libya, which resulted in the overthrow of Muammar el-Qaddafi; and
- maintaining access to the Mediterranean through the naval base at Tartus, on which it signed a 49-year lease in 2017.

In Syria, against a complex backdrop of competing countries, groups, and agendas, operating in such close proximity, the United States and Russia activated a pre-established communications hotline to attempt to de-conflict military operations in Syria. DoD reports indicate that, although de-confliction between U.S. and Russian military operations decreased in the second quarter of 2018, the two sides used the hotline on at least three occasions, including as both sides simultaneously struck ISIS forces retreating across the Euphrates River.[4]

RUSSIA PUSHES BACK AGAINST NATO

At the July 2018 NATO summit in Brussels, with U.S. encouragement, NATO allies agreed to significantly increase defense spending, partly in response to perceived shifts in their security landscape. At the same event, alliance nations, including the United States, unanimously reaffirmed support for Georgia in its desire to join NATO, while calling on Russia to withdraw its forces from disputed territories in that country.

Ukraine— a country bordering four NATO nations—has confronted sustained covert Russian support of pro-separatist rebels, a conflict that has resulted in over 10,000 deaths, nearly one-third of them civilians. Following the meeting of the North Atlantic Council at the 2018 Brussels Summit, NATO restated its continued commitment to Ukraine, urging Russia to "reverse its illegal and illegitimate annexation of the Crimean peninsula," with the attendant armed conflict characterized as "a major challenge to Euro-Atlantic security."

In what NATO characterized as a rehearsal for "large-scale conflict," in September 2018 Russia conducted its single largest joint military exercise

[4] Lead IG Report to Congress, "Overseas Contingency Operations: Operation Inherent Resolve, Operation Pacific Eagle-Philippines, April 1, 2018 - June 30, 2018," August 6, 2018.

since the Cold War. According to media reports, Russia's massive exercise, which included units from China, involved hundreds of thousands of Russian soldiers and 1,000 aircraft.

U.S. RESPONSES TO RUSSIAN CHALLENGES

The 2018 National Defense Strategy stated that Russia seeks "to shatter the North Atlantic Treaty Organization and change European and Middle East security and economic structures to its favor." In the FY 2019 National Defense Authorization Act, Congress called for a U.S. response aimed at deterring and, if necessary, defeating Russian aggression.

Russian cyber attacks remain a key threat to U.S. security. The DoD has announced a "defend forward" strategy that focuses on disrupting or halting malicious Russian cyber activity at its source. In particular, the DoD Cyber Strategy 2018 states that the United States will conduct cyber operations to gather intelligence to be used in the event of crisis or conflict with states that can pose strategic threats to U.S. security, including Russia.

The U.S. European Command is also seeking to integrate offensive and defensive cyberspace into its contingency plans in order to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other warfighting elements of the Command. The DoD OIG issued a classified report in March 2018 that examines whether these efforts met the Command's objectives.

Marines park assault amphibious vehicles following a multi-national amphibious assault raid during the Rim of the Pacific exercise at Bellows Beach, Hawaii, July 28, 2018. (U.S. Navy photo)

The Obama Administration, in coordination with NATO allies, created the European Reassurance Initiative in 2014 in response to Russia's occupation of Crimea. The Trump Administration renamed this effort the European Deterrence Initiative to characterize its focus on deterring an increasingly assertive Russia. The FY 2019 $6.5 billion budget authorization for this initiative doubles its annual expenditure, and funds significant increases in U.S. military unit rotations to Europe and improvements in the capacity and capabilities of our European allies and partners.

One element of the European Deterrence Initiative is what the U.S. Air Force calls "an expeditionary base in a box"—which are containerized European Contingency Air Operation Sets prepositioned on large Air Force bases in Europe. Prepositioning the equipment needed to establish an expeditionary air base—such as fuel trucks to dining facilities to hospital tents—allows the Air Force to respond quickly to a crisis in Europe posed by adversaries such as Russia. The DoD OIG is currently conducting an audit examining U.S. European Command and U.S. Air Forces-Europe development and implementation of this equipment and initiative. A separate DoD OIG evaluation of the European Deterrence Initiative planned for 2019 will determine the extent to which the overall program has improved U.S. and NATO deterrent capabilities.

NORTH KOREA

According to the 2018 Defense Intelligence Agency Worldwide Threat Assessment, North Korea's intercontinental ballistic missile and nuclear weapon capabilities, combined with its potential to proliferate weapons of mass destruction, make it the most volatile strategic threat to the United States and to U.S. regional allies in the Pacific. North Korea's economic and military partnerships with Russia and China and its threat of proliferating nuclear technology to Iran or terrorist organizations increases the threat from North Korea. As the United States exerts economic and diplomatic pressure on North Korea to denuclearize, the DoD must maintain military readiness to be able to deter any North Korea aggression.

NORTH KOREA'S RELATIONS ARE IMPROVING WITH SOUTH KOREA BUT DECLINING WITH CHINA

South Korea focused its diplomatic efforts in 2018 on increasing its dialogue with North Korea, while maintaining its relationship with its allies and continuing to address the military and economic threats that China poses. South Korea's goal of reunifying the peninsula guided its economic and social efforts with North Korea under its "Sunshine Policy." This policy demonstrated its greatest effect in the 2018 Winter Olympics, where a composite team of North and South Korean athletes competed as one.

Additionally, China's leaders have publically stated that their support for international efforts to strengthen sanctions against North Korea. However, while China has leverage over North Korea as its principal trade partner and source of aid, China has not fully used that leverage. According to analysts at the Center for Strategic and International Studies, China fears a refugee crisis precipitated by a North Korean regime collapse. China also regards North Korea a "buffer zone" against U.S. forces in the south.

Marines maneuver to secure a notional enemy position during a live-fire training at Pohakuloa Training Area, Hawaii, July 13, 2018. (U.S. Marine Corps photo)

NORTH KOREA BALLISTIC MISSILE AND NUCLEAR CAPABILITIES

During this past year, North Korea continued to improve its ballistic missile and nuclear weapon capabilities, despite broad international condemnation and the imposition of additional United Nations security resolutions. In 2017, North Korea launched a record number of missiles and conducted the most nuclear tests in the history of North Korea's missile program, with launches and tests demonstrating the technological advances required to strike targets in South Korea, Japan, and now the U.S. mainland. Given this capability, in November 2017 Chairman Kim stated that he "had gone as far as he needed to go in his development," ceasing missile tests and launches as of that date.

The North Korean military remains a significant threat on the peninsula. In addition to its nuclear threat, North Korea's 1.5-million-man army possesses large chemical and conventional weapons capabilities. Improved medium- and short-range missile platforms currently can deliver conventional, chemical, or biological payloads against South Korean targets.

In April 2018, then Central Intelligence Agency Director Mike Pompeo visited North Korea and met with Kim Jong-un ahead of a June summit between President Trump and the North Korea leader. President Trump and Chairman Kim Jong-un held a summit in Singapore on June 12, 2018. During the summit, the two leaders discussed establishing new

U.S.–North Korean relations and building lasting peace on the Korean Peninsula. The progress on these goals since the summit has been halting, as the United States and North Korea seek agreement on denuclearization and what that means. Recently, North Korea has indicated that the only way it will permanently dismantle its nuclear complex is if the United States takes corresponding steps. U.S. diplomatic negotiations with North Korea are ongoing, most recently with a September 2018 visit there by Secretary of State Pompeo.

One positive outcome from the June 2012 summit has been the repatriation of the remains of what is believed to be 55 service members. However, according to Secretary Pompeo, North Korea continues to violate United Nations sanctions.

Recent advancements in North Korean missile and nuclear weapon technology also magnify the historical threat that proliferation of weapons of mass destruction poses throughout the world. As stated by the Director of National Intelligence in his 2018 Worldwide Threat Assessment, North Korea's history of exporting ballistic missile technology to countries like Iran and Syria and the help it provided during Syria's construction of a nuclear reactor demonstrate its willingness to proliferate dangerous technologies.

Lieutenant General Robert P. Ashley, the Director of the Defense Intelligence Agency, stated in his 2018 Worldwide Threat Assessment, "North Korea is a critical threat to the United States and our allies in Northeast Asia and is our hardest intelligence collection target." This intelligence deficit presents a significant challenge to the DoD's ability to verify or monitor North Korean efforts to abide by any agreement as the possibility of North Korea's denuclearization efforts materialize.

Meanwhile, North Korea continues to develop and employ sophisticated cyber capabilities, particularly used against foreign financial sectors. For example, North Korean cyber hackers have committed cyber theft from Far Eastern International Bank of Taiwan in 2017; and Bancomext of Mexico and Banco de Chile in 2018. U.S. officials have singled out North Korea among countries that pose growing cyber threats to the United States. For example, in its 2018 Worldwide Threat Assessment report released in February, the Office of the Director of National Intelligence said Russia, China, Iran and North Korea "will pose the greatest cyber threats to the United States during the next year."[5]

U.S. RESPONSE TO NORTH KOREAN CHALLENGES

The United States and its allies continued to strengthen their offensive and defensive ground, air, and sea-borne capability in the region. Recent improvements in defensive capabilities include Japan's approval to procure two Aegis Ashore anti-missile systems. Additionally, in 2017 the U.S. Army deployed the Terminal High Altitude Area Defense anti-missile systems to South Korea. Despite heavy criticism from both Moscow and Beijing, the deployment of Terminal High Altitude Area Defense bolsters South Korea's defensive capabilities against a potential missile strike from the north.

However, in 2018 the Government Accountability Office reviewed the Aegis Terminal High Altitude Area Defense systems, which are integral elements of the Ballistic Missile Defense System that identify and intercept enemy threats. The Government Accountability Office found that some of the computer models that the Missile Defense Agency uses to operationally assess the Aegis Terminal High Altitude Area Defense systems introduced ambiguity into the test results and needed to be accredited—programmed with the latest technical capability and threat intelligence data—to better reflect real-world conditions.[6]

[5] Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, March 6, 2018.

[6] GAO 18-324, "Missile Defense: The Warfighter and Decision Makers Would Benefit From Better Communication About the System's Capabilities and Limitation," May 2018.

To provide oversight of U.S. Forces Korea's ability to sustain its combat formations while countering the threat from North Korea, the DoD OIG is conducting an audit to determine whether the U.S. Indo-Pacific Command and U.S. Forces Korea have a distribution network to receive and deliver critical munitions in support of operation plan requirements.

IRAN

Iran remains a significant threat to security and stability within the Middle East and Southwest Asia, and U.S. security interests. Iran continues to engage in regional destabilizing activities, supports the Assad regime in Syria, backs the militant Shi'a terrorist organization Hezbollah in Syria and Lebanon, and contributes to disorder in Yemen and Iraq.

IRAN AND IRANIAN-BACKED GROUPS THREATEN THE CENTRAL REGION

The Department of State considers Iran the world's "most active state sponsor of terrorism." For example, with the support of Iran, the Lebanese Hezbollah sent thousands of fighters to Syria and provided weapons, tactics, and direction to militant and terrorist groups. Iran supports the Houthis, a Shiite group in North Yemen. Iran's financial support enables the Houthis to attack shipping near the Strait of Bab-el-Mandeb and other land-based targets within Saudi Arabia and the United Arab Emirates.

On February 27, 2018, General Joseph Votel, Commander of U.S. Central Command, testified before the House Committee on Armed Services that Iran remains "the major threat to U.S. interests and partnerships in the [U.S. Central Command] Region." He also stated that the competition between Iran and Saudi Arabia was exacerbating "multiple security dilemmas" in Yemen, Lebanon, and elsewhere. He added, "Iran has extended its tentacles across the region through numerous proxies, including Lebanese Hezbollah operating in multiple countries, hardline Iranian-backed Shi'a Militia Groups in Iraq and Syria, and Iranian support has enabled the Houthis."

A soldier hands out candy to a group of kids during a patrol along the demarcation line outside Manbij, Syria, July 14, 2018. (U.S. Army photo)

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

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. It supports about 20 percent of the world's oil flow and is vital to the national and economic interests of many nations around the world. The United States has imposed sanctions on Iran, which seek to deter countries from importing Iranian oil by November 4, 2018. In response, Iran threatened to block all oil exports through the Strait.

For several years, the Iranian Navy and the Islamic Revolutionary Guard Corps Navy have harassed U.S. warships operating there. The U.S. Navy classified approximately 10 percent of these interactions as "unprofessional or unsafe."

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

IRAN'S BALLISTIC MISSILE PROGRAM THREATENS THE REGION

Iran has the largest inventory of short- to intermediate-range ballistic missiles in the Middle East, and Iran has also proven its capability to develop, test, and produce an intercontinental ballistic missile. For example, in July 2017, Iran launched its *Simorgh* space launch vehicle, an expendable, small-capacity, orbital-carrier rocket. According to Daniel Coats, Director of National Intelligence, this could potentially shorten a pathway to an intercontinental ballistic missile because space-launch vehicles use similar technologies.

IRAN IS BUILDING ITS CYBERWARFARE CAPACITY

In his 2018 Worldwide Threat Assessment, the Director of National Intelligence Coats discussed Iran's desire to penetrate U.S. and allied partner information technology networks to conduct espionage and to position itself for future cyber interventions. According to U.S. officials at the 2018 Aspen Security Forum, Iranian hackers have laid the foundation to carry out widespread cyber attacks against private U.S. and European companies.

THE UNITED STATES' ACTIONS TO DETER IRANIAN THREATS

On May 8, 2018, the United States withdrew from the 2015 Joint Comprehensive Plan of Action—an agreement between Iran and the United States, China, France, Russia, the United Kingdom, and Germany regarding verification of Iran's compliance with nuclear related provisions that limited Iran's enrichment of uranium. After the announcement of the withdrawal, Secretary Mattis testified that the United States would continue to work with other nations to ensure that Iran does not acquire a nuclear weapon and to address the range of Iranian malign influences throughout the Mideast. He stated that the United States needed to confront Iran not only for its nuclear program, but also for its development of ballistic missiles, support of terrorism, launching of cyber attacks, and threats to international commerce.[7]

Withdrawal from the Joint Comprehensive Plan of Action resulted in the United States re-imposing 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. The effects of these sanctions remain unclear. Experts reported that Iran spends a large portion of its $350 billion budget on military and political interventions in Syria, Iraq, Yemen, and Lebanon. Moreover, Iran reportedly increased its military spending by 128 percent over the past 4 years. However, analysts disagree whether U.S. sanctions will prevent or provoke Iran's military expansion.

In summary, the United States and the DoD face formidable challenges in countering the individual and collective threats presented by competitor states such as China and Russia, as well as Iran and North Korea. Each nation presents the DoD with various challenges, including existing or emerging nuclear capabilities, cyber attacks, and weapons of mass destruction. Each is modernizing its weapons systems and pursuing various technological advances. The challenge for the DoD is to continue to maintain military superiority to deter military operations from U.S. adversaries, to prevent increased development of nuclear weapons, to counter support of terrorism, to combat cyber intrusions, and to mitigate threats to U.S. allies and partner countries.

[7] Senate Appropriations Committee, Subcommittee on Defense, "Review of the FY 2019 Budget Request for the U.S. Dept. of Defense," May 9, 2018.

Marines with 1st Marine Division, fire an M777 Howitzer at known targets during training at Mount Bundy Training Area, Northern Territory, Australia. (U.S. Marine photo)

Challenge 3: Countering Global Terrorism

The DoD defines terrorism as the unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political. The 2017 National Security Strategy asserts that terrorism, particularly violent attacks by al Qaeda, ISIS and their affiliated groups, remains a persistent worldwide threat. According to the 2017 Department of State Country Reports on Terrorism, terror attacks and related deaths are on the decline worldwide, but potent threats remain. The number of global terrorist attacks fell 23 percent in 2017 from the year before, and deaths attributed to these attacks decreased by 27 percent. However, the report noted that "the terrorist landscape grew more complex."

Violent extremist organizations, including al Qaeda and ISIS, undermine transregional security in the Middle East, Afghanistan, Africa, Southeast Asia, and Europe and across multiple domains, including air, land, maritime, and cyberspace. According to the 2015 National Military Strategy, violent extremist organizations are strongest where governments are weakest, and often coexist with transnational criminal organizations. These groups employ tactics that combine traditional terrorist tactics, such as improvised explosive devices, suicide vests, and vehicle ramming attacks, with tailored cyber campaigns that leverage available information tools to propagate destructive extremist ideologies, recruit and incite violence, and amplify the perceived power of their movements. Additionally, violent extremist organizations may use emergent and increasingly dangerous technologies, such as unmanned aerial vehicles and chemical, biological, radiological, or nuclear weapons.

The 2017 National Security Strategy directs the DoD to deter, disrupt, and defeat potential terrorist threats before they reach the United States. The DoD seeks to implement this strategy through overseas contingency operations and other counterterrorism activities. The DoD is now executing six named overseas contingency operations—Operation Inherent Resolve in Iraq and Syria, Operation Freedom's Sentinel in Afghanistan, Operation Pacific Eagle-Philippines in the Philippines, and three classified operations in the U.S. Africa Command and U.S. Central Command areas of responsibility. Through these overseas contingency operations and other security cooperation efforts, the DoD works with allies and partners to deter and disrupt terrorist groups.

Anbar Operations Center Commandos take a knee during training at Al-Taqaddum Air Base in Iraq, June 21, 2018. (U.S. Army photo)

DOD CHALLENGES IN COUNTERING TERRORISM

DoD efforts to detect and deter terrorism have many inherent challenges. For example, the DoD's counterterrorism operations often have timelines that span leadership changes, annual appropriations cycles, and authorizing legislative processes. Counterterrorism operations require flexibility and must be executed in a politically, financially, and militarily sustainable manner, often with the participation of Coalition partners. Moreover, the National Security Strategy now ranks great power competition as a higher priority over countering terrorism. "While terrorism [is a] clear and present danger – [and] remains a significant threat — Great power competition is now our primary challenge," Secretary Mattis said in September 2018. "It's increasingly clear that China and Russia seek to shape the world consistent with their authoritarian models."

Some of the most important challenges associated with counterterrorism operations, include addressing the nontraditional nature of the fight; coordination with Coalition partners; execution of a whole-of-government approach; adequacy of focus and resources; working with sovereign nations and foreign forces; and focusing limited resources and effort on the terrorist threat.

THE NONTRADITIONAL NATURE OF THE FIGHT

Violent extremist organizations are constantly changing to more effectively counter international efforts to defeat them. Terrorists regularly adapt their tactics, techniques, and procedures, particularly with respect to technology. For example, ISIS has employed conventional military tactics and guerilla warfare, as well as sophisticated media information operations, vehicle-borne improvised explosive devices, unmanned aerial systems, and various types of electronic jamming in Iraq and Syria. According to the Department of Justice, ISIS, al Qaeda, and similar groups are adopting new technologies, such as simple chemical weapons and small drone systems. They are also becoming more dispersed and clandestine, using the Internet to inspire and direct attacks in ways that are less vulnerable to conventional military action.

Countering this changing and increasingly complex threat requires resource management and coordination efforts at national and international levels. The DoD deploys relatively small numbers of U.S. military forces and leverages globally integrated command and control processes to enable transregional counterterrorism operations. This requires significant planning, coordination, and communication, both within the DoD and across bilateral and Coalition partnerships. The DoD also must remain nimble and adaptable in order to respond to frequent innovations in terrorist tactics and technology.

However, U.S. Government oversight agencies have identified ways that ongoing counterterrorism efforts can be more effective. For example, in a December 2017 report, the DoD OIG determined that U.S. Central Command and U.S. Africa Command did not provide effective oversight of counternarcotic activities. This is a critical weakness, because violent extremist organizations use many of the same smuggling and communications networks used for narcotics trafficking, and drug trafficking helps finance terrorist activity. Yet, neither U.S. Central Command nor U.S. Africa Command maintained reliable data for the completion status and funding of counternarcotic-related training, equipping, and construction activities.[8]

In another example, the Treasury OIG recently examined the extent to which information sharing is occurring among various Government and financial institutions. The majority of law enforcement agencies' program users stated that the Financial Crimes Enforcement Network's program helped law enforcement agencies by locating financial assets owned by subjects of terrorism and money laundering investigations and by identifying recent transactions. However, the Treasury OIG determined that increased use of Financial Crimes Enforcement Network's resources could enhance the disruption of ISIS finances and provide information to assist in investigations and subpoena preparation.[9]

COORDINATION WITH COALITION PARTNERS

To execute Coalition-based counterterrorism operations successfully, partner nations and organizations must overcome coordination challenges, including achieving a common strategic understanding of threats posed by violent extremist organizations and campaign objectives; overcoming interoperability issues; and aligning resources and tactics. Such coordination must also consider partners' political perspectives, considerations, and individual interests related to campaign activities.

The Defeat ISIS Coalition, which now includes 79 nations and international organizations, confronts these challenges as it leads the worldwide effort to counter ISIS. According to Combined Joint Task Force—Operation Inherent Resolve, the Coalition's military operations against ISIS have weakened that terror group in Iraq and Syria and enabled the Coalition partners to bring the full might of their national power—including diplomatic, informational, economic, and law enforcement—to fight against ISIS.

The DoD OIG continues to evaluate the effectiveness of coordinated counter-ISIS operations in Syria, Iraq, and elsewhere. For example, in 2016, the DoD OIG reviewed DoD policies related to the sharing of terrorism information with partner nations under Operation Inherent Resolve. While the DoD OIG determined that these policies allow information sharing, it also identified opportunities to improve the application of these policies, including improved enforcement of information sharing policies, tracking clearances of foreign partners, and awareness of sharing needs when developing information.[10]

In addition to challenges with coordinating operations, the success of Coalition-based counterterrorism efforts varies based on the amount of access to host nation leadership, security forces, and facilities, as well as based on the types and levels of political and military support from partner countries. These challenges have been particularly evident in the Defeat ISIS Coalition efforts in Iraq and Syria. In Iraq, the Coalition's policy was to only provide support that was accepted by, and coordinated through, the central government in Baghdad. However, at least one Coalition-member government initially only allowed training and equipping of Iraqi Kurdish Peshmerga

[8] Report No. DODIG-2018-059, "U.S. Central and U.S. Africa Commands' Oversight of Counternarcotic Activities," December 26, 2017.

[9] Treasury OIG-18-040, "Terrorist Financing/Money Laundering: FinCEN's Regulatory Helpline Provides Guidance But Controls Need to be Enhanced," February 26, 2018.

[10] Report No. DODIG-2016-081, "Evaluation of U.S. Intelligence and Information Sharing With Coalition Partners in Support of Operation Inherent Resolve," April 25, 2016.

forces, which operate under the Kurdistan regional government, and may have provided some of this support without the consent of the central government in Baghdad.

Similarly, some Coalition partners may place restrictions on their participation in a shared mission. For example, some Coalition members have limited or restricted their involvement in Syria because they are uncomfortable with the level of threat to their forces inside Syria or the potential for involvement in the ongoing Syrian civil war. Syria is a particularly challenging environment because the Defeat ISIS Coalition operates there without the permission or support of the Syrian regime and in the vicinity of several other foreign entities and their surrogates (including Iran, Russia, Gulf Cooperation Council countries, Syria, Israel, and Turkey), which have different and often conflicting goals and operational activities.

THE WHOLE-OF-GOVERNMENT APPROACH AND INTERAGENCY COORDINATION

According to Brett McGurk, the Special Envoy for the Global Coalition to Defeat ISIS, the counter-ISIS fight will extend far into the future, requiring all elements of the Coalition's collective national powers, including military, economic, diplomatic, intelligence, law enforcement, counter-finance, and counter-messaging efforts. A major challenge in counterterrorism is that while offensive military operations significantly affect the capacity of violent extremist organizations to conduct terrorist acts, counterterrorism operations may not change the political conditions on the ground that foster terrorism. In addition, counterterrorism also requires action to address destruction of property and infrastructure, weakened civilian governance institutions, casualties, and civilian dislocation resulting from terrorism and counterterrorism operations. However, the DoD is not structured, resourced, or trained to fully address these types of problems. Instead, it must rely on other agencies, such as the Department of State and the U.S. Agency for International Development, which have specialized capacity to address these complex governance and humanitarian challenges, but who may not be adequately resourced. Defeating violent extremist organization threats requires a whole-of-government approach, with adequate resources, to plan and coordinate the multiple aspects of counterterrorism operations and the stabilization efforts that follow.

Master Sgt. Andrew Ensman, Train, Advise and Assist Command – Air loadmaster advisor, discusses the high velocity ballistic airdrop mission with Lt. Col. Samuel Mcintyre, TAAC-Air pilot advisor, Maj. Gen. Barre Seguin, Deputy Commander-Air for U.S. Forces-Afghanistan, and an Afghan Air Force loadmaster, September 26, 2018, Kabul, Afghanistan. (U.S. Air Force photo)

A Marine Corps explosive ordnance disposal technician supporting Operation Inherent Resolve talks to partnered forces. (U.S. Army photo)

The U.S. Government has struggled to coordinate and execute whole-of-government counterterrorism strategies consistently across agencies. For example, the Operation Inherent Resolve campaign is based on a whole-of-government, Coalition-supported strategy with responsibilities for achieving nine original lines of effort divided between multiple U.S. agencies, including the Departments of State, Treasury, Homeland Security, Justice, and Energy, and the U.S. Agency for International Development. The DoD has been in the lead in the effort to defeat ISIS since the fall of 2014. ISIS has been largely defeated as a military force, with ongoing operations against small pockets of fighters remaining in both Syria and Iraq.

However, the focus of Operation Inherent Resolve activities in Iraq is now shifting away from traditional military operations and into stabilization and governance building activities, which requires greater participation by other government agencies. For example, the DoD, with Coalition assistance, has been training and equipping local hold forces and border guards in Iraq. However, the DoD core capabilities cannot adequately address significant stabilization needs related to governance, humanitarian assistance and development.

The Secretaries of State and Defense and the Administrator of the U.S. Agency for International Development have developed a 2018 framework, called the Stabilization Activities Review, which identifies ways to maximize the effectiveness of U.S. Government efforts to stabilize conflict-affected areas. This document recommends formally delegating primary responsibility for stabilization activities to the Department of State, placing the DoD in a supporting role. The Stabilization Activities Review highlights the need for continuous interagency coordination for stabilization activities, yet it does not identify a single office or individual responsible for resolving disputes between the agencies. While the Operation Inherent Resolve campaign plan provides guidance on military coordination with interagency partners, and support for their activities, it remains uncertain how the stabilization effort will be led, de-conflicted, and coordinated outside of the DoD.

WORKING WITH SOVEREIGN NATIONS AND FOREIGN FORCES

To execute counterterrorism missions, the DoD increasingly deploys small numbers of rotating forces, while relying heavily on the cooperation of foreign partner governments and security forces. This strategy, known as "by, with, and through," seeks to build the capacity of partners through focused, host-nation-validated train, advise, and assist activities designed to achieve specific objectives linked to a broader campaign plan. The DoD augments these activities with the provision of combat-enabling weapons, equipment, and military tools (such as intelligence, targeting, reconnaissance, air attack, logistics, and planning assistance) in support of partner-led operations.

While this approach seeks to empower local forces and political leadership and reduces the political and cultural impact associated with the presence of Coalition forces, it also presents challenges. With their own forces and territory at risk, the host nations may not allow their security forces time away from ongoing operations to participate in training. Similarly, host nations may be reluctant to coordinate and adjust their military activity to align with Coalition objectives and timelines. Some governments also may face political consequences

Soldiers during an air assault training mission on Marine Corps Base Hawaii, Kaneohe, Hawaii. (U.S. Army photo)

if they acknowledge their need for assistance or foreign troop presence. Local political and cultural factors, endemic corruption, and other local considerations, such as access, legal protections, and security for DoD forces in conflict areas, may also complicate the DoD's mission execution. Additionally, it may be difficult to secure continued host-nation support and commitment (political or otherwise) after "victory" against the military threat.

These challenges are particularly evident in the Operation Freedom's Sentinel mission in Afghanistan. U.S. and NATO forces train, advise, and assist Afghanistan's security forces. This Coalition-based mission, called Resolute Support, seeks to build the capacity of the Afghan Ministries of Defense and Interior to plan, budget, organize, recruit, and operate and to strengthen the operational effectiveness of the Afghan security forces. Afghan security forces assumed leadership of the counter-Taliban fight in 2015, which reduced the burden on the United States. However, the Afghan forces have struggled against a resilient Taliban insurgency and attacks by the local ISIS affiliate, and have suffered extensive casualties.

The DoD OIG has identified challenges associated with this approach to working through host-nation forces within the complex NATO mission in Afghanistan, including sustainment planning, contract management, corruption and effectively assessing outcomes. For example, in a 2018 report, the DoD OIG described how the train, advise, and assist efforts in Afghanistan resulted in notable accomplishments in three broad areas: (1) A-29 aircraft mission performance, (2) night-vision capability, and (3) air-ground integration between the Afghan Air Force and the Afghan National Army. However, the report also identified that there was insufficient planning for developing the Afghan Air Force, including no identified desired end-state capabilities and capacities and a lack of metrics to track its development. The DoD OIG also determined that the existing Contractor Logistics Support agreements reduce the maintenance opportunities for the Afghan Air Force mechanics to perform maintenance work, thus slowing efforts to develop organic maintenance capability.[11]

The DoD is experiencing similar challenges in conducting train, advise, and assist activities in Iraq and Syria. Compared to previous DoD operations in Iraq, under Operation Inherent Resolve the DoD has fewer deployed forces, limited access to many parts of the conflict area, limited authorities in terms of rules of engagement and accompanying partner forces, and a much-reduced infrastructure of bases and support facilities in theater. These factors require increased dependence on working with local partners and the use of their facilities. However, this dependence has resulted in inadequate storage, maintenance, and tracking of equipment required for train, advise, and assist efforts. For example, in a 2017 report, the DoD OIG determined that U.S. forces used the Iraq Train and Equip Fund procurement process to equip the Iraqi Counterterrorism Service for combat operations in accordance with the applicable law. At the same time, U.S. and Coalition advisers had difficulty drawing equipment from Counterterrorism Service warehouses to

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

provide adequate training to Counterterrorism Service recruits. In addition, training courses developed by the U.S. and the Coalition did not contain well-defined standards of evaluation for Counterterrorism Service trainees.[12]

In short, as the terrorist threat continues to expand geographically, the importance of effective partner collaboration will increase. To ensure effective use of coalitions and partnerships, the DoD must conduct regular assessments of worldwide threats and partner capabilities, effectively manage its deployed assets, and regularly coordinate with the other Government agencies and international partners that can offer expertise and resources to counter a complex threat and achieve shared goals.

FOCUSING RESOURCES AND EFFORT

As the DoD continues to address transregional terrorist threats, it will also need to effectively balance counterterrorism needs for resources and personnel with other DoD priorities. The DoD must constantly review and prioritize how to deploy limited resources—including personnel, equipment, and intelligence capacity—for counterterrorism operations around the world.

The challenges of fighting terrorism on multiple fronts has been evident in the Philippines, where the DoD provided significant support and partnering efforts with the Armed Forces of the Philippines for 13 years under Operation Enduring Freedom-Philippines to counter various jihadist terror groups. Based on improvements in the capabilities of the Armed Forces of the Philippines,

A member of the Iraqi Counter Terrorism Service stands guard as a helicopter lands during fast-rope training in Baghdad, April 25, 2018. (U.S. Army photo)

[12] Report No. DODIG-2017-074, "Assessment of U.S. and Coalition Plans and Efforts to Train, Advise and Equip the Iraqi Counterterrorism Service and the Iraqi Special Operations Forces," April 19, 2017.

Soldier with 17th Combat Sustainment Support Battalion, fires an M136E1 AT4-CS confined space light anti-armor weapon at Joint Base Elmendorf-Richardson, Alaska, October 12, 2017. (U.S. Air Force photo)

successes against terrorists, and continuing resource constraints, the DoD ended that operation in 2014. As the DoD shifted its focus and resources more toward operations in Afghanistan, Iraq, and Syria, the Philippines was no longer a DoD counterterrorism priority. In the summer of 2017, ISIS-Philippines attacked and took over Marawi. This noteworthy ISIS-Philippines military success brought renewed DoD focus to the terrorist threat in the Philippines, and resulted in the designation of Operation Pacific Eagle-Philippines as an overseas contingency operation. Under this operation, U.S. special operations forces provide training, advice, and other assistance, including intelligence, surveillance, and reconnaissance support to the Armed Forces of the Philippines.

In the Philippines and other areas, it is important that the DoD use metrics to evaluate campaign success, to continuously assess progress, and to allow decision makers to assess the level of threat and properly allocate resources. To support this effort, the DoD OIG is evaluating U.S. train, advise, assist, and equip efforts to build and sustain the capabilities of the Armed Forces of the Philippines to counter the expansion of violent extremist organizations. The evaluation will address multiple factors, including specific unit effectiveness and metrics for success

Similarly, the DoD must ensure it counters the complex terrorist threat posed by Iran. Secretary Mattis recently stated, “Everywhere you go in the Middle East, where there’s instability, you’ll find Iran.” According to the 2017 Department of State Country Reports on Terrorism, Iran remains the world’s leading state sponsor of terrorism with funding networks and operational cells working around the world. Iran is responsible for intensifying multiple conflicts and undermining U.S. interests in Syria, Yemen, Iraq, Bahrain, Afghanistan, and Lebanon.

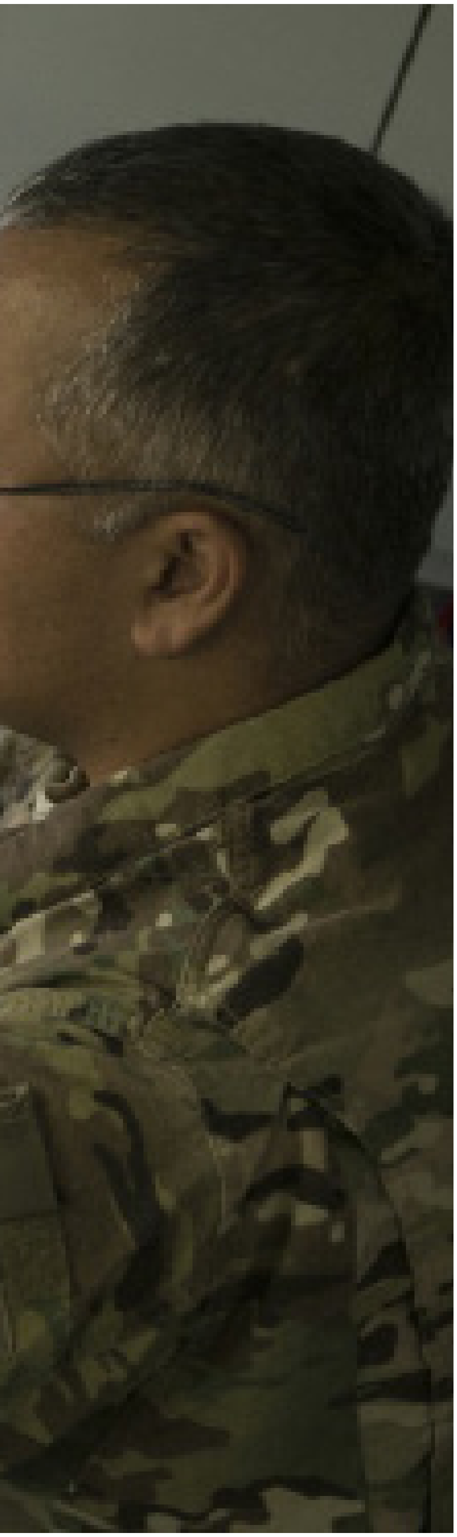
Africa is also an increasingly complex arena for counterterrorism operations. The 2017 National Security Strategy characterizes many African states as battlegrounds for violent extremism and jihadist terrorists. ISIS, al Qaeda, and their affiliates (such as Boko Haram and Al Shabab) operate on the continent and have increased the lethality of their attacks, expanded into new areas, and targeted U.S. citizens and interests. ISIS West Africa is one of the largest ISIS affiliates in terms of estimated strength and territory under its control. It conducts attacks against government forces and civilians in the Lake Chad region of Nigeria, Chad, Niger, and Cameroon. ISIS in the Sahel region south of the Sahara Desert is small but has temporary alliances with other extremist groups and aspires to conduct attacks against local interests and security forces across the region. ISIS in the North African Maghreb continues to be a hub for training and facilitation of resource movement, and ISIS in the Horn of Africa is small but attempting to expand its footprint. ISIS and other groups in the Sinai continue attacks against Egypt and Israel.

African terrorism has generally been a lower DoD priority than the conflicts in Iraq, Syria, and Afghanistan. However, to help counter these threats, the DoD is assisting several African nations to improve the ability of their security services to counter terrorism, and promote regional stability. The United States is not engaged militarily as part of a coalition in Africa but works with partners, including Nigeria, Morocco, and France, to support their efforts to deny space to ISIS and other extremist groups and to close facilitation networks and transit routes running through Libya, Sudan, and the Maghreb. Because of resource constraints, U.S. Africa Command is reducing its special operations presence in Africa, which could further complicate the DoD's ability to adequately address these threats, and potentially lead to a resurgence or more dangerous violent extremism there.

The DoD OIG is evaluating the DoD's counterterrorism activities in Africa. For example, the DoD OIG is conducting an audit to determine whether Army units assigned to U.S. Africa Command as Regionally Aligned Forces were trained to meet mission requirements, as described in the U.S. Africa Command Theater Security Cooperation Plan. This plan documents plans, priorities, and allocation of DoD resources across the full spectrum of military engagement within an area of operations, and serves as the roadmap for the execution of security cooperation activities. Additionally, the DoD OIG plans to assess whether U.S. Africa Command personnel planned and executed Military Information Support Operations to degrade the enemy's relative combat power, reduce civilian interference, minimize collateral damage, and maximize the local populations support for operations. These operations allow the military to convey selected information to foreign audiences to influence their attitudes, perceptions, and objective reasoning to reduce the likelihood of terrorist attacks.

In summary, the DoD faces significant challenges in countering the evolving terrorist threat, while at the same time addressing the top priority threats from global powers such as Russia and China. Working by, with, and through foreign partners, and the increased employment of the Coalition model, also presents significant challenges, including the need for joint planning, interoperability, and addressing the political and operational challenges of individual nations. In addition, counterterrorism requires a whole-of-government approach, with particular emphasis on related non-security issues, such as stabilization.

U.S. Air Force Master Sgt. Michael Duchesne Jr., 353rd Special Operations Group financial analysis section chief reviews numbers in the accounting system during end of year close out. (U.S. Air Force photo)



Challenge 4: Financial Management: Implementing Timely and Effective Actions to Address Financial Management Weaknesses Identified During the First DoD-Wide Financial Statement Audit

A key component of the 2018 National Defense Strategy signed by Secretary Mattis is budget discipline and affordability of DoD forces. In addition, as stated by Under Secretary of Defense (Comptroller)/Chief Financial Officer David Norquist, it is important that Congress and the American people have confidence in the DoD's management of every taxpayer dollar. The National Defense Strategy states that better management begins with effective financial stewardship.

To accomplish this goal, the DoD must make continuous process improvements to its financial management. As a result of a legislative requirement in the National Defense Authorization Act for FY 2014, the DoD was required to assert audit readiness and to undergo its first full financial statement audit in 2018. Because the DoD faces and will continue to face significant challenges related to financial management due to the complexity of the DoD and the shortcomings of its current financial management processes, the DoD did not receive a clean audit opinion for FY 2018. However, the benefit of the audit is not based on the overall opinion in the first year of a full financial statement audit; rather the benefit will be determined by whether the DoD addresses the Notices of Findings and Recommendations identified during the audit, and whether it continually improves its financial management and business processes.

IMPORTANCE OF FINANCIAL AUDITABILITY

In FY 2018, the DoD received more than 50 percent of the total U.S. Government's discretionary funding. It also has the majority of Government financial assets. For example, in FY 2017, of the $3.5 trillion in assets reported on the Government-wide financial statements, the DoD accounted for $2.6 trillion. Because of the size of the DoD budget, until the DoD obtains an unmodified or clean audit opinion, the Government-wide financial statements will not receive an unmodified or clean audit opinion.

On September 27, 2017, as required by the National Defense Authorization Act for FY 2014, Secretary Mattis and Under Secretary Norquist notified the DoD Inspector General that the DoD was ready for a financial statement audit. However, the DoD also noted that it was not expecting an unmodified or clean audit opinion on its first full audit of the Agency-Wide consolidated financial statements. In his notification to the DoD Inspector General, Secretary Mattis stated that he was not certifying that the DoD financial statements or Components' financial statements were reliable; rather, he was asserting that the DoD had the capabilities to allow an auditor to scope and perform a full financial statement audit that could result in actionable feedback on various financial management processes, systems, and documentation.

Secretary Mattis also notified Congress that the DoD would begin full financial statement audits in FY 2018. He wrote that it would take time for the DoD to go from being audited to passing an audit, and he acknowledged that the challenge of achieving a favorable opinion is significant. In expressing the importance of the financial statement audit, Secretary Mattis stated, "Being under audit goes hand-in-hand with rebuilding and modernizing our armed forces… ." He explained that the full financial statement audit is a fundamental part of his goal to reform the DoD and its way of doing business.

The Chief Financial Officers Act of 1990 requires that the DoD OIG either perform or contract for DoD financial statement audits. The DoD OIG is the principal auditor for the DoD Agency-Wide basic financial statements. The DoD Agency-Wide basic financial statements provide the financial status of the entire Department. Additionally, there are reporting Components within the DoD that, while included in the DoD Agency-Wide statements, are also required by the Office of Management and Budget to prepare stand-alone audited financial statements.

The National Defense Authorization Act for FY 2016 required the use of independent public accountants to audit the stand-alone financial statements of DoD Components. In addition, it required the DoD OIG to monitor those audits. The DoD OIG performs audits of DoD Components that are not required by the Office of Management and Budget and are not individually material to the Agency-Wide financial statements, but taken as a whole are material to the Agency-Wide financial statements. The DoD OIG uses the results of the DoD Component audits to support its audit of the Agency-Wide financial statements. During FY 2018, the DoD OIG completed or oversaw the completion of 21 financial statement audits, including the Audit of the FY 2018 and FY 2017 Agency-Wide Basic Financial Statements.

These audits identified numerous findings and recommendations. For example, the audits found that DoD Components had incomplete universes of transactions; incomplete and inaccurate lists of financial management systems; unsupported journal vouchers; incomplete valuations of inventory and General Property, Plant, and Equipment (PP&E); unreconciled Fund Balance With Treasury; and lack of corrective actions for findings from prior year audits. As a result, the DoD received a disclaimer of opinion from the DoD OIG for FY 2018, meaning an overall opinion could not be expressed on the financial statement under audit.

Financial statement audits not only determine the accuracy of financial statements, they also identify weaknesses and inefficiencies in the DoD financial management processes, including transactions to account for transportation of people and things; acquisition of property, parts, and supplies; and storage of inventory. Improvements to these

DoD financial management processes can lead to efficiencies that can have clear financial and operational impact for the DoD. For example, because of findings during the FYs 2017 and 2018 audits of the Defense Logistics Agency Working Capital Fund financial statements and other audits performed by the DoD OIG, Defense Logistics Agency management began developing actions to improve its identification and analysis of inventory it stored for itself and others.[13] Specifically, these reviews identified obsolete inventory that was being held in long-term storage and excess spare parts that were not needed.[14] Removing these items from the inventory can free up funds that were spent on storage to address other requirements for the warfighter. In addition, improved inventory management can also ensure that defective parts are identified and removed from the inventory in a timely manner.[15]

There are other benefits to accurate records related to inventories and PP&E. For example, if a Military Service does not have accurate counts of equipment, such as helicopters, it might not know how many helicopters it has, which could impact its operational readiness if the Service does not have enough helicopters to perform its required missions. Or if a Service does not know whether it has enough spare parts to ensure that aircraft are able to fly, it may have to spend significant amounts of money to get spare parts quickly because of operational requirements.

Further, accurate information on costs related to assets such as inventory and PP&E can help the DoD make more informed decisions on future purchases and repair cost of those assets. For example, establishing proper baselines or historical costs can provide the DoD accurate life-cycle costs of weapon systems so it can develop proper forecast and budget request on future purchases. In short, improvements to identification and analysis of inventory could provide the DoD management more accurate information, leading to improved readiness, greater efficiency, and improved operations.

Additionally, testing of DoD information technology systems, and interfaces between information technology systems, that is conducted as a part of the financial statement audits can identify vulnerabilities of those systems and result in recommendations to improve the DoD’s cyber security.

A Romania IAR-330 Puma helicopter and an American UH-60 Blackhawk conduct air movement procedures back to Mihail Kogalniceanu Air Base. (U.S. Army photo)

[13] Report No. DODIG-2016-036, “Management of Items in the Defense Logistics Agency’s Long-Term Storage Needs Improvement,” December 22, 2015 and Report No. DoDIG-2018-054, “Transmittal of the Disclaimer of Opinion on the Defense Logistics Agency Working Capital Fund Financial Statements and Related Footnotes for FY 2017,” December 12, 2017.

[14] Report No. DODIG-2016-036, “Management of Items in the Defense Logistics Agency’s Long-Term Storage Needs Improvement,” December 22, 2015.

[15] Report No. DODIG-2017-059, “Defense Logistics Agency Land and Maritime Can Improve Its Processes to Obtain Restitution From Contractors That Provide Defective Spare Parts,” February 23, 2017.

TONE AT THE TOP

"Tone at the top" is a fundamental component of an effective internal control environment.[16] The tone at the top of the DoD, from the Secretary of Defense to the DoD Comptroller on down, has supported the importance of DoD financial statement audits.

For example, on May 25, 2018, Secretary Mattis issued a memorandum to all DoD personnel clearly expressing the need for and benefits of sound financial management. The Secretary stated: "[E}very decision we make must focus on both lethality and affordability, thereby gaining full value for each taxpayer dollar spent on defense. To reinforce this requirement, in December the Department launched its first full-scale audit across the entirety of our business processes and systems. Audits provide an objective assessment of how we fulfill our missions, conduct our programs, issue contracts, mitigate cyber threats to our information technology systems, and manage our people and finances."

Secretary Mattis's memorandum explained his vision for action on the part of each and every member of the DoD: "Each of us, at every level within the Department, are accountable to the American public. We are responsible for taking immediate corrective action when a discrepancy is uncovered, and to develop a plan of action and associated milestones for the longer term. We must then identify the fundamental, underlying problem and change our processes to prevent its reoccurrence. We will provide periodic updates to Congressional leaders and in November we will publish our annual results on the DoD's public website to ensure full transparency."

Secretary Mattis closed his memorandum by explaining the costs, benefits, and the obligation of each of the 2.1 million members of the DoD: "Professionals invite scrutiny. Remediate findings from audits and introduce rigor into the DoD systems, processes, and controls to help achieve our Department's third line of effort: reforming the Department for performance and affordability. While a clean audit may take years to achieve, your efforts and your leadership foster transparency, accountability, and business process reform, enabling us to meet our fundamental obligation to turn over this Department better than we found it."

Following Secretary Mattis's lead, other DoD leaders have also expressed support for or initiated actions to promote his tone at the top and his direction to maximize the value of the financial statement audit and to improve the financial management processes and systems. During testimony before the Armed Services Committee, Under Secretary Norquist stated, "We don't have to wait for a clean opinion to see the benefits of the audit. The financial statement audit helps drive enterprise-wide improvements to standardize our business processes and improve the quality of our data." He noted, for example, that the Air Force identified 478 buildings and structures at 12 installations that were not in its real property system and the Army found 39 Black Hawk helicopters that had not been properly recorded in its property system.

Under Secretary Norquist also stated, "Transparency, accountability and business process reform are some of the benefits of a financial statement audit. Regarding transparency, the audit improves the quality of our financial statements and the underlying data that we make available to the public, including a reliable picture of our assets, liabilities and spending."

WEAKNESSES IN THE DOD FINANCIAL MANAGEMENT PROCESSES

In his notification of audit readiness to the DoD Inspector General, Secretary Mattis also stated that he expected to receive actionable feedback on various financial areas, including existence, completeness, and valuation of certain assets. As anticipated, during FY 2018, auditors identified weaknesses in these and other DoD financial

[16] GAO-14-704G, "Standards for Internal Control in the Federal Government," September 10, 2014.

management processes. To ensure the audits result in changes, the auditors regularly issue Notices of Findings and Recommendations throughout the audit. Auditors use these notices to communicate to management the weakness they identified, the impact of these weaknesses on the financial management processes, the reason the weaknesses exist, and recommendations to management for correcting the weaknesses.

As of November 15, 2018, the auditors had issued more than 1,000 Notices of Findings and Recommendations related to multiple financial management processes. Some of the most significant recommendations relate to:

- Universes of Transactions, which refers to the entirety of underlying, individual, accounting transactions that support a balance or line item on the financial statements of each DoD Component;
- Fund Balance With Treasury, which is the checkbook for each of the Components and identifies the amount of funds available and spent through the U.S. Department of the Treasury;
- PP&E, which refers to the identification and valuation of assets such as land, buildings, and military equipment; and
- Service-Owned Inventory in the Custody of Others, which includes items, such as spare parts and ammunition, that are being held or stored by an organization that is not the owner.

DoD Components must assign ownership of each contributing issue to an individual organization or command, which ensures accountability closest to the root cause. The responsible organization then develops a corrective action plan or plans and associated milestones for correcting that condition. Organizations must regularly report progress on implementing their corrective action plans to the Financial Improvement and Audit Results Governance Board and Secretary Mattis.

The following sections provide more detailed discussion of weaknesses in each of these financial management processes and the challenges the DoD faces in correcting the weaknesses identified by the auditors. The financial management processes discussed below are not meant to be a comprehensive listing of all the challenges the DoD faces, but rather systemic deficiencies that impact multiple DoD Components.

Stryker armored vehicle at Maryland's Aberdeen Proving Ground. (U.S. Army photo)

UNIVERSE OF TRANSACTIONS

A significant roadblock to the DoD achieving a clean audit opinion on its financial statements is 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. A universe of transactions is a central repository of financial transactions that are combined from multiple systems. In order to undergo an audit, the DoD Components must be able to identify a universe of transactions and reconcile those transactions with the General Ledger.

The DoD Comptroller has developed a tool called the Auditable Universe of Data – Intelligence Tool that is designed to consolidate millions of transactions from 19 different DoD accounting systems in one location for over 100 DoD Components. In addition, the DoD is developing universes of transactions to consolidate their financial and financial-related transactions. Once established, the universes of transactions will provide auditors one location to obtain the necessary transactions to perform a financial statement audit of the DoD Components.

However, due to the significant number of transactions, systems, and users, DoD Components are experiencing challenges in producing complete, accurate, and reconcilable universes of transactions. Once the DoD is able to produce one universe of transactions that is accurate and complete, it will not only have auditable financial statements, it can also use the universe of transactions to improve its operations. For example, the DoD plans to use the universe of transactions to perform cost management analysis of its programs, to improve budgeting, and forecasting of programs such as the Joint Strike Fighter Program; link cost performance data to related priority missions, such as Operation Inherent Resolve; and, provide assurance that internal controls are in place and effective at managing risk, such as the risk for duplicate payments.

FUND BALANCE WITH TREASURY—BALANCING THE DOD CHECKBOOK

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 balance in its respective accounting system, similar to a personal checkbook. As of September 30, 2017, the DoD reported a Fund Balance with Treasury account balance of $502 billion.

Similar to a personal checking account, a key internal control is balancing the checkbook against the bank statement to ensure that all deposits and payments are accounted for. Each month, the DoD Components have the critical task of reconciling their checkbooks with their bank accounts. Although this may appear to be a relatively easy process, it is not; auditors continue to find deficiencies in the DoD's process to routinely reconcile these accounts and resolve discrepancies. For example, 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. In addition, the DoD Components struggle with balancing their checkbooks due to a complicated business process that allows them to use each other's funds.

A recent DoD OIG audit determined that 104 "Other Defense Organizations," including Defense agencies, defense-wide appropriations and programs, trust funds, and other accounts, share one checkbook known as the TI-97 Fund Balance With Treasury account. Because the Treasury reports one balance for all Other Defense Organizations, these organizations face unique challenges in balancing their individual checkbooks with the

Treasury.[17] Effective reconciliations assist in preventing Other Defense Organizations' payments from exceeding the money provided to them by Congress and providing an accurate measurement of the status of available resources. Although the DoD has a process to perform reconciliations between the TI-97 checkbook and the Department of the Treasury, recent reports have found that reconciliations are inaccurate and that the DoD continues to make unsupported adjustments to balance its checkbook.

As highlighted by continued audit findings related to Fund Balance With Treasury for the DoD Components, auditors cannot verify the completeness and accuracy of this balance. More important, DoD leadership continues to make spending decisions without knowing the accurate balance of funds available with the Treasury. Without a proper checkbook balance, the DoD's spending decisions could result in an over- or underutilization of its appropriation. For example, if a DoD Component believes it will overspend its appropriation, it might not hire sufficient staff, make needed repairs, or maintain critical equipment.

GENERAL PROPERTY, PLANT, AND EQUIPMENT

General Property, Plant, and Equipment (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 it, 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 $762 billion as reported by the DoD on the FY 2017 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 items on the PP&E list exist, and that the list of PP&E is complete. However due to the size, age, and locations of the PP&E, the DoD faces challenges in verifying all assets have been inventoried and obtaining evidence to support how much the DoD paid. 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.

The DoD must also ensure that PP&E is reported on the correct DoD Component's financial statements. This process is not clear due to the interdependency of the DoD Components. For example, U.S. Special Operations Command is dependent on the Component Special Operations Commands for providing General Equipment balances for reporting purposes. A recent DoD OIG report determined that U.S. Special Operations Command overstated its General Equipment account balance by $5.7 billion and could not support another $261 million in General Equipment on its FY 2015 financial statements. This occurred, in part, because the U.S. Special Operations Command did not effectively coordinate with the Component Special Operations Commands to obtain the necessary information from their property systems. In addition, the property systems of the Component Special Operations Commands did not contain accurate and complete data.[18]

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 should procure to effectively support the readiness of its military forces. In addition, if DoD management's decisions on future acquisitions

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

[18] Report No. DODIG-2018-123, "U.S. Special Operations Command Reporting of General Equipment on Its Financial Statements," June 4, 2018.

and equipment distribution are based on an inaccurate inventory, it could lead to unnecessary expenditures and harm equipment readiness. For example, the DoD OIG recently determined that the Army did not properly account for $5.1 billion of Army Prepositioned Stock in Kuwait and Qatar. In addition, Army did not properly account for shortages, losses, and delivery of Army Prepositioned Stock in Kuwait. As a result, the Army did not know what equipment it should procure to effectively support its deployed soldiers.[19]

SERVICE-OWNED INVENTORY IN THE CUSTODY OF OTHERS

The Military Services and DoD Components own inventory that they are responsible for reporting on their financial statements. However, this inventory can be in the custody and managed by the Military Service or DoD Component that owns it or it can be in the custody and managed by another organization. For example, as of October 1, 2017, the Military Services reported that the Defense Logistics Agency held approximately 46 percent of the Army's inventory, 39 percent of the Navy's inventory, and 45 percent of the Air Force's inventory, ranging from clothes to spare parts to engines.

When inventory is held by others, the entity that holds the inventory is known as the service provider. However, the owners of the inventory rely on the accuracy of the service providers' data for both accounting transactions and for operational decision-making. For example, if a Military Service believes that it has a low quantity of a spare part based on a service provider's inaccurate report, or the Military Service does not review the inventory held by others, it may decide to order additional parts that it does not need. Alternatively, if a Military Service believes that it has a sufficient quantity of a spare part based on a service provider's inaccurate report and does not review the inventory held by others, it may decide to not order additional parts and ultimately impact the readiness of the warfighter.

For example, after reviewing the Army's management of the MQ-1C Gray Eagle spare parts, the DoD OIG identified internal control weaknesses in its inventory management process. Specifically, the Army did not include the spare parts in its inventory for FY 2017, did not consider inventory located at DoD-fielded locations when forecasting a future need for spare parts, or did not require the use of existing Defense Logistics Agency inventory before purchasing the spare parts. This resulted in the Army maintaining millions of dollars in excess spare parts.[20]

The DoD is now making improvements to its inventory processes, such as establishing a baseline by performing physical counts of millions of inventory items to ensure the information in its systems is accurate. However, the DoD faces challenges in this effort because of a variety of factors, including the resources needed to complete the counting process, the decentralized nature of the DoD inventory, and the need to implement improvements while not interrupting the delivery of mission essential items to the Military Services.

To improve their inventory processes, the Military Services need to maintain records of the inventory purchased and perform periodic reconciliations with the service providers reported quantities. During the FY 2018 financial statement audits, auditors have found that these reconciliations are not performed or that differences noted in the reconciliations remained unresolved. For example, auditors determined that the Army did not design and implement a consistent, formal reconciliation process between contractor inventory management systems and the Army's inventory management system. In addition, the Army reviewed only the

[19] Report No. DODIG-2018-132, "Management of Army Equipment in Kuwait and Qatar," June 29, 2018.

[20] Report No. DODIG-2016-080, "Army's Management of Gray Eagle Spare Parts Needs Improvement," April 29, 2016.

U.S. and coalition forces pose for a group photo following a joint coalition exercise at Camp Lemonnier, Djibouti, Sep. 5, 2018. (U.S. Navy photo)

10 largest discrepancies identified during the reconciliations performed in FY 2018 between Defense Logistics Agency inventory management systems and the Army inventory management system. This resulted in a large number of deficiencies that were not addressed or corrected in FY 2018. Without proper accounting and internal controls, the DoD will continue to lose track of its assets, buy additional items unnecessarily, and store obsolete items.

INFORMATION TECHNOLOGY

Obtaining and maintaining reliable information technology systems, including financial systems, is critical to DoD operations as well as to obtaining a clean audit opinion. In May 2018, the DoD Deputy Chief Financial Officer explained the importance of a proper information technology environment, stating that the goal of the DoD is to link accurate and complete financial information to performance for better accountability.

However, the DoD's information technology systems include a mix of legacy and modern systems. In 2016, the DoD reported that it had nearly 400 separate information technology systems used to process accounting data that supported the financial statements of the DoD. Most of the legacy systems were originally designed to support a particular function, such as human resource management, property management, or logistics management, and were not designed for financial statement reporting.

In addition, financial transactions are rarely completed using only one information technology system from the point of initiation to the point the transactions are reported on the financial statements. DoD Components do not own and operate all of the information technology systems that they use to process their transactions. To process and record contract payments, for example, the Military Services depend on over a dozen information technology systems that are owned and operated by other DoD Components. This complex interdependency between the DoD Components increases the difficulty of defining critical responsibilities for the information technology system owners and the reporting Components in the financial management processes.

For example, the Navy, U.S. Air Force, and Marine Corps rely on Army data from the munitions inventory management system to value its munition inventory and know how much munitions it has available. Establishing roles and responsibilities as presented in the Army's "Report on the Suitability of the Design of Controls in the United States Army's System Supporting the Delivery of Munitions Inventory Management

Services" should result in accurate inventory quantities reported to the Military Services for valuation and identification of it munitions.

In FY 2017, auditors issued 560 Notices of Findings and Recommendations related to the DoD's information technology systems. For example, auditors identified control weakness in the processes of sharing information between financially related systems (interfaces). Management also did not identify all of the interfaces for information technology systems and did not confirm that controls existed to ensure that data is shared completely and accurately between systems. Without these controls the integrity of the data cannot be relied on for financial reporting. Auditors also identified similar concerns during the FY 2018 audits.

With nearly 400 information technology systems in the DoD, it is essential that the DoD identifies all the information technology systems that share information, reduce the overall number of information technology systems being used throughout the DoD, and develop sufficient internal controls over the sharing of information among these systems.

Ineffective information technology system controls can result in significant risk to DoD operations and assets. For example, without effective internal controls on information technology systems, information, such as payments and collections, could be lost or stolen; computer resources could be used for unauthorized purposes; or critical operations, such as those supporting national defense and emergency services, could be disrupted. For example, without effective internal controls, the DoD's military operation systems could be penetrated, which would undermine military operations. In addition, establishing and reviewing user access to information technology systems and reviewing the roles of each user are key controls that help reduce risk to operations and assets. For example, during the FY 2018 financial statement audit, auditors determined that while personnel from the Defense Information Systems Agency performed periodic reviews of user access, they did not have a process to review and document modifications to users' access.

ACCOUNTING STANDARDS, GUIDANCE, AND PROCESS REQUIREMENTS

The DoD's inability to account for financial transactions and report associated financial data in accordance with Generally Accepted Accounting Principles for Federal Government entities is a longstanding impediment to receiving a clean or unmodified financial statement opinion. Generally Accepted Accounting Principles is a collection of commonly followed accounting rules and standards for financial reporting that ensure Federal entities track accounting transactions according to the same standards. The Federal Accounting Standards Advisory Board issues Federal financial accounting standards and provides guidance to Federal entities for financial accounting requirements.

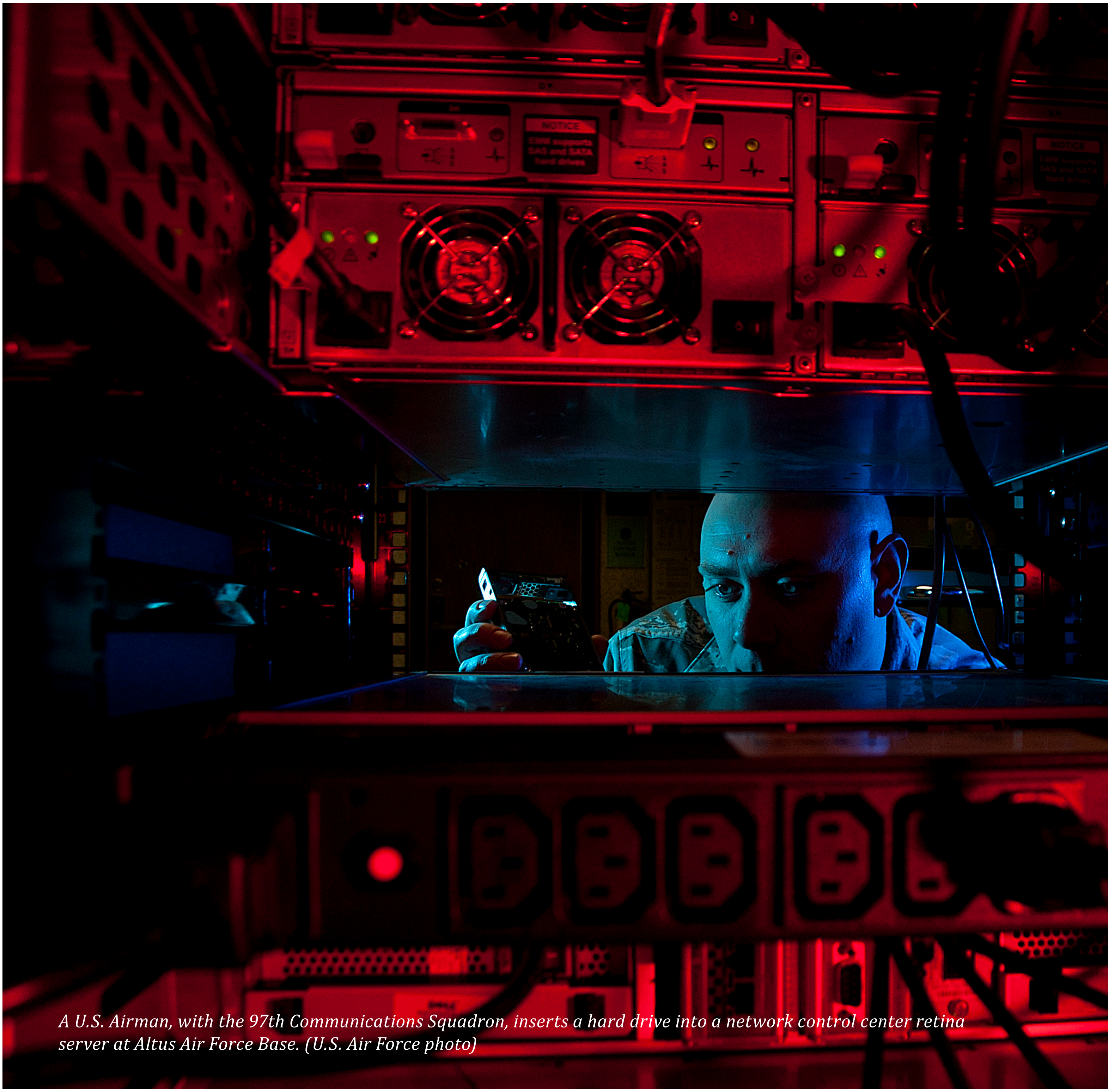
The DoD has determined that unique requirements and limitations, such as the reporting of classified information, continue to cause challenges to its compliance with Generally Accepted Accounting Principles. DoD Components that have classified or sensitive activities have encountered problems with reporting financial activity in unclassified financial statements. The DoD has requested the Federal Accounting Standards Advisory Board to consider alternative methods of accounting or presentation to assist in overcoming the challenges the DoD faces. For example, the DoD and the Federal Accounting Standards Advisory Board have coordinated to address the need to protect national security and ensure classified information is not released through financial statements.

The Federal Accounting Standards Advisory Board recognized the DoD's need to keep sensitive information from being released through financial statements and released Statement of Federal Financial Accounting Standards 56, “Classified Activities.” The Federal Accounting Standards Advisory Board is working to finalize and release its Interpretation of Federal Financial Accounting Standards 56, “Classified Activities.” This proposed Interpretation permits specific modifications to prevent the disclosure of classified information within unclassified Federal financial statements. The Standard 56 and its interpretation will affect not only the reporting and disclosure of the DoD financial statements but also the reporting of and disclosures related to classified information that are made by other Government entities and consolidated in the Government-Wide Financial Statements.

In addition, the DoD continues to face challenges in determining the historical value of its PP&E and developing a sustainable process to value new PP&E as it is purchased or constructed. For example, the Army could not provide sufficient documentation to support the historical cost of its PP&E. Army officials have stated that the PP&E valuation documentation was not readily available because controls had not been fully designed and implemented to maintain historic supporting documentation as it relates to past acquisitions of PP&E. To help address this type of issue, the DoD worked with the Federal Accounting Standards Advisory Board to develop an alternative method for establishing a baseline, or starting value of its PP&E at the time it was acquired. Although the DoD has established a formula that will be used by all DoD Components to value their PP&E, the Federal Accounting Standards Advisory Board has made clear that the alternative method for valuing assets is a one-time exception to the established standards.

As the DoD continues to identify challenges in complying with Generally Accepted Accounting Principles, the DoD will need to continue its coordination with the Federal Accounting Standards Advisory Board. As it works with the Board and implements the flexibilities provided, however, the DoD must also meet the challenge of ensuring that the standards are consistently and accurately implemented throughout the entire DoD.

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 continue to 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 budget provided to the DoD.



A U.S. Airman, with the 97th Communications Squadron, inserts a hard drive into a network control center retina server at Altus Air Force Base. (U.S. Air Force photo)

Challenge 5: Improving Cybersecurity and Cyber Capabilities

Cybersecurity is essential to the DoD's mission. The DoD must ensure adequate security when acquiring, deploying, operating, and maintaining information technology and DoD data residing on systems and networks across the DoD, including DoD data that resides on contractor systems and networks. At the same time, threats to DoD systems and networks continue to increase as systems and networks become more interconnected and malicious tools become more prevalent.

As discussed in this challenge, technology alone will not solve the cybersecurity and information technology challenges that the DoD faces. Adequately addressing this challenge requires safeguarding sensitive data and information systems, networks, and assets against cyber attacks and insider threats; modernizing and managing information technology systems; improving supply chain risk management practices; and recruiting and retaining a skilled cybersecurity workforce.

The scope of the challenge is constantly evolving. In the past few years, cyber threats have changed as nation-states (Russia, China, Iran, and North Korea) and non-nation-states (terrorists, criminals, hacktivists, and other malicious actors) use the Internet to exploit cyber vulnerabilities and to obtain unauthorized access to, and use of, sensitive and classified information. Since 2013, the Director of National Intelligence has identified cyber threats as the top strategic global threat facing the United States.

The DoD relies heavily on cyberspace and the DoD Information Network, which is composed of thousands of systems and networks worldwide, including DoD-owned and leased communications, software, security devices, data, and other associated services, to perform the full spectrum of the DoD's military, intelligence, and business operations. U.S. Cyber Command (USCYBERCOM) leads DoD cyberspace operations by planning, coordinating, synchronizing, and directing activities to conduct defensive and offensive cyberspace operations to support military operations in air, land, sea, space, and cyberspace. In May 2018, USCYBERCOM became the 10th combatant command. The Cyber Mission Force, which is staffed and equipped by the Military Services, is a specialized force within the DoD that conducts cyberspace operations to defend national interests and priority networks against specific threats, and that supports combatant command objectives.

The 2017 National Security Strategy states that cyberspace offers adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple U.S. businesses, weaken U.S. Government networks, and adversely affect technology that Americans rely on to communicate and conduct business, without ever having to physically cross U.S. borders. As billions of new devices are connected to the Internet—most with little built-in security—the United States, its allies, and international partners will face an increased risk of cyber attacks that threaten U.S. national security interests.[21]

In the face of these threats, in May 2018 the Office of Management and Budget reported that 71 of 96 Federal agencies (approximately 75 percent), including the DoD, had enterprise-wide gaps in monitoring network activity and lacked standardized cybersecurity tools and capabilities. The report concluded that the Federal agencies were not prepared to determine how cyber attackers accessed their data, and minimize the impacts of a cybersecurity incident if detected.[22]

The 2018 DoD Cyber Strategy identifies key objectives to help overcome these challenges, and preserve U.S. military advantages in cyberspace and defend U.S. interests against adversaries, particularly China and Russia that pose long-term strategic risks to the Nation and U.S. allies and partners. The DoD's cyberspace objectives include ensuring the Joint Force can achieve its missions in a contested cyberspace environment; defending U.S. critical infrastructure from malicious cyber activity; and securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned systems and networks.

The cybersecurity risks for the DoD now and in the future are continual critical challenges it must address. In short, a well-trained cybersecurity workforce; strong partnerships with U.S. allies, international partners, and the private sector; effective programs to monitor system and network activity and identify and promptly mitigate system and network vulnerabilities; and a robust risk-based strategy to modernize it information technology infrastructure are needed to address the cybersecurity and information technology challenges faced by the DoD.

PROTECTING DOD INFORMATION FROM INSIDER AND EXTERNAL THREATS

The emergence of increasingly sophisticated threats and the number of reported cyber incidents underscores the continuing and urgent need for strong cybersecurity controls and processes. In March 2018, the Defense Intelligence Agency Director testified that evolving and malicious cyberspace activities increasingly target DoD networks, systems, and information, including mobile devices, critical infrastructure, and U.S. military technology (intellectual property). Systems and networks used by Federal agencies, including by the DoD, are often riddled with security vulnerabilities, both known and unknown. For example, the DoD Chief Information Officer stated in July of 2018 that countless cyber incident reports show that the overwhelming majority of incidents could be prevented by implementing basic cyber hygiene and data safeguards. Cyber hygiene is general user, administrator, and leadership compliance with policies and standards necessary to protecting systems and networks against cyber threats. This fiscal year, the DoD OIG intends to examine whether the DoD is implementing effective cyber hygiene programs.

In the past few years, the DoD has undertaken several initiatives to defend its systems, networks, and data. For example, the DoD is implementing the Joint Regional Security Stacks to improve enterprise-based capabilities that secure and defend the DoD Information Network. The Joint Regional Security Stacks are a suite of equipment with network applications that provide data processing platforms and network capabilities, such as firewalls, intrusion detection and prevention, and enterprise risk management solutions.
The DoD OIG is assessing whether the DoD's

[21] Director of National Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community," February 13, 2018.

[22] Office of Management and Budget Report, "Federal Cybersecurity Risk Determination Report and Action Plan," May 2018.

implementation of the Joint Regional Security Stacks initiative is reducing the DoD's exposure to insider and external cybersecurity threats.

In addition, the DoD is exploring options to implement an automated patch management capability to distribute software and configuration patches and updates to mitigate known, major vulnerabilities on DoD systems and networks. The DoD is also increasing its use of "big data" and applying predictive and behavioral analytic tools to identify potential threats and other anomalies, detect actual threats, gather intelligence about cyber attacks, and execute DoD-wide responses before threats become significant or operational. Furthermore, the DoD has used "bug bounties programs" that offered cash rewards to independent hackers who found and disclosed software bugs in the DoD's systems and networks to mitigate hundreds of previously unknown vulnerabilities. These types of efforts seek to improve the DoD's defenses against cybersecurity threats, as well as improve its cybersecurity hygiene practices.

For the past decade, however, the DoD OIG and the General Accountability Office have both found problems in access control, configuration management, and agency-wide security management challenges affecting the DoD's ability to defend its systems and networks from cyber attacks and protect its sensitive and classified data. For example, in May 2018, the DoD OIG reported weaknesses in Navy, Air Force, and Defense Health Agency efforts to protect their networks and systems that process, store, and transmit patient health information.[23] In July 2018, the DoD OIG determined that Air Force squadrons did not remediate vulnerabilities identified during command cyber readiness inspections, identify system and network vulnerabilities, and take timely action to mitigate those vulnerabilities.[24]

To address the DoD's progress in protecting systems, networks, and data from cyber threats, the DoD OIG is now examining whether DoD Components are implementing effective security controls and processes at DoD facilities to protect Ballistic Missile Defense System technical information from insider and external cyber threats. The DoD OIG is also examining whether the combatant commands and Military Services are implementing controls to protect Air Force Space Command's Global Command and Control System-Joint data and information technology assets. This fiscal year, the DoD OIG intends to assess, among other issues, whether DoD Components are implementing cybersecurity controls to protect DoD information transmitted over wireless networks, and are securing cross-domain solutions to protect classified information and networks. The DoD OIG also plans to determine whether the Military Services are mitigating cybersecurity vulnerabilities in major acquisition programs identified during operational testing.

In addition to protecting data on DoD systems and networks, the DoD must also ensure that DoD data maintained on contractor networks are secure. Over the past few years, cyber attacks against DoD contractor systems and networks have increased. In February 2018, the Director of National Intelligence testified that most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or information technology and communications firms whose products and services support the U.S. Government. In May 2018, the Under Secretary of Defense directed the Defense Security Service to develop a risk-based approach to identify DoD controlled unclassified information with the potential to impact national security and oversee its protection through a collaborative effort with industry partners. Controlled unclassified information is information, such as technical data or personally identifiable information, that requires safeguarding or dissemination controls according to and consistent with applicable law, regulations, and Government-wide polices but is not classified. In June 2018, the Deputy Under Secretary of Defense

[23] Report No. DODIG-2018-109, "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities," May 2, 2018.

[24] Report No. DODIG-2018-137, "Command Cyber Readiness Inspections at Air Force Squadrons," July 11, 2018.

Cyber-warfare specialists serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard engage in weekend training. (U.S. Air Force photo)

for Intelligence stated that the DoD must begin including security as a major factor in considering whether to do business with certain contractors.

The importance of securing information on contractor systems was discussed in a March 2018 DoD OIG report that found weaknesses in the controls for protecting classified and unclassified Ballistic Missile Defense System technical information at seven Missile Defense Agency contractor facilities.[25] In addition, the DoD OIG is again assessing whether DoD contractors have security controls in place to protect the DoD controlled unclassified information maintained on contractor systems and networks from insider and external cyber threats.

The DoD must also be vigilant to risks posed by insiders. An insider is any person with authorized access to U.S. Government resources, including personnel, facilities, information, equipment, networks, and systems. This access can provide insiders a unique opportunity to damage the United States through espionage and unauthorized disclosures of national security information. In May 2016, the DoD began requiring contractors to establish and implement an insider threat program. In October 2016, the DoD also created the Defense Insider Threat Management and Analysis Center to analyze, monitor, and audit insider threat information derived from DoD insider threat programs. This fiscal year, the DoD OIG intends to assess whether the Defense Insider Threat Management and Analysis Center is providing an enterprise-level capability for integrating and managing insider threat information, and is safeguarding sensitive insider threat information.

Although the DoD has made progress defending against insider threats, more progress is needed. For example, in November 2017, despite efforts to limit insider risks, 100 gigabytes of data from an Army intelligence project maintained by the National Security Agency was uploaded to an unsecured web server. In addition, multiple data breaches by insiders have occurred at the National Security Agency. In a classified review completed in December 2017, the DoD OIG identified significant and immediate actions needed by the National Security Agency to secure its highest risk assets (top secret network and other segmented areas of the enterprise).[26]

To further assess the DoD's ability to manage insider threats, the DoD OIG is assessing whether combatant commands are implementing adequate processes and procedures to ensure the effectiveness of their insider threat programs. This fiscal year, the DoD OIG also intends to assess whether DoD Intelligence Community agencies are implementing security controls to manage classified enclaves and protect them from insider and external threats.

In July 2018, the DoD OIG published a Compendium of Open Recommendations that identified all open recommendations from prior reports. These open recommendations included approximately 200 recommendations, which if implemented, would improve the DoD's efforts to reduce its risks of insider threats and protect its systems, networks, and data.[27] For example, in response

[25] Report No. DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018.

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

[27] DoD OIG, "Compendium of Open Office of Inspector General Recommendations to the Department of Defense," July 30, 2018.

to a DoD OIG recommendation, USCYBERCOM has not yet developed a capability baseline and interoperability standards for all Cyber Protection Teams. In addition, the Missile Defense Agency has not taken action to hold contractors accountable for complying with the Federal standards for protecting controlled unclassified information on their systems and networks.

In short, 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. However, the DoD must prioritize the systems, networks, and data it needs to focus on protecting because of their impact on critical missions; consistently assess the risk of known vulnerabilities and take timely action to mitigate these risks; implement processes and programs to assess the sufficiency and effectiveness of contractor security; and improve the effectiveness of its cyber hygiene programs to ensure fundamental cybersecurity practices are followed. These are not easy or short-term actions, but they are critical to the DoD's ability to successfully meet mission requirements.

PROTECTING DOD CRITICAL INFRASTRUCTURE

The United States also depends on reliable and functioning critical infrastructure for many DoD activities and to support DoD operations. Critical infrastructure includes assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on national security, the economy, public health, or safety. Examples of critical infrastructure include power plants, dams, the election system, nuclear reactors, and communication networks. The growing interconnection of systems within U.S. critical infrastructure, as well as the increased complexity and connectivity of critical infrastructure systems and the significant increase of Internet-connected devices, creates a greater risk for cyber attacks that have direct physical consequences. Vulnerabilities affecting U.S. critical infrastructure can provide malicious actors the ability to disrupt military command and control, as well as the electrical grid, financial institutions, and almost every means of communication.

In February 2018, the Director of National Intelligence stated that the risk that adversaries will conduct cyber attacks, such as those related to deleting data or using malware to temporarily disrupt operations, against U.S. critical infrastructure is increasing. In July 2018, the Director stated that warning lights about cyber threats to U.S. national security were "blinking red" and cyber attacks to undermine the United States were occurring daily. For example, the Department of Homeland Security and the Federal Bureau of Investigation issued an alert in 2018 specific to Russian government cyber actors targeting small commercial facilities' networks and industrial control systems used to operate critical infrastructure.[28]

The DoD relies on a global network of critical infrastructure and the systems used to operate the assets that protect, support, and sustain its forces, and to conduct military operations worldwide. Protecting its critical infrastructure and ensuring mission availability of DoD systems and networks used to operate the infrastructure continues to be challenging. In June 2018, the DoD estimated that it could cost about $250 million over the next 4 years to identify and secure all systems and networks used to operate its critical infrastructure.

To examine the DoD's progress in protecting critical infrastructure from cyber attacks, the DoD OIG is assessing whether the DoD has programs to detect, report, and respond to security incidents affecting mission-critical industrial control systems. The DoD OIG is also examining whether the Air Force Space Command is implementing security controls

[28] United States Computer Emergency Readiness Team Alert TA18-074A, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," March 15, 2018.

to protect the Air Force Satellite Control Network against cyber attacks. This fiscal year, the DoD OIG intends to determine whether the DoD is planning and executing cyberspace operations in accordance with mutually agreed upon Department of Homeland Security requirements.

The National Security Strategy also states that the United States must work with critical infrastructure partners to assess information and security needs and reduce barriers to sharing information. The Cybersecurity Information Sharing Act requires Government and private sector entities to share cyber threat indicators and defensive measures. The DoD OIG is assessing whether DoD Components had sufficient policies and procedures, properly classified information, shared the information in a timely manner, protected personally identifiable information, and assessed barriers to sharing cyber threat indicators.

In short, the DoD is continuously challenged to protect and support other Government agencies in protecting critical infrastructure. To address these challenges, the DoD needs to fully identify physical and cybersecurity risks affecting each asset, identify all systems, networks, and data used to operate the assets, continuously assess security risks and promptly mitigate vulnerabilities, improve processes to share threats with other infrastructure owners faster, and adequately fund security improvements.

MODERNIZING INFORMATION TECHNOLOGY

Historically, Federal agencies have struggled with planning and budgeting to modernize outdated information technology systems, upgrade their underlying infrastructure, and invest in higher-quality, lower-cost services and technology, including cloud computing.

In 2014, the President signed the Federal Information Technology Acquisition Reform Act to improve how Federal agencies manage information technology, including chief information officer authorities, improved risk management in information technology investments, and data center consolidation. In December 2017, the Modernizing Government Technology Act was enacted to require Federal agencies to improve their technology by making additional resources and technical expertise available to, among other actions, improve, retire, or replace legacy systems, and transition data to the cloud. Cloud computing is an internet-based service that provides shared processing resources and data on demand.

However, the DoD OIG and the Government Accountability Office have repeatedly reported or testified about Federal agencies' failed efforts, including those of the DoD, to modernize their information technology infrastructure.[29] For example, the DoD has continuously had challenges with consolidating data centers; building the Joint Information Environment, which is a single enterprise architecture that supports the migration to cloud computing; delivering secure cloud services; replacing legacy systems; migrating to

[29] GAO-18-460T, "Further Implementation of Recommendations is Needed to Better Manage Acquisitions and Operations," March 14, 2018; GAO-17-686T, "Sustained Management Attention to the Implementation of FITARA Is Needed to Better Manage Acquisitions and Operations," June 13, 2017; GAO-16-468, "Federal Agencies Need to Address Aging Legacy Systems," May 2016; GAO-16-696T, "Federal Agencies Need to Address Aging Legacy Systems," May 25, 2016; GAO-18-142SP, ":Emerging Opportunities, Challenges, and Implications," March 2018; and GAO-18-644T, "Emerging Opportunities, Challenges, and Implications for Policy and Research," June 26, 2018.

supported operating systems; and strengthening cybersecurity governance, training, authentication, and risk management practices.

The 2018 President's Management Agenda outlines three priorities for modernizing information technology. The Management Agenda focuses on increasing the use of cloud-based solutions, leveraging current commercial capabilities to reduce cybersecurity risks, and building a modern information technology workforce who can drive modernization using up-to-date technology.

In July 2018, the DoD Chief Information Officer stated that the DoD would focus on four priorities—cloud migration, cybersecurity, artificial intelligence programs, and command, control, and communications systems—to support the National Defense Strategy and the DoD's information technology modernization efforts. Since developing its first cloud computing strategy in 2012, the DoD has been slow to transition to the cloud environment, primarily because of cybersecurity concerns. In September 2017, the Deputy Secretary of Defense approved a new initiative to expedite the DoD's transition to a commercial cloud infrastructure. This fiscal year, the DoD OIG intends to examine whether DoD Components have implemented security and privacy controls to protect DoD information hosted in the cloud.

The 2018 DoD National Defense Strategy also states that the DoD plans to invest broadly in advanced autonomous systems, including military applications of artificial intelligence, to gain military advantages. Artificial intelligence is generally defined as technology that emulates human performance by learning and developing conclusions through an understanding of complex content (exhibits humanlike characteristics and behaviors).[30] Artificial intelligence programs also provide the DoD opportunities to predict parts failures and improve operational mission outcomes, and they can also provide significant benefits in detecting threats and identifying and executing solutions to mitigate those threats in real time.

In September 2017, the DoD began developing a plan to manage its approximately 600 artificial intelligence initiatives. In June 2018, the Deputy Secretary of Defense established the Joint Artificial Intelligence Center to accelerate the delivery of artificial intelligence-enabled capabilities and synchronize DoD artificial intelligence efforts. The DoD OIG believes that a centralized office responsible for managing these types of projects and building on lessons learned is needed to maximize resource investments. This fiscal year, the DoD OIG intends to examine whether the DoD is implementing a strategy to resource, develop, and use artificial intelligence technology in current and future DoD programs, and cybersecurity and physical security controls are in place to protect the technology and data used in those programs.

In short, the DoD has taken steps to modernize its information technology infrastructure, but significant, long-term challenges remain. Modernizing the DoD's information technology infrastructure can result in increased mission effectiveness, stronger cybersecurity, lower information technology acquisition costs, faster capability delivery, and improved interoperability. Transforming the DoD's information technology systems and infrastructure into a modernized, flexible architecture will require significant resources and continuous coordination by DoD leaders across DoD-wide programs and operations. In addition, the DoD will need to collaborate with other Federal agencies, private industry, and academia to maintain modernized, effective information technology infrastructure.

[30] Researchers generally make two distinctions when describing artificial intelligence: narrow and general. Narrow refers to applications that provide domain-specific expertise or task completion, whereas general refers to an application that exhibits intelligence comparable to a human, or beyond, across the range of contexts in which humans interact.

IMPROVING SUPPLY CHAIN RISK MANAGEMENT PRACTICES

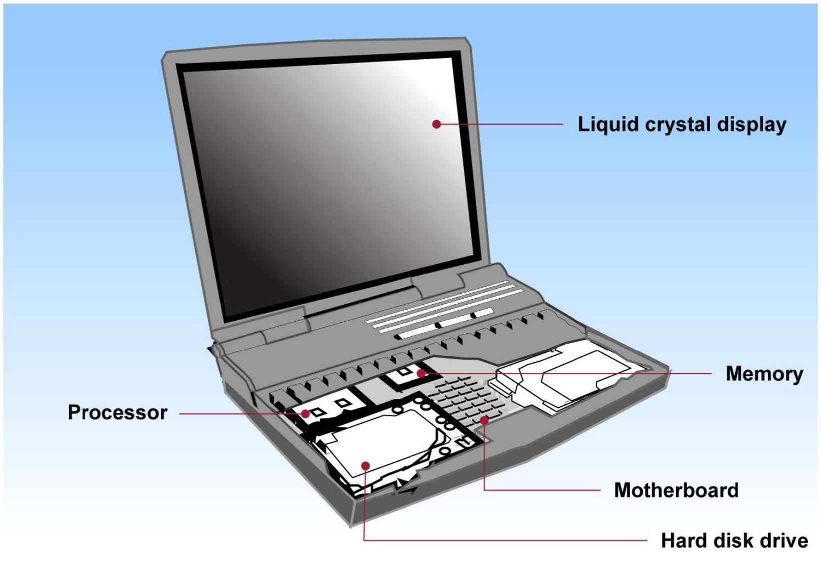
The design and development of nearly all weapon systems, information systems, and other products include hardware, firmware, and software. Each of the components in these systems can come from one or more supply chains. Today's complex and globally distributed supply chains affect the DoD's ability to ensure the integrity, security, resilience, and quality of products as it modernizes its information technology infrastructure and relies on the private sector, open source software, and commercial, off-the-shelf products to perform its missions.

Figure 1 illustrates an example of potential countries that commonly provide various components in building commercially available laptops.

Supply chain risks include acts by an adversary or insider to sabotage, maliciously introduce unwanted functions or malware, or otherwise change the design, integrity, and operation of a system to degrade its use or functionality. Cybersecurity risks in the supply chain are especially challenging when the DoD is developing and acquiring weapon systems or any system that relies on technology. However, ensuring DoD warfighting mission capabilities are not impaired by vulnerabilities introduced through the supply chain process by an insider or external adversary is essential to ensuring uncompromised weapons and information systems.

For example, in April 2018, the U.S. China Economic Security Review Commission reported a decades-long strategy by the Chinese government to compromise the U.S. supply chain. The DoD OIG is currently examining whether the DoD is

Figure 1. Commercially available laptop



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information. | GAO-18-667T assessing and mitigating cybersecurity risks when purchasing and using select commercial items. In a management alert arising from this audit, the DoD OIG identified cybersecurity vulnerabilities associated with using commercial, off-the-shelf unmanned aerial vehicles (drones), particularly those by a Chinese manufacturer. This alert prompted the Deputy Secretary of Defense to halt the purchase and use of all commercial, off-the-shelf drones until the DoD developed and fielded a solution to mitigate known cybersecurity risks.

The DoD OIG has regularly reported on supply chain risks, including information technology and cybersecurity risks, that the DoD faces.[31] For example, in August 2018, the DoD OIG reported that the Air Force Space Command did not fully implement DoD supply chain risk management policy throughout the Space-Based Infrared System's life cycle to ensure the design or integrity of critical hardware, software, and firmware is not compromised.[32] In addition, the DoD OIG is now examining whether the DoD's supply chain risk management program is mitigating cybersecurity risks for critical networks or systems that comprise the Nuclear Command and Control System.

In November 2017, the DoD Deputy Chief Information Officer testified that the DoD had implemented processes and procedures to mitigate supply chain risks. The Deputy Chief stated that the DoD established the Threat Analysis Center to provide supply chain threat assessments on critical components and the Joint Federated Assurance Center to share hardware and software testing capabilities. The DoD is also developing a criticality analysis process to identify mission capabilities, mission-critical functions, and system components.

The National Defense Authorization Act for FY 2018 requires the DoD to establish a process to improve the integration of supply chain risk management into the overall acquisition decision cycle. Some of those required improvements include developing product risk profiles based on integrated intelligence sources, continuously assessing software product risks, and removing prohibited products from DoD networks when risks cannot be mitigated.

While the DoD is taking steps to reduce its supply chain risks, more must be done to manage the risks associated with acquiring assets containing technology. The DoD needs to develop and consistently implement software assurance countermeasures across all acquisition programs and implement risk-based programs to evaluate commercially purchased items containing components that could introduce cybersecurity risks. To effectively manage risk, the DoD must identify vulnerabilities and threats throughout its supply chains and develop mitigation strategies to combat those risks. Further, the DoD needs to coordinate with other Federal agencies and the private sector to improve cybersecurity over products for which the DoD has limited to no direct control within the manufacturing process.

PLANNING AND CONDUCTING DEFENSIVE AND OFFENSIVE OPERATIONS

Defensive and offensive cyberspace operations, whether conducted individually or simultaneously, are critical to defending U.S. national interests and conducting missions directed by combatant commanders. Defensive cyberspace operations include activities to discover, detect, analyze, and mitigate threats against critical information technology assets to ensure mission success.

[31] GAO-18-667, "Supply Chain Risks Affecting Federal Agencies," July 12, 2018; GAO-17-768, "DoD Needs Complete Information on Single Sources of Supply to Proactively Manage the Risks," September 2017; GAO-17-688R, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations," July 27, 2017; Report No. DoDIG-2017-076, "The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System," April 27, 2017; Report No. DODIG-2016-082, "DoD Needs to Require Performance of Software Assurance Countermeasures During Major Weapon System Acquisitions," April 29, 2016; GAO-13-652T, "Addressing Potential Security Risks of Foreign-Manufactured Equipment," May 21, 2013; and GAO-12-361, "National Security-Related Agencies Need to Better Address Risks," March 2012.

[32] Report No. DODIG-2018-143, "Air Force Space Command Supply Chain Risk Management of Strategic Capabilities," August 14, 2018.

Offensive cyberspace operations, which are generally classified, include the use of cyberspace capabilities to achieve a specific effect in and through cyberspace.

The DoD continues to face challenges in developing or acquiring unique cyber capabilities to conduct cyberspace operations, obtain detailed intelligence of the cyberspace environment, incorporate cyberspace operations into command plans, use cyberspace capabilities similarly to other weapons to meet mission objectives, and strike a balance between the speed of conducting cyber operations and making operational decisions based on traditional warfare. For example, in July 2018, the House Armed Services Committee reported concerns about the Defense Intelligence Enterprise's ability to provide the cyber community with all-source intelligence support, consistent with the support provided to operations in other domains.

USCYBERCOM, the Military Services, and the Defense Information Systems Agency seek to identify, prioritize, and develop Service-specific and joint infrastructure and cyber capabilities. The DoD continues to build the Unified Platform, a joint cyber operations infrastructure platform that supports mission planning, data analytics, and other offensive and defensive operational needs, to enable the Cyber Mission Force to perform its full spectrum of cyberspace operations. In 2018, the Air Force became the executive agent to procure the platform. However, despite previous efforts to build the platform and the $30 million requested by the Air Force to continue developing the platform, it will not be operational for several years. In addition, USCYBERCOM, the Military Services, the National Security Agency, and the Defense Information Systems Agency continue to develop a wide variety of cyber capabilities to use when needed; however, according to the USCYBERCOM Commander, those tools must be refined for specific cyber actors and specific operating environments to be successful.

Since 2011, Secretary Mattis has issued three strategies for operating in cyberspace to guide the DoD's cyber activities and operations, which include accelerating the integration of cyber requirements into combatant command plans. Yet, developing the appropriate skillsets for planners who understand the cyber domain or cyber subject matter experts who have planning experience has been challenging. In March 2018, the DoD OIG determined that the U.S. European Command made limited progress in integrating offensive and defensive cyberspace operations into its command plans.[33] In early 2018, the DoD began staffing planning cells with cyber operators and planners to support combatant commanders' coordination and planning efforts.

In short, despite the DoD's efforts to effectively conduct defensive and offensive cyberspace operations, critical challenges remain in this area. The DoD needs to continue prioritizing which systems and networks it must defend to meet critical mission objectives, ensure appropriate and timely intelligence is available to inform strategic, operational, and tactical planning, and identify solutions to rapidly develop or acquire capabilities. Additionally, the DoD also needs to build and maintain strong international alliances and partnerships to deter shared threats.

INCREASING AND RETAINING THE DOD'S CYBER WORKFORCE

Despite Federal policies and strategies designed to increase the Federal cybersecurity workforce, the DoD and the U.S. Government continue to struggle in attracting and retaining a skilled cyber workforce. The DoD must compete with other Federal agencies and the private sector to recruit, develop, promote, and retain a skilled and diverse military and civilian cybersecurity workforce. The DoD cyber workforce includes personnel who build,

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

secure, operate, and defend DoD systems, networks, infrastructure, and data, and who conduct related intelligence activities and operations in or through cyberspace.

The DoD and other Federal agencies face unique challenges in building and retaining their cyber workforces. Pay gaps and a cumbersome hiring process that includes lengthy personnel security clearance investigations complicate the U.S. Government's ability to compete with the private sector.[34]

In 2017, the Government Accountability Office identified the shortage of cybersecurity professionals as a separate high-risk area. To help address these and other challenges, the Federal Cybersecurity Workforce Assessment Act of 2015 established the CyberCorps Scholarship for Service Program to focus on recruiting and training the next generation of information technology professionals. The Act also requires the Office of Personnel Management, the National Institute of Standards and Technology, and other Federal agencies to, among other actions, implement a coding structure for civilian cybersecurity positions and develop baseline assessments of existing agency cybersecurity workforces to use in filling staffing specific skillset gaps.

According to the DoD Chief Information Officer and USCYBERCOM Commander, the DoD is using cyber-excepted service authorizations to directly hire qualified applicants; developing cyber capability and capacity within the Reserve and National Guard; and expanding training capacity by developing a persistent cyber training environment.

The shortage of cybersecurity staff directly affects the DoD's ability to protect its systems, networks, and data from malicious cyber attacks. For example, the demand for DoD Red Teams, which are independent testing and assessment units that emulate threats and exploit vulnerabilities to identify security weaknesses in systems, networks, or facilities, has outpaced the DoD's ability to staff, train, and certify these teams. This fiscal year, the DoD OIG intends to examine whether DoD Red Teams and DoD Components have taken actions to correct problems identified in a 2013 DoD OIG report related to the composition and certification of Red Teams. The DoD OIG also intends to examine whether USCYBERCOM and the Military Services have corrected problems identified in DoD OIG reports from 2015 and 2016 related to organizing, staffing, training, and equipping the Cyber Mission Force.

Although the DoD continues to make gains in building the Cyber Mission Force and the entire DoD cybersecurity workforce, attracting and retaining a skilled cyber workforce remains a significant challenge. These challenges include fully staffing the Cyber Mission Force, ensuring existing and planned training capacity meets the DoD's needs now and in the future, leveraging unique strengths of the Reserve and National Guard and integrating them into the DoD's cybersecurity workforce, and expanding partnerships with other Federal agencies and the private sector.

In summary, while the DoD continues to take steps to improve security over its systems, networks, and data, significant challenges remain. The DoD needs to build and retain a skilled cyber workforce; modernize its information technology infrastructure; support contractors in hardening their cybersecurity defenses to protect sensitive and classified data and hold them accountable for security lapses that compromise national security; and evolve its tactics, techniques, and technologies to defend DoD systems, networks, infrastructure, and data from insider and external threats. It is also essential that the DoD improve user activity monitoring and other programs to reduce insider threat risks, integrate cyberspace operations into command plans, build and sustain international alliances and partnerships, and develop and use cyber capabilities to perform offensive and defensive operations.

[34] GAO-17-533T, "Federal Efforts Are Under Way That May Address Workforce Challenges," April 4, 2017.

U.S. Military Academy Class of 2018 cadets celebrate after receiving their diplomas during a graduation ceremony. (U.S. Army photo)

Challenge 6: Ensuring Ethical Conduct

Ensuring ethical conduct throughout the DoD is an enduring challenge for all DoD leaders, supervisors, and personnel. Ethical conduct helps promote public confidence in the DoD. By contrast, ethical failures, even by a few employees, can undermine trust in the DoD and foster an unwarranted perception that undermines the work and sacrifice of U.S. service members and civilians throughout the world.

Ethical leadership starts at the top of the DoD. Early in his tenure, Secretary Mattis emphasized the importance of ethical conduct, as well as the work of the DoD OIG and other oversight entities throughout the DoD in holding DoD personnel accountable for misconduct. For example, in an April 4, 2017, memorandum to all DoD employees, he stated that the essence of ethical conduct is "doing what is right at all times, regardless of the circumstances or whether anyone is watching."

In the past year, the Secretary has continued to issue messages emphasizing ethical values. For example, on September 13, 2018, in a memorandum to all DoD personnel, he communicated his expectation that all personnel be "ethics sentinels" and uphold the highest degree of honor, while always operating in the "ethical midfield." In addition, in the Secretary's memorandum dated March 26, 2018, "Be Peerless Stewards of Taxpayers' Dollars," he emphasized "sound judgement and managerial integrity" in executing the budget and "to establish a culture of performance where results and accountability matter on every expenditure."

Other DoD leaders have emphasized the Secretary's message in their own guidance on ethical behavior. For example, the Deputy Secretary of Defense addressed ethics in policies on engaging with industry, creating a lethal and disciplined force, and in emphasizing DoD's role as stewards of taxpayer dollars. In a message to DoD leadership, the Deputy Secretary of Defense stated that one key component of leadership in delivering high-performance results of U.S. tax dollars is "reinforcing ethical behavior across the full spectrum of our work, recognizing it is a foundation of our ability to make sound, informed decisions." He also wrote that members of the DoD must "cultivate an environment where we practice good judgment and respect ethical boundaries."

INSTILLING AN ETHICAL ETHOS WITHIN THE DEPARTMENT OF DEFENSE

As part of their missions, the DoD OIG and Military Service Inspectors General (IGs) seek to investigate allegations of misconduct thoroughly, fairly, and timely and to hold accountable those individuals who have committed misconduct, or if they have not committed misconduct, to clear them in a timely manner. In addition, the DoD OIG and Service IGs also have an important role in trying to prevent misconduct before it happens. The DoD OIG focuses on proactive education and training for senior officials about potential misconduct. For example, the DoD Inspector General speaks to new DoD Senior Executive Service employees at APEX, a joint orientation for new Executives within the DoD, as well as to more experienced Senior Executive Service leaders at the Vanguard course. The DoD Inspector General discusses the work of the DoD OIG, ethical issues DoD leaders may face, the types of actions that can get them in trouble, the need to avoid reprisal if there is a complaint against them, and other potential ethical issues. Similarly, the DoD Inspector General has begun speaking to new generals and admirals about these topics at the CAPSTONE course, a Joint Service course for newly selected brigadier generals and rear admirals. These sessions seek to help prevent senior officials from crossing ethical lines inadvertently or willingly.

The DoD OIG also operates a well-publicized DoD Hotline that allows anyone to confidentially report allegations of misconduct. The DoD Hotline receives allegations related to misconduct; reprisal; other matters involving fraud, waste, and abuse; or issues related to national security involving DoD programs and operations. The DoD Hotline advertises on radio, television, Twitter, outreach events, and posters displayed at DoD facilities worldwide, as well as at Defense Contractor workplaces. The DoD Hotline receives approximately 13,000 contacts every year. Some of those involve frivolous complaints or issues having nothing to do with the DoD, and some are passed on to the appropriate agency. However, the DoD Hotline receives many serious and credible allegations involving DoD operations. The DoD Hotline both opens and closes approximately 6,000 cases annually. The Service IGs also operate hotlines for service members and employees to report misconduct or to obtain assistance in matters within their Service.

In a recent initiative, in July 2018 the DoD OIG announced the selection of a new, full-time DoD Whistleblower Protection Coordinator. The Coordinator, who was previously known as the Whistleblower Protection Ombudsman, seeks to ensure that DoD employees—uniformed military personnel, DoD civilians, as well as Federal contractors and subcontractors—understand the rights of whistleblowers and the responsibility not to retaliate against them. The Whistleblower Protection Coordinator is also responsible for educating agency employees about how they can seek review of allegations of reprisal, and the roles of the DoD OIG, the Office of Special Counsel, the Merit Systems Protection Board, and other relevant entities in this process.

Additionally, the DoD OIG conducts targeted outreach to educate DoD employees about the prevention and investigation of sexual assault. In recent years, military sexual assault investigations and allegations of reprisal for reporting allegations of sexual assault have increased. The DoD OIG has conducted outreach and education on these issues. For example, DoD OIG representatives have briefed the National Guard Bureau, Special Victims Counsels, and the National Organization for Victims Assistance at their annual conferences, covering issues such as the DoD OIG complaint, investigative and reporting processes, to assist victims and their representatives to understand what to expect after filing a sexual assault related reprisal complaint.

Pass and Review at the United States Military Academy West Point.

In addition, DCIS conducts fraud awareness briefings for Government and contractor procurement officials, legal counsels, agency heads, auditors, law enforcement officials, and other individuals in key management positions. These briefings emphasize management's responsibilities to promptly report criminal activity within the DoD and provide information on how to recognize illegal activity involving procurement fraud, public corruption, and bribery and how to report such activities to the appropriate authorities. In FY 2018, DCIS personnel briefed over 15,000 officials on these issues.

Other oversight entities in the DoD pursue similar education and training initiatives on ethics. For example, the Army IG promotes training, called the "DAIG Senior Official Front Office Exportable Training Package," to help Army personnel avoid potential ethical pitfalls or actions that lead to allegations of impropriety. The training package uses vignettes derived from real investigations. The Air Force IG, in addition to the educational briefings, has begun publishing brief case studies of misconduct allegations against Air Force senior officials. Separately, the Air Force IG trains Air Force leaders, including Air Force group and wing commanders courses and the Air Force Senior Leader Orientation Course, on ethical pitfalls and trends in misconduct. Similarly, the Naval IG speaks to newly promoted flag officers and captains yearly to provide them with examples of unethical behavior from recent Navy cases.

The Marine Corps IG published a campaign plan in 2017, which includes providing additional ethics-related instruction at professional military education schools for all grades within the Marine Corps. This instruction focuses on ethical standards and the importance of compliance with those standards. The Marine Corps IG also uses mobile training teams to update command IGs and legal staffs on IG matters.

The Joint Staff IG participates in Joint Staff assistance visits, with teams of subject matter experts, at all combatant commands to review a variety of ethical issues. The staff assistance visits are designed to help commanders identify and avoid ethical pitfalls related to the acceptance of gifts, misuse of subordinates, use of official representation funds, and official travel. The Joint Staff Assistance Visits team also conducts ethics roundtable discussions with support staff who provide direct support to all senior leaders in the command. The discussion provides information about their roles in ensuring ethical conduct within the command and highlights recent case examples of ethical misconduct. The team shares best practices with each combatant command, including the development of a tailored ethics handbook for support staff, an automated log to track incoming and out-going gifts, ethical checklists, and standard operating procedures designed to help command personnel identify and avoid ethical pitfalls.

The Defense Contract Audit Agency has created a series of ethics podcasts for employees to use for annual ethics training. Other agencies have developed a "Jeopardy"-style ethics training that allows employees to learn ethics in an entertaining and interactive manner. The Defense POW/MIA Accounting Agency sends monthly scenarios to all employees that depict common ethical dilemmas and provides detailed responses.

The Naval War College has established the Naval Leadership and Ethics Center, which seeks to prepare commanders and their support teams to avoid ethical lapses. The goal of the Naval

Leadership and Ethics Center is to groom ethical and responsible command leaders through interactive coursework, cases studies, personal coaching, and other training exercises.

The Commander of the U.S. Special Operations Command hosts a guest speaker series that invites speakers to discuss values and ethics. He also hosted an offsite senior leader round table that emphasized values, ethics, and professionalism.

The Defense Finance Accounting Service meets individually with all senior executives to offer them the chance to discuss any ethics questions they may have. It also provides them tools to promote and model the ethical culture within their own organizations. The Defense Logistics Agency uses a "Leader-Led, Values-Based" ethics training where commanders train the troops.

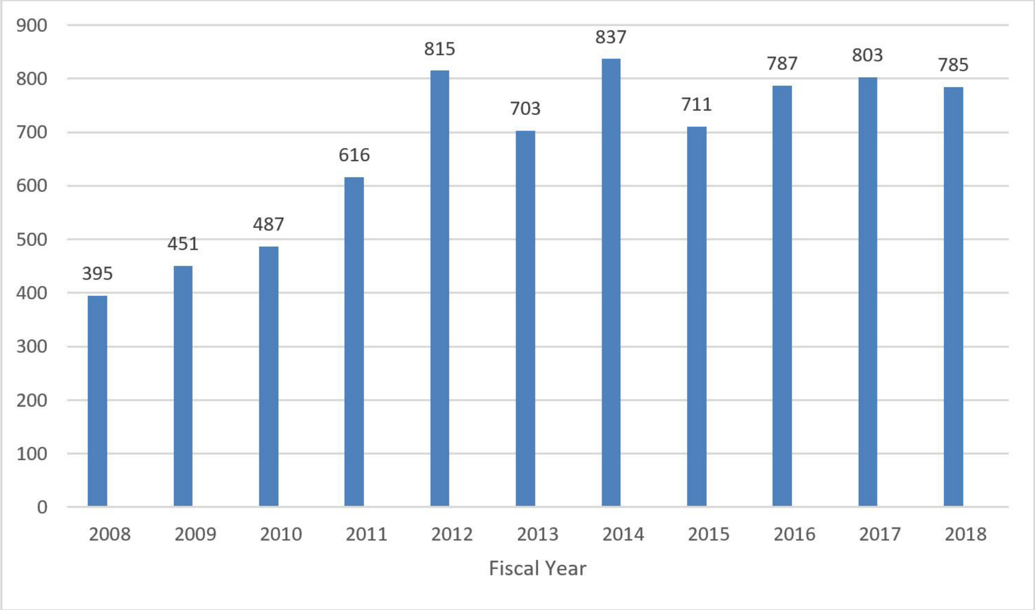
TRENDS IN ETHICAL MISCONDUCT

SENIOR OFFICIAL MISCONDUCT INVESTIGATIONS

While these initiatives can help educate DoD personnel, ethical lapses will occur in any large organization, including the DoD.

The following two tables show the trends in DoD senior official misconduct cases. As reflected in Figure 2, the number of complaints alleging misconduct by senior DoD officials increased significantly from FY 2008 to FY 2012. Specifically, the number of complaints of senior official misconduct complaints rose from 395 in FY 2008 to 815 in FY 2012, and has remained relatively steady since then.

Figure 2. Misconduct Complaints Against Senior Officials



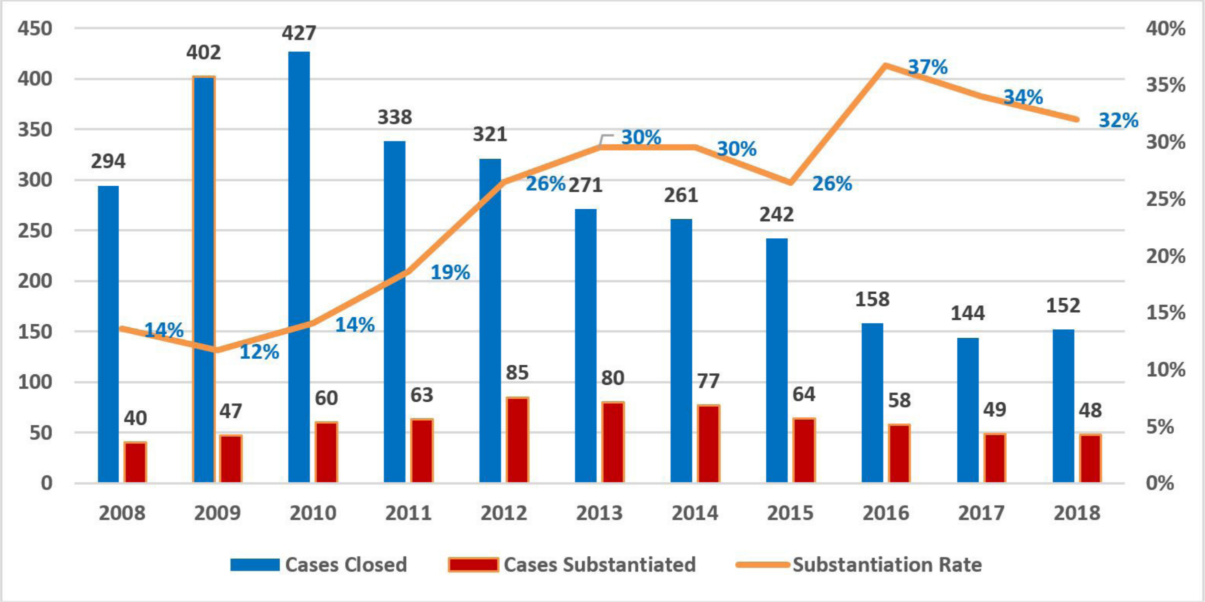
Note: The totals include complaints received by the DoD OIG and those reported by the Service and Component IGs to the DoD OIG.

Source: The DoD OIG.

However, as reflected in Figure 3, during the same period, the number of these complaints warranting investigation decreased, while the overall substantiation rate of the cases investigated has increased. The DoD OIG believes that the decline in the numbers of full investigations conducted and the increase in the substantiation rates is attributable to the implementation of a more thorough complaint intake process that is designed to quickly address complaints that do not warrant investigation.

Overall, in recent years, the number of substantiated cases of misconduct by senior DoD officials has decreased. Specifically, the number of full investigations conducted by the DoD OIG and Service and Component IGs has steadily declined since FY 2010, from 427 in FY 2010 to 152 in FY 2018. Meanwhile, the substantiation rate of investigations conducted has increased from 14 percent in FY 2010 to 32 percent in FY 2018.

Figure 3. Number of Senior Official Misconduct Cases Closed, Substantiated, and Substantiation Rates



Note: Cases closed include closed investigations across the DoD.

Source: The DoD OIG Semiannual Reports to the Congress from FYs 2008 through 2012.

The number of senior official cases with any findings of substantiated misconduct rose from 40 in FY 2008 to its peak of 85 in FY 2012, but has steadily declined since then. For FY 2018, the overall number of substantiated cases totaled 48, continuing the overall downward trend that started in FY 2013.

When assessing trends in ethical conduct within the DoD, it is important to recognize that the vast majority of DoD senior officials and personnel perform their challenging jobs with dedication and integrity. Despite some well-known instances of misconduct, only a very small fraction of senior officials commit misconduct. By virtue of their positions, however, at some point in their careers, they may be accused of misconduct. Most of these allegations are not substantiated. In fact, only a small percentage of these officials fail to uphold the high ideals and ethics required of their critical positions. To place misconduct trends in context, in FY 2017, the number of DoD senior officials—general and flag officers and Senior Executive Service members—totaled 2,327 (963 general and flag officers and 1,364 Senior Executive Service members). In FY 2017, there were 49 cases of substantiated misconduct, which therefore involved only approximately 2 percent of the DoD senior official population. However, any misconduct by a senior official is unacceptable. The following are examples of a recently substantiated allegation of ethical lapses by senior officials within the DoD.

- An Army major general engaged in inappropriate online conversations with an enlisted soldier's spouse using flirtatious language and sexual innuendo.
- A Marine Corps brigadier general misused his aide when he requested or permitted his aide to perform tasks or errands that had no connection to official Government business, and solicited and accepted gifts from marines who received less pay than himself.
- An Air Force Senior Executive Service member used his public office for private gain by arranging temporary duty travel to New Mexico for his personal benefit.
- A former Air Force Audit Agency Senior Executive Service member used Government funds on official travel for primarily personal reasons by directing and authorizing a needless travel to Europe and the Middle East.
- A former U.S. Army Senior Executive Service member failed to fulfill her leadership responsibilities by calling subordinates by other than their professional name, using racial slurs, and making disparaging and inappropriate comments. The member also misused a civilian subordinate for other than official purposes when she frequently directed that employee to fax her animal insurance claim forms.
- A Navy rear admiral wrongfully disclosed protected personal information to non-Government personnel.

Other substantiated senior official misconduct cases investigated by the DoD OIG and the Service and Defense agency IGs include inappropriate conduct toward subordinates, such as unwelcomed and intentional touching, profanity, sexual jokes, and disparaging and inappropriate comments about weight and appearance.

IGs across the DoD strive to conduct senior official investigations in a timely manner, which is a challenge. From FY 2013 through FY 2017, the average days to complete senior official investigations generally went up.

Several factors affected the timeliness of investigations. One factor is the increased complexity of the matters under investigation, including the increasing amount of digital and electronic evidence that needs to be reviewed. Another factor is the increased scrutiny these cases receive, which leads to greater thoroughness and lengthier reports. At the same time, IGs within the DoD have had relatively static or decreasing resources to assign to conduct senior official investigations, which impacts timeliness.

The efforts DoD investigators take to ensure due process for the subjects also impact timeliness of investigations. For example, to enhance thoroughness as well as fairness, the DoD OIG gives the subjects of substantiated investigations an opportunity to comment on their tentative conclusions before the final report is completed. This allows the subject to provide the investigators any additional information the subject believes is relevant, and to correct any inaccuracies in the report before it is completed.

Yet, having noted all these factors that affect timeliness, the DoD OIG and the Service and Component IGs recognize that these investigative timelines are too long. Timeliness of investigations can affect morale and readiness, and the pendency of an investigation can prevent senior military officers from being promoted or retiring. The DoD OIG believes that if senior officials commit misconduct, they should be held accountable in a timely manner; if they did not commit misconduct, they should be cleared in a timely manner. The DoD OIG and the Service and Component IGs are therefore seeking ways to improve timeliness, including streamlining and standardizing investigative processes across the DoD. These efforts are having an impact. For example, the average days in investigation for DoD OIG senior official investigations fell 45 percent from 455 days in FY 2017 to 250 days in FY 2018.

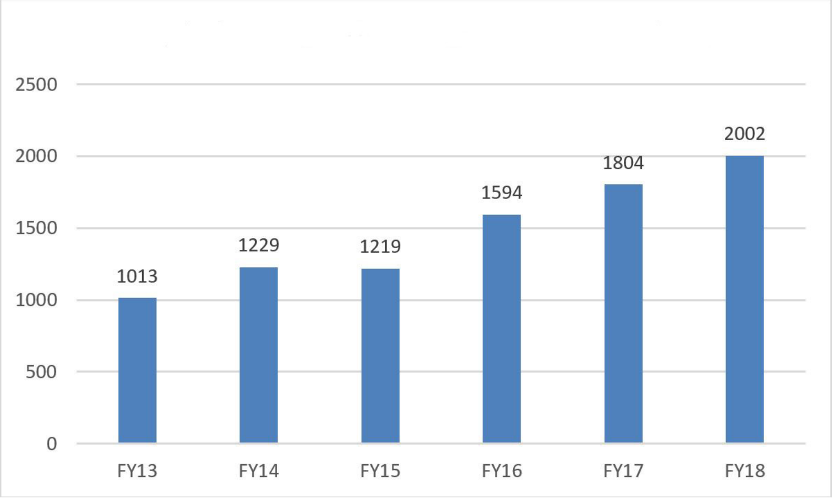
Mr. Glenn Fine testifies before the House Armed Services Committee on April 18, 2018.

WHISTLEBLOWER REPRISAL INVESTIGATIONS

In a trend similar to senior official misconduct complaints, the number of whistleblower reprisal complaints for both the DoD OIG and the Service IGs has also increased significantly. The following two tables show the trends in DoD whistleblower reprisal investigations. As reflected in Figure 4, between FY 2013 and FY 2018, reprisal complaints received across all applicable statutes grew from 1,013 to 2,002, (an increase of 98 percent).

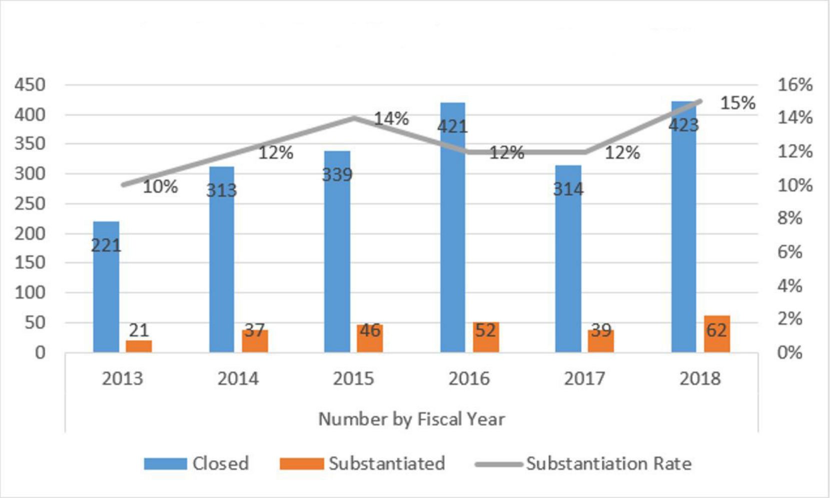
As the number of allegations increased, the number of substantiated allegations has risen slightly over time. As shown in Figure 5, the number of substantiated reprisal and restriction complaints during the period from FY 2013 through FY 2018 generally increased as the number of complaints increased. The substantiated rates did, however, remain consistent with the historic range of 10 to 15 percent for the DoD as a whole. The substantiation rate in any given year is not predictable because each investigation is a fact-dependent inquiry; the results are driven by the available evidence.

Figure 4. Number of Reprisal and Restriction Complaints Received



Source: The DoD OIG.

Figure 5. Number of Reprisal and Restriction Investigations Closed, Substantiated, and Substantiation Rate



Source: The DoD OIG.

The following are examples of recently substantiated allegations of reprisal and restriction within the DoD.

- Two Air Force captains co-wrote and issued a letter of counseling to an Air Force technical sergeant in reprisal for an e-mail the sergeant sent to his chain of command regarding evidence of gross mismanagement in a medical clinic.
- An Army National Guard major threatened an Army National Guard sergeant with nonjudicial punishment (Article 15, Uniform Code of Military Justice), directed the sergeant to undergo a mental health evaluation, removed the sergeant from the promotion list, and issued the sergeant an unfavorable non-commissioned officer evaluation report in reprisal for reporting the major for ethical violations.
- An Air National Guard colonel recommended that an Air National Guard major not be retained in reprisal for the major's participation in an official audit.
- An Army colonel reassigned and issued an unfavorable officer evaluation report to an Army major in reprisal for the major's reports of ethics violations and unfair treatment of civilian employees to the chain of command.
- A Defense Intelligence Agency division chief and a branch chief recommended that an intelligence officer be terminated during the officer's probationary period in reprisal for the officer reporting that the branch chief was not working an 8-hour workday and for criticizing the division and branch chief's leadership.
- After an investigation did not substantiate allegations of discrimination against a Navy lieutenant commander, the lieutenant commander made comments intended to restrict subordinates from making equal opportunity complaints. The lieutenant commander warned subordinates of potential consequences for making complaints and that future complaints should be handled within the chain of command. The lieutenant commander also threatened subordinates that they would have to "answer for their accusations" if they filed complaints that were determined to be without merit.
- A Navy commander relieved a lieutenant of duties as division officer in reprisal for the lieutenant stating the intent to meet with an inspector general to discuss various concerns about actions and decisions of superior officers in the chain of command.

The DoD OIG and the Service IGs continue to implement initiatives to improve the quality and timeliness of whistleblower reprisal investigations. For example, the DoD OIG recently hired additional staff to reduce the caseload per investigator. With this more manageable distribution of cases, the DoD OIG has been able to focus on completing the oldest investigations while more efficiently completing investigations of newer complaints. However, the Service IGs, which investigate the vast majority of military reprisal and restriction complaints, with oversight by the DoD OIG, have not received a commensurate increase in resources, which affects the timeliness of their investigations.

Another initiative the DoD OIG has recently implemented to help improve timeliness in reprisal investigations is an alternative dispute resolution program similar to the program used by the Office of Special Counsel. Alternative dispute resolution is a voluntary process in which parties use mediation or facilitated settlement negotiations to seek resolution of a complaint before an otherwise lengthy investigative process. Voluntary resolutions through alternative dispute resolution can help reduce the time for resolving cases, and alternative dispute resolution can also allow limited investigative resources to be allocated to completing other investigations in a timely manner. Instead of waiting for remedial action to be

A U.S. Airman with 733rd Logistics Readiness Squadron material control specialist, reads a poem during the Sexual Assault Theater Group performance of "Same Script, Different Cast."
(U.S. Air Force photo)

taken in response to recommendations made in a report of investigation, complainants are made whole quickly when agreement can be reached by both parties. The DoD OIG's program, which began in September 2017, has already shown positive effects. In 1 year, alternative dispute resolution resolved 46 complaints voluntarily, avoiding lengthy investigations.

In August 2018, the DoD OIG initiated a DoD working group to consider and propose process and policy changes to further enhance the efficiency and effectiveness of whistleblower reprisal investigations.

SEXUAL ASSAULT PREVENTION AND RESPONSE INVESTIGATIONS

The DoD is also faced with the challenge of reducing sexual assault. According to the 2017 DoD Sexual Assault and Prevention Office Annual Report, published on April 27, 2018, the annual rates of sexual assault decreased to the lowest levels since the DoD began measuring sexual assaults in 2006. The DoD also determined that a higher percentage of victims reported allegations of sexual assault. According to this report, 1 in 3 service members reported experiencing a sexual assault in 2016, a significant change from the 1 in 14 service members making a report in 2006.

Although sexual assault remains an underreported crime, the higher proportion of reporting is an indicator that victims are gaining more confidence in the sexual assault prevention and response and military justice systems, especially when increased reporting is paired with decreased sexual assault prevalence. Since FY 2012, according to the DoD Sexual Assault and Prevention Office Annual Report, sexual assault reporting has increased by over 88 percent within the DoD, while prevalence has decreased by nearly 45 percent for the same period.

However, sexual assaults in the military need to be fully investigated and addressed. In 2017, the DoD had sufficient evidence to take disciplinary action in 62 percent of its cases involving accused service members.

CRIMINAL PUBLIC CORRUPTION INVESTIGATIONS

Public corruption cases involve criminal misconduct; and the matters investigated often threaten national security; compromise the safety and security of DoD operations, systems, and personnel; waste tax dollars; and undermine the mission of the DoD.

In FY 2018, public corruption investigations by the Defense Criminal Investigative Service (DCIS) resulted in 32 criminal charges and 20 convictions. These investigations resulted in over $25.4 million in recoveries for the Government and the debarment of 29 entities from Government contracting. Recent public corruption cases investigated by DCIS and other military criminal investigative organizations include stealing Government funds or equipment and accepting bribes.

For example, investigators determined that an Army civilian employee stole donations dedicated to assisting wounded warriors, and used them for personal affairs, including gambling. Investigators determined that a Navy civilian employee accepted more than $250,000 in cash bribes while preparing and processing retail transactions at a Navy Exchange warehouse. In another recent case, an Army civilian employee engaged in a theft of more than $4 million of Government property, including more than $1 million worth of military-grade optics or rifle scopes.

As reported in last year's management challenge report, a troubling example of public corruption in DoD programs involves an ongoing case relating to Glenn Defense Marine Asia PTE, LTD, a defense contracting firm based in Singapore that provided ship maintenance and supply services to U.S. Navy ships throughout the Pacific. Leonard Glenn Francis, a Malaysian national, was the former President and Chief Executive Officer of Glenn Defense Marine Asia. A joint DCIS/Naval Criminal Investigative Service investigation determined that Francis conspired with former and current U.S. Navy officials to commit bribery and to defraud the U.S. Government. The scheme involved the fraudulent billing of goods and services Glenn Defense Marine Asia provided to Navy ships at various Asian seaports, including fuel, tugboat services, and sewage disposal. In exchange for things of value, such as dinners, hotel stays, travel, and prostitutes, Navy officers overlooked excessive bills and provided Glenn Defense Marine Asia employees with classified U.S. Navy ship schedules, contract data, and offered preference and assistance in Navy contracting decisions. Additionally, a corrupt U.S. Federal agent provided access and insights into criminal investigations involving Glenn Defense Marine Asia.

As of October 2018, 33 individuals have been criminally charged in connection with this case. Of those 33 individuals, 22 have pleaded guilty, including one Navy flag officer, a former member of the DoD Senior Executive Service, four Navy captains, several other Navy officers and enlisted personnel, a supervisory Naval Criminal Investigative Service Special Agent, Mr. Francis, three former Glenn Defense Marine Asia employees, and the Glenn Defense Marine Asia corporate entity. Sentences ranging from 18 months to 12 years have been imposed on 14 individuals.

In addition, as a result of the active duty military personnel potentially involved in either criminal or unethical behavior involving Glenn Defense Marine Asia, the Secretary of the Navy established a Consolidated Disposition Authority, headed by a four-star admiral, to review Glenn Defense Marine Asia investigations forwarded by the Department of Justice to the U.S. Navy for evaluation under the Uniform Code of Military Justice. Dispositions by the Consolidated Disposition Authority may range from no action to various forms of disciplinary measures, including court martial.

In summary, substantiated cases of misconduct by senior officials have declined in recent years. However, to sustain that downward trend, the DoD must continue to emphasize the need for ethical behavior. In reinforcing ethical decision making, the DoD OIG, Component IGs, ethics officials, and senior leaders need to continually emphasize the Defense Secretary's goal for senior leaders to stay in the ethical midfield and to make ethical conduct a foundation for their actions.

A U.S. Sailor writes down training notes during an anti-submarine exercise aboard the guided missile destroyer USS Stockdale during an exercise in the Pacific Ocean. (U.S. Navy photo)

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

The 2018 National Defense Strategy acknowledges that current and potential adversaries are moving aggressively to field forces that can challenge the United States' space-based capabilities from the ground, from space, and in cyberspace. From widely available and affordable jammers to highly sophisticated anti-satellite weapons, the United States is facing serious threats in these domains. The National Defense Strategy warns that the U.S. ability to deter aggression will be challenged if sufficient action is not taken to counter these threats.

For example, the threats posed by U.S. adversaries' ballistic missile delivery systems are likely to continue to increase and grow more complex. The Defense Intelligence Ballistic Missile Analysis Committee reported in 2017 that there has been a significant increase in worldwide ballistic missile testing over the last decade. Adversary ballistic missile systems are becoming more mobile, survivable, reliable, and accurate while also achieving longer ranges. Hypersonic glide vehicles delivered by ballistic missile boosters are an emerging threat that will pose new challenges to the DoD's missile defense systems.

In addition, at a time when other nations continue to modernize and upgrade their nuclear forces, nearly all elements of the U.S. nuclear weapon stockpile, delivery systems, and other critical infrastructure are operating well beyond their designed service life. The DoD is faced with the challenge of simultaneously sustaining legacy space and nuclear systems while modernizing and replacing these systems to meet future threats.

The DoD's backlog of deferred readiness, procurement, and modernization requirements has grown in the last decade and a half. To address the scope and pace of adversary ambitions and capabilities, the DoD is investing in modernization of key capabilities in space-based operations, missile detection and response, and nuclear deterrence.[35] However, space-based operations, missile defense, and nuclear deterrence remain a significant and existential challenge.

[35] National Air and Space Intelligence Center and Defense Intelligence Ballistic Missile Analysis Committee, "Ballistic and Cruise Missile Defense Review Report," June 30, 2017.

REEMERGENCE OF GREAT POWER COMPETITION

Senior DoD officials testified to the House Armed Services Committee's strategic forces subcommittee in 2018 that the nation's nuclear deterrence enterprise remains as important as ever in light of the return of superpower competition and the instability created by rogue nation threats. While the United States has reduced the number of its nuclear weapons, other nations, including Russia and China, have moved in the opposite direction. They and other nations, including North Korea, have added new types of nuclear capabilities to their arsenals, increased the importance of nuclear forces in their strategies and plans, and engaged in increasingly aggressive behavior, including in outer space and cyberspace. For example, China, Russia, Iran, and North Korea have been implicated in several cyber attacks against U.S. space assets.

The National Defense Strategy acknowledges that the DoD's competitive military advantage is being challenged and that modernization is needed to provide the capabilities and agility required to prevail in conflict. To address these challenges, the DoD recently implemented strategies and defense objectives to ensure the DoD's ability to sustain and modernize space-based operations, missile detection and response, and nuclear deterrence.

SPACE BASED OPERATIONS

According to the 2018 National Defense Strategy, the DoD has taken steps to implement initiatives to ensure the DoD's ability to sustain and modernize space-based operations, such as prioritizing investments in resilience, reconstitution, and operations to assure U.S. space capabilities. However, the DoD is challenged with the difficult task of simultaneously sustaining systems that are decades past their end of life-design and fielding replacement systems to meet current and future threats.

The Secretary of Defense stressed in the 2017 National Defense Strategy and the 2018 Nuclear Posture Review that every domain is now contested—including space. In May 2017, the

An Atlas V rocket carrying a Space Based Infrared System Geosynchronous Earth Orbit satellite for an Air Force mission lifts off from Cape Canaveral Air Force Station, Florida, January 19, 2018. (United Launch Alliance photo)

A U.S. Air Force B-2 Spirit Bomber and two F-15 Strike Eagle aircraft at RAF Fairford, England. (Air Force photo)

Director of National Intelligence testified that Russia and China perceive a need to offset any U.S. military advantage derived from military, civil, or commercial space systems and are increasingly considering attacks against satellite systems as part of their future warfare doctrine. The Director said that both countries will continue to pursue a full range of anti-satellite weapons as a means to reduce U.S. military effectiveness.

To address this challenge, the National Defense Authorization Act for FY 2019 establishes the U.S. Space Command, a subordinate unified command under U.S. Strategic Command. The mission of the unified command is to centralize joint space warfighting operations.

Additionally, the Secretary Mattis outlined in the Nuclear Posture Review initiatives intended to ensure space-based assets (specifically the nuclear command, control, and communications system) remain survivable and effective. These initiatives include strengthening protection against cyber threats, strengthening protection against space-based threats, enhancing integrated tactical warning and attack assessment, improving command post and communication links, advancing decision support technology, integrating planning and operations, and reforming governance of the overall nuclear command, control, and communications system.

The 2018 Nuclear Posture Review also emphasizes that the nuclear command, control, and communications system, while once state-of-the-art, is now subject to challenges from both aging system components and new, growing 21st century threats. Of particular concern are expanding threats in space and cyber space. Among other things, space-based assets perform the crucial functions of detecting adversary missile launches or nuclear detonations, warning to key decision makers, and characterizing the type of attack.

DETECTION AND WARNING

During the late 1970s, as the accuracy of the Soviet nuclear arsenal improved, Space Command planners identified the need for missile warning systems that could survive a nuclear attack. The first of these was the Integrated Tactical Warning and Attack Assessment's Mobile Ground System, designed to provide survivable missile launch detection, attack assessment, and warning to North American Aerospace Defense Command in the event of war. However, these systems are still in use today, approximately 23 years past the end of life-design. In 2013, the Air Force reported that sustaining the Mobile Ground System was becoming increasingly difficult because of the age of the equipment and the lack of replacement parts. Additionally, the Air Force has been challenged in balancing the requirement to sustain the Mobile Ground System while simultaneously designing and manufacturing the new replacement system.

In 2015, the DoD OIG evaluated the sustainment risks associated with the Mobile Ground System, along with the acquisition risks to the Mobile Ground System replacement system. The DoD OIG reported that the Air Force lacked adequate plans to sustain the Mobile Ground System and to field the new replacement system. In response, the Air Force developed an integrated plan to reduce the risk in sustainment and modernization efforts.[36] The DoD OIG intends to conduct a followup review to measure and report the DoD's progress in

[36] Report No. DODIG-2015-133, "Evaluation of the Integrated Tactical Warning and Attack Assessment's Mobile Ground System," June 18, 2015.

implementing the DoD OIG recommendations to reduce sustainment and acquisition risk of the Mobile Ground System replacement.

ATTACK CHARACTERIZATION

Attack characterization is the ability to correctly identify the type and intent of an attack on the United States or its allies. The primary system that provides warning to senior decision-makers against missile threats to North America is the Integrated Tactical Warning and Attack Assessment System. The DoD OIG is now evaluating the system's ability to properly characterize ballistic missile events.

The United States Nuclear Detonation Detection System provides a near real-time worldwide, survivable capability to detect, locate, characterize, and report any nuclear detonations in the earth's atmosphere or in near space. This system supports users throughout the Government. However, in a 2018 evaluation, the DoD OIG determined that there is no clearly defined governance structure to ensure United States Nuclear Detonation Detection System requirements and capabilities are planned, resourced, sustained, or modernized. The absence of a governance structure has led to a lack of coordination with appropriate interagency leadership, which increases the risk of mission failure. In response to this report, the Deputy Secretary of Defense directed the Air Force to ensure synchronization of United States Nuclear Detonation Detection System policies, procurement plans, and survivability requirements within the DoD and across the interagency.[37]

SPACE AS A WARFIGHTING DOMAIN

The U.S. military is reliant on space across the full spectrum of operations, from counterterrorism operations to combat against a near-peer adversary. According to the Center for Strategic and International Studies' 2018 Space Threat Assessment, China continues to increase its activity and experience in space, launching 31 payloads in 2017, second only to the United States in payloads launched.

To ensure assured access to space, the DoD created the Evolved Expendable Launch Vehicle Program (EELV) to provide critical space lift capability to support DoD and other National Security missions. Since 2002, the EELV completed 57 National Security Space launches in support of the Navy, National Reconnaissance Office, and the Air Force. However, the DoD has experienced quality assurance management problems with the EELV.

For example, in 2017, the DoD OIG determined that the DoD EELV prime contractors and subcontractor did not perform adequate quality assurance management of the EELV as evidenced by the 181 nonconformities to applicable quality requirements. This inadequate quality assurance management could increase program costs, delay launch schedules, and increase the risk of mission failure to ensure assured access to space.[38]

Another system, the Global Positioning System, provides positioning, navigation, and timing data to civilian and military users who depend on this satellite-based system. Since 2000, the DoD—led by the Air Force—has been working to modernize Global Positioning System and to keep the current system of satellites—known as the Global Positioning System constellation—operational, however these efforts have experienced cost and schedule growth. In December 2017, the Government Accountability Office determined that the Air Force still faces technical risks and schedule pressures in both the short and long term. In the short term, schedule compression with the first Global Positioning System III satellite is placing the satellite's launch and operation at risk of further delays. The Government Accountability Office

[37] Report No. DODIG 2018-160, "Evaluation of the Space-Based Segment of the U.S. Nuclear Detonation Detection System," September 28, 2018.

[38] Report No. DODIG-2018-045, "Evaluation of the Evolved Expendable Launch Vehicle Program Quality Management System," December 20, 2017.

also determined that in the long term, most of the satellites under contract will have been launched before operational testing is completed, limiting Air Force corrective options if issues are discovered.[39]

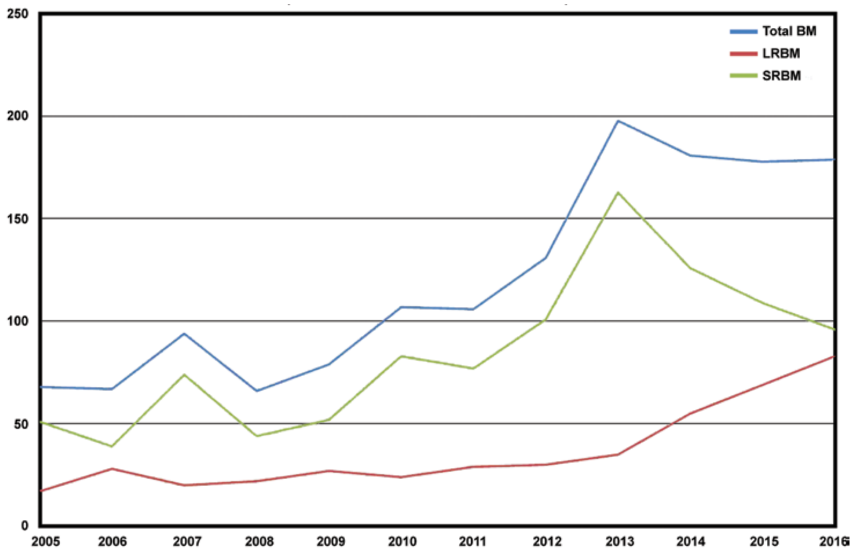
MISSILE DEFENSE

Along with the threat to space-based operations, the DoD must continue to defend the United States and deployed troops against ballistic missile attack. Ballistic and cruise missiles, with their relatively low operating costs, potential to penetrate defense systems, and value as a symbol of national power, will continue to be the offensive weapons of choice for many nations. The potential use of these missiles by U.S. adversaries must be addressed in military planning and operations. Over the last decade, there has been a significant increase in worldwide ballistic missile testing. The emphasis on ballistic missile development around the world was highlighted in the 2017 National Air and Space Intelligence Center and Defense Intelligence Ballistic Missile Analysis Committee's Ballistic and Cruise Missile Threat report. The report notes that Chinese scholars have stated, "Ballistic missiles have become an important factor that influences the world political setup, controls the battlefield posture, and even decides the outcome of war" and "It is appropriate to say that ballistic missiles have become an important sign of national defense strength and symbol of national status."

Figure 6 depicts the approximate number of ballistic missiles launched per year from 2005 to 2016. In the graphic, all ballistic missiles are categorized by range, regardless of launch platform; all missiles with a range of 1,000 km or greater are classified as long-range ballistic missiles, and all missiles with a range from 300 km to 1,000 km are classified as short-range ballistic missiles. This graphic does not include close-range ballistic missiles (missiles with a range less than 300 km) or ballistic missiles launched in combat.[40]

Since 2002, the Missile Defense Agency has been developing a Ballistic Missile Defense System that can identify and intercept enemy threats. The Missile Defense Agency has received approximately $132 billion in direct funding since 2002, and it is planning to spend an additional $47.8 billion through

Figure 6. Ballistic Missile Launches Per Year From 2005 Through 2016 (Excludes Combat Launches)



Source: Ballistic and Cruise Missile Defense Review Report, June 2017.

[39] GAO-18-74, "Better Planning and Coordination Needed to Improve Prospects for Fielding Modernized Capability," December 12, 2017.

[40] National Air and Space Intelligence Center and Defense Intelligence Ballistic Missile Analysis Committee, "Ballistic and Cruise Missile Defense Review Report," June 2017.

The Air Force's 45th Space Wing supported SpaceX's successful launch of the KoreaSat-5A satellite aboard a Falcon 9 rocket. (SpaceX photo)

FY 2022 to continue these efforts. The Government Accountability Office determined that in FY 2017, some of the system-level integrated capabilities, such as the ability to differentiate the warhead-carrying vehicle from decoys, were delayed and delivered with performance limitations. Although several programs achieved notable firsts, including the first intercept of an intercontinental ballistic missile, another interceptor failed to intercept its medium-range ballistic missile target, and other tests were delayed or canceled. Moreover, the Government Accountability Office found challenges in the Missile Defense Agency's processes for communicating the extent and limitations of integrated capabilities when they are delivered. As a result, according to the Government Accountability Office, warfighters do not have full insight into the capabilities the Missile Defense Agency delivers.[41]

The DoD OIG reported in April 2017 that the Missile Defense Agency had established several initiatives to manage supply chain risk for the Ground-Based Midcourse Defense System (one of the most critical subsystems of the Ballistic Missile Defense System) and was piloting a DoD software assurance program to improve the supply chain security for its critical software. Supply chain risk includes vulnerabilities that an adversary may exploit to sabotage, maliciously introduce an unwanted function, or otherwise compromise the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system. However, the DoD OIG reported that the Missile Defense Agency had not fully implemented DoD supply chain risk management policy. Specifically, the Missile Defense Agency did not maintain an accurate critical components list and did not identify the suppliers of all its critical components or use rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing for malicious threats, to detect vulnerabilities within critical components for the Ground-Based Midcourse Defense System.[42]

In May 2017, Secretary Mattis directed the start of the DoD's Ballistic Missile Defense Review. The review, led by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff, is being

[41] GAO-18-324, "The Warfighter and Decision Makers Would Benefit from Better Communication about the System's Capabilities and Limitations," May 30, 2018.

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

conducted to identify ways to strengthen missile-defense capabilities, rebalance homeland and theater defense priorities, and provide the necessary policy and strategy framework for the Nation's missile defense systems. The review is ongoing.

Ballistic and cruise missile threats continue to increase with the proliferation of missile technology. Over 20 countries have ballistic missile systems, and missiles likely will be a threat in future conflicts involving U.S. forces. As a result, the DoD must continue to develop a ballistic missile defense system that can identify and intercept present and future enemy threats.

NUCLEAR MODERNIZATION

The United States strategic nuclear triad, largely deployed in the 1980s or earlier, consists of submarine-launched ballistic missiles, land-based intercontinental ballistic missiles, strategic bombers carrying gravity bombs, and air-launched cruise missiles. The nuclear triad is supported by non-strategic nuclear forces, which consist of U.S. F-15E fighter aircraft and allied dual-capable aircraft that carry nuclear-armed gravity bombs. However, the 2018 Nuclear Posture Review emphasizes that the triad, non-strategic nuclear forces, and nuclear command, control, and communications system have relied on life extension programs since the 1980s. Specifically, the 2018 Nuclear Posture Review highlights the concern that multiple delays in the modernization of the nuclear force increase the risk of successfully sustaining the legacy nuclear systems and the fielding of planned replacement systems.

The United States faces several challenges as it undertakes an extensive nuclear modernization program. One of the largest challenges is a budgetary one. Modernization efforts will substantially increase the annual costs for the nuclear enterprise above the amounts the DoD and the Department of Energy currently spend. At a time when modernization of other conventional systems is planned and defense spending is likely to be constrained by long-term fiscal pressures, nuclear modernization must compete for funding with other defense priorities. Overall, the Congressional Budget Office estimated that planned modernization would cost $1.2 trillion through 2046. These figures do not take into consideration new capabilities called for in the 2018 Nuclear Posture Review or missile defense. According to the Congressional Budget Office:

- $772 billion would be allocated for the operation, sustainment, and modernization of strategic nuclear delivery systems and weapons—the long-range aircraft, missiles, and submarines that launch nuclear weapons; the nuclear weapons they carry; and the nuclear reactors that power the submarines.
- $25 billion would be allocated for the operation, sustainment, and modernization of tactical nuclear delivery systems—the aircraft capable of delivering nuclear weapons over shorter ranges—and the weapons they carry.
- $445 billion would be allocated for the complex of laboratories and production facilities that support nuclear weapons activities and the command, control, communications, and early-warning systems that enable the safe and secure operation of nuclear forces.[43]

In addition to these costs, the 2018 Nuclear Posture review calls for the DoD to modify a small number of existing submarine launched ballistic missile warheads to provide a low-yield option, and in the longer term, pursue a modern nuclear-armed sea-launched cruise missile. There are no cost estimates yet for these additional capabilities.

There is not much time between the necessary retirement of legacy nuclear systems and the additional capabilities called for in the 2018 Nuclear Posture Review. This heightens the need for the effective management and oversight of the modernization efforts. However, in a report issued

[43] Congressional Budget Office 53211, "Approaches for Managing the Costs of U.S. Nuclear Forces, 2017 to 2046," October 2017.

in 2016, the DoD OIG identified that the DoD had not developed guidance to implement, measure, or track recommendations from the 2010 Nuclear Posture Review. Further, the DoD OIG determined that the only governance structure to bring together senior leaders from all elements of the nuclear enterprise into a coherent structure—the Nuclear Deterrent Enterprise Review Group—was temporary, with no charter or plan in place to ensure permanency.[44] In response to the report, the Deputy Secretary of Defense agreed to codify the review group in DoD guidance as a permanent, DoD Senior Governance Council.

In May 2018, the Deputy Secretary of Defense approved guidance to implement the 2018 Nuclear Posture Review. The Deputy Secretary emphasized that implementation guidance was critical to ensure that the 2018 Nuclear Posture Review is translated into action. The guidance identifies a process for monitoring progress and a process for reporting on progress. The Deputy Secretary also directed the DoD to develop a charter for the Nuclear Deterrent Enterprise Review Group as an interim step until a DoD Directive regarding the review group is published. These steps seek to ensure current nuclear delivery systems can be sustained while simultaneously designing and fielding replacement systems.

However, the DoD is challenged with sustaining and replacing every major nuclear system, including nuclear ballistic missile submarines, strategic bombers, nuclear air-launched cruise missiles, intercontinental ballistic missiles, and associated nuclear command and control. These challenges also increase the risk of the DoD having a temporary gap in the required number of nuclear forces available. For example, in 2017, the Government Accountability Office reported that any unexpected delays in fielding the *Columbia*-class nuclear ballistic submarine, which will replace the *Ohio*-class nuclear ballistic submarine, could postpone the deployment of the new submarine past the 2031 deadline.[45]

Because of potential delays with fielding the *Columbia*-class submarine noted by the Government Accountability Office, the DoD OIG evaluated whether the Navy can sustain the current *Ohio*-class Nuclear Ballistic Missile Submarines until the replacement *Columbia*-class nuclear ballistic submarines are fielded. The DoD OIG determined that the Navy has taken steps to sustain the *Ohio*-class nuclear ballistic submarines until the replacement *Columbia*-class nuclear ballistic submarines are fielded. Specifically, the Navy designated strategic nuclear deterrence as its top priority in order to meet the minimum U.S. Strategic Command requirements. The Navy also prioritized nuclear ballistic submarines ahead of aircraft carriers at the naval shipyards, overcome submarine homeport dry dock challenges, trained additional shipyard workers, and optimized maintenance procedures and schedules.[46] However, the Navy will need to continue to monitor *Ohio*-class nuclear ballistic submarine sustainment until the replacement *Columbia*-class nuclear ballistic submarines are fielded, especially if unexpected delays in fielding the *Columbia*-class submarine occur.

Along with modernizing the strategic nuclear triad, the 2018 Nuclear Posture Review directs that, "in support of a strong and credible nuclear deterrent, the United States must maintain a nuclear force with a diverse, flexible range of nuclear yield and delivery modes that are ready, capable, and credible . . . which includes

[44] Report No. DODIG-2016-125, "Evaluation of DoD Nuclear Enterprise Governance," September 29, 2016.

[45] GAO 18-158, "Immature Technologies Present Risks to Achieving Cost, Schedule, and Performance Goals," December 2017.

[46] Report No. DODIG-2018-127, "Evaluation of Nuclear Ballistic Missile Submarine Sustainment," June 15, 2018.

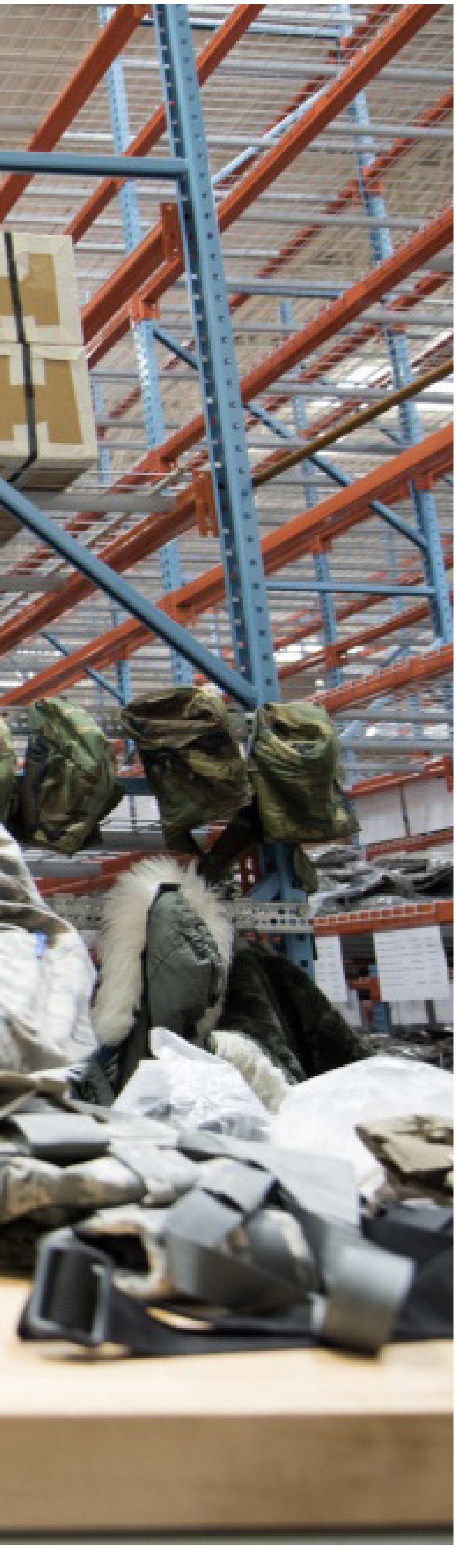
dual-capable aircraft." Dual-capable aircraft, which can deliver conventional or nuclear weapons, are a key contributor to continued regional deterrence stability and the assurance of allies.

In the past, the DoD OIG raised concerns about the DoD's ability to meet dual capable aircraft requirements. In a 2015 evaluation of nuclear planning, the DoD OIG reported that the DoD lacked expertise to effectively integrate nuclear capabilities into conventional theater operations. The DoD OIG also reported that theater nuclear planning guidance and oversight were inadequate.[47] While the DoD has initiated actions to address these findings, there is indication that efforts to meet dual capable aircraft requirements may have stalled. Because of this, the DoD OIG is now evaluating U.S. European Command's ability to conduct Nuclear Command and Control as required by presidential guidance. Additionally, the Senate Armed Services Committee's report accompanying the National Defense Authorization Act of FY 2019 included a provision directing the Comptroller General to review the DoD's efforts to incorporate the geographic combatant commands into nuclear planning and operations, including command and control responsibilities. In particular, this mandate requires the Government Accountability Office to assess the ability of the geographic combatant commands to conduct command and control operations and any changes to command and control infrastructure as a result of the 2018 Nuclear Posture Review.

In summary, the threats posed by space, nuclear, and ballistic missile delivery systems will continue to increase in number and complexity. Denying U.S. space capabilities is a central tenet of adversary strategies. In addition, at a time when other nations continue to modernize and upgrade their nuclear forces, nearly all elements of the U.S. nuclear weapon stockpile, delivery systems, and other critical infrastructure are operating well beyond their designed service life. To remain military superiority, the DoD needs to continue to balance the need to sustain current systems while simultaneously fielding replacement systems.

[47] Report No. DODIG-2015-134 "Assessment of the U.S. Theater Nuclear Planning Process," June 18, 2015.

U.S. Airmen with the 50th CPTS, inspect deployment gear at the 50th Logistics Readiness Flight warehouse at Schriever Air Force Base, Colorado, June 29, 2018. (U.S. Air Force photo)



Challenge 8: Improving Readiness Throughout the DoD

Secretary Mattis stated in the 2018 National Defense Strategy, "Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding." The Secretary also stated, "Without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people."

According to the National Defense Strategy, the central challenge to U.S. security is the reemergence of a long-term strategic competition between the United States and "revisionist powers," notably Russia and China. The Military Services find themselves having to balance two equally challenging environments, the need to continue to provide ready forces for ongoing operations aimed at defeating the ISIS while also developing the future force to address emergent threats and competitors.

The DoD Dictionary of Military and Associated Terms defines readiness as the ability of military forces to fight and meet the demands of assigned missions. According to the Chairman of the Senate Armed Services Committee Subcommittee on Readiness and Support, building a more lethal force begins with rebuilding and maintaining the DoD's readiness while also modernizing the force structure. The Chairman stated during a 2018 hearing that maintaining the delicate balance between the sustained readiness gains while modernizing is more important than ever.

For FY 2019, the DoD requested $161.2 billion for operations and maintenance to organize, staff, train, and equip the forces and to increase the readiness and lethality of the forces. These efforts present challenges as the Military Services work with each other and industry to increase their lethality within budgetary limits.

ORGANIZATION AND MANNING OF FORCE STRUCTURE

The ability of the Military Services to meet current and emerging threats depends in part on their ability to recruit and retain sufficient personnel. Effective recruitment and retention of personnel directly impacts the force structure of the DoD. According to the National Defense Strategy, the force structure of the Joint Force is the combination of military personnel and weapon systems needed to maintain "decisive advantages for any likely conflict while remaining proficient across the entire spectrum of conflict."

The National Defense Strategy stated that the DoD will focus on increasing personnel and platforms to meet key capability and capacity needs, as well as implement efforts to maximize efficiencies with current manning levels in order to manage its force structure. DoD OIG audits have noted that the Military Services are creating new positions to address force structure gaps that previously were not required, including cyber network defenders and unmanned system (drone) operators that are new career fields.[48]

However, attracting qualified recruits to fill positions is a critical challenge for each Military Service. According to testimony from the Army Vice Chief of Staff at a February 2018 hearing of the Senate Armed Services Subcommittee on Readiness and Management Support, about 27 percent of eligible American youth are not physically or mentally qualified to enter the Army. In addition, the Military Services have difficulty retaining certain personnel, such as pilots and maintenance personnel. According to the Deputy Commandant for Marine Corps Aviation, commercial airlines have recruited many pilots and maintenance personnel from the Military Services' ranks.

The FY 2019 DoD budget includes an overall increase of 15,600 military personnel and an increase in weapon systems and equipment throughout the Military Services. For example, the budget funds 93 F-35 Joint Strike Fighters and F-35 spares, modifications and depot repair capability. The budget also fully funds development of the B-21 Raider. In addition, the budget fully funds 13 new battle force ships and accelerates funding for several future ships, including three *Arleigh Burke*-class destroyers and two *Virginia*-class submarines. According to the DoD's submission to Congress in support of its budget request, the increase in military personnel, weapon systems, and equipment are needed not only for future missions but also to address current critical military personnel, weapon systems, and equipment shortages.

For example, the Army has set a readiness goal of 66 percent of all active duty Army units and 33 percent of Reserve Component units.[49] According to the U.S. Army Chief of Staff, Gen Milley, the readiness goal is to ensure that two-thirds of the Army's 31 active-duty brigade combat teams are fully trained and prepared to "fight tonight." The Army also wants one-third of its 27 National Guard combat brigade teams trained to the highest possible level. Even with increases in military personnel, weapon systems, and equipment, the Army estimates that it will not achieve that readiness goal until 2022. Increasing the readiness of Brigade Combat Teams to conduct military operations has been the focus of recent Army readiness efforts.

In October 2017, the Navy released its Comprehensive Review of Recent Surface Force Incidents. This review was conducted to address the series of ship collisions in the Indo-Pacific region that occurred in 2017, resulting in the death of 17 sailors. In addition, in December 2017 the Navy released its Strategic Readiness Review report, which focused on identifying trends and contributing factors that may have compromised performance and the readiness of the fleet. Based on the recommendations contained in the two reviews, the Navy made a series of administrative and personnel changes in an attempt to improve the safety and readiness of the fleet. Those recommendations focused on corrective actions necessary to ensure the safety of Navy personnel, safe operations at sea, and the readiness of naval forces. The recommendations also addressed naval operations from individual and unit training to how the naval force is generated and employed.

[48] Report No. DODIG-2018-092, "DoD Emergency Management Programs in the U.S. Africa Command," March 28, 2018; Report No. DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018; and Report No. DODIG-2018-096, "Followup Audit: The Defense Enrollment Eligibility Reporting System Security Posture," March 30, 2018.

[49] The readiness goal is to ensure two-thirds of Army 31 active-duty brigade combat teams are fully trained and prepared to fight. The Army also wants one-third of its 27 National Guard combat brigade teams trained to the highest possible level.

To confirm that the administrative and personnel changes taken by the Navy are resulting in increased fleet readiness, the DoD OIG is now reviewing how the Navy is addressing the readiness challenges of the *Arleigh Burke*–class destroyers.

The Air Force has also focused on staffing challenges related to aircraft pilots and maintenance personnel. According to a report from the Government Accountability Office, Air Force pilot staffing level and authorizations data for FYs 2006 through 2017 showed that the Air Force had fewer fighter pilots than authorizations for 11 of 12 years from FYs 2006 through 2017. This gap increased from 192 fighter pilots (5 percent of authorizations) in FY 2006 to 1,005 (27 percent) in FY 2017.

According to the Air Force, the pilot gap is concentrated among fighter pilots with fewer than 8 years of experience. In January 2017, the Air Force forecasted that the fighter pilot gap will persist over time, even as the Air Force takes steps to train more fighter pilots and improve retention.[50] The Air Force stated that it was able to reduce its aircraft maintenance personnel shortfall from approximately 4,000 airmen in FY 2015 to approximately 400 in FY 2017; however, the Air Force also stated that low experience levels will continue to be an issue for several years for both the Active and Reserve Components. Additionally, staffing challenges may continue to impact the Air Force's ability to conduct depot-level maintenance and supply chain management as the Air Force faces continuing challenges in recruiting, retaining, training, and developing its scientist and engineer workforce.

Similar to the Army and Navy, the Marine Corps is addressing readiness issues by refocusing operations to the types of warfare that were outlined in the National Defense Strategy. In his testimony before the Senate Armed Services Committee, the Commandant of the Marine Corps discussed how the Marine Corps must further develop and integrate force capabilities in support of the Navy. The Commandant stated that this effort would require "measured shifts" from a focus on a near symmetric land-based enemy (similar forces fighting) to an asymmetric (dissimilar forces fighting) view where Marine forces ashore threaten enemy naval and air forces from expeditionary advance bases. The Commandant also stated that the available inventory of amphibious warships and connectors is well below the requirement. He noted that the Marine Corps' ability to adequately address challenges such as these will directly affect how the United States engages with its allies and near peer competitors for the foreseeable future.

In short, the DoD needs to monitor its readiness and force structure to integrate new capabilities, adapt warfighting approaches, and change business practices to achieve and maintain readiness.

TRAINING OF FORCES

The DoD focuses on training forces in the manner they fight, and fighting in the manner they train. However, as the DoD's top priority shifts from counterterrorism to strategic competition with other nations, the focus of the Military Services' training programs will need to adapt.

For example, according to the Secretary of the Army, the Army has determined that, although its personnel have conducted extensive training for counterinsurgency operations for the ongoing war on terrorism, other training needs to be emphasized. In his April 2018 testimony before the Senate Armed Services Committee, the Secretary discussed the need to re-engage in large-scale exercises involving the movement and employment of large forces, which is a departure from the small unit training that has dominated training for units preparing to deploy to Afghanistan or other theaters of operations to combat terrorism. With the refocus of the National Defense Strategy, the Navy is also assessing how its personnel are

[50] GAO-18-113, "Military Personnel: DOD Needs to Reevaluate Fighter Pilot Workforce Requirements," April 2018.

trained and certified for operations. In addition, the National Defense Authorization Act for FY 2019 directs the Navy to perform a comprehensive individual proficiency assessment prior to a surface warfare officer starting a tour.

The Marine Corps, along with the other Military Services, recognizes that if the United States is to prevail in the new strategic environment, training in all types of climates and terrain must be provided, including training for cold weather operations. In his March 2018, testimony before the Senate Armed Services Committee, the Deputy Commandant for Combat Development and Integration stated that the Marine Corps is considering expanding training conducted at places such as the Joint Pacific Alaska Range Complex in Alaska. In addition, he also discussed the Marine Corps' challenges of amphibious operations in the digital era, and that the Marine Corps is having to rethink how to conduct amphibious operations. The Deputy Commandant discussed how advancements in the abilities of potential adversaries to prevent U.S. forces from gaining access to areas, or restricting the abilities of U.S. forces to operate in an area of conflict, combined with the integration of drones into smaller size units, creates challenges to how the Marine Corps conducts traditional amphibious operations that will need to be overcome. Those challenges include when and how to employ amphibious assault vehicles, how to support an amphibious operation, or even how many Marines should constitute units such as the rifle squad.

In FY 2019, the DoD OIG intends to conduct an audit of joint exercises to assist the Military Services in determining how the changes that affect amphibious operations are being addressed. Further, in FY 2019, the DoD OIG intends to evaluate the training of military personnel in various settings and under various conditions.

The Military Services also share the challenge of having available, sufficient, and realistic space to conduct training. For example, in 2018 the DoD OIG determined that training ranges and airspace did not have the capability or capacity to effectively support aviation training for units supporting the units assigned to U.S. Indo-Pacific Command. Advances in weapons technology and encroachments on existing training areas have limited the use of the training ranges and made their continued use questionable. Most military training ranges were established over 75 years ago when the United States prepared for World War II. The ranges were generally located in remote rural areas, but over the years urban and suburban development began to encroach upon military ranges. As technology improved, the development of advanced weapon systems created the demand for larger ranges for aviators and operators to adequately train in the aircraft and operate the systems. From 2001 through 2018, the DoD identified the challenges encroachment presents to military training and reported it to Congress, but, the DoD OIG compared the reports from 2001 and 2017, and found no reported improvement in range capability. The National Defense Authorization Act for FY 2019 requires the DoD to identify, plan for, and resolve long-standing limitations on training ranges in a strategic plan that is due on April 1, 2019.

EQUIPPING THE FORCES

As the DoD strives to proactively equip its forces, it also faces the challenge of using technology that was cutting edge not that long ago but may now be outdated and vulnerable to adversaries. The Military Services have identified critical equipment priorities to seek to ensure they have military superiority over U.S. adversaries.

In addition, to improve the lethality of the forces, the Military Services have identified new or additional capabilities required to become a more lethal force. The Army identified six modernization priorities in its FY 2019 budget request. Specifically, the Army requested funding to modernize long-range precision missiles; the next generation of combat vehicles; future vertical lift; a robust network that is not vulnerable to cyber attacks; air and missile defense; and soldier lethality. The Army's implementation of the six moderation priorities will affect the Army's ability to reach its readiness goals in the near term.

The Commandant of the Marine Corps identified, during a 2018 hearing before the Senate Armed Services Committee, a need for longer-range artillery as a solution to address the long-range weapons that potential adversaries have developed. To satisfy another capability requirement, the Army and Marine Corps have partnered to develop the new Joint Light Tactical Vehicle, the successor to the venerable Humvee.

The Chief of Naval Operations testified before the Senate Armed Services Committee that, to address the Navy's capability requirements, the Navy is adding new items of equipment to its portfolio of weapon systems, such as the *Columbia*-class ballistic submarine, additional Littoral Combat Ships and Frigates, and the MQ-25 Stingray tanker drone. The Navy is adding these new items to replace aging weapon systems and to introduce new capabilities into the Navy's portfolio. The Chief of Naval Operations stated that the Navy is also procuring the spare parts and support needed to maintain the new equipment, as well as to maintain an increased readiness posture. The Navy is also working to increase the amount of maintenance performed to ensure maintenance that has been deferred to satisfy warfighting requirements is still conducted.

The Air Force is examining the additional need for specific types of aircraft, such as the RC-135 family of special aircraft, to address the increased number of missions. According to the Air Force, although the DoD had sufficient quantities of RC-135s for operations in the past, as technology advances and is integrated into the modern battlefield, additional RC-135s are needed for the DoD and its allies. The Air Force is also seeking to replace the E-8C Joint Surveillance Target Attack Radar System aircraft, which provides airborne battle command and control.

While it is important to identify critical capabilities and new technology to meet critical needs, it is equally important to maintain equipment. Various DoD OIG reviews have identified instances where the Military Services are not properly maintaining weapon systems and equipment. For example, in June 2018, the DoD OIG reported that the Army did not ensure that vehicles and weapons stored in Kuwait and Qatar as part of Army Prepositioned Stock received the prescribed cyclic scheduled maintenance.[51] Similarly, in June 2018, the Government Accountability Office reported that delays in returning Patriot surface-to-air missile systems from depots to units is affecting unit training. The Government Accountability Office determined that only one of seven Patriot batteries that underwent reset from 2014 through 2017 received its equipment within 180 days in accordance with Army policy, which adversely affected the amount of time the unit had to train on the equipment before deployment.[52]

In short, while the National Defense Authorization Act for FY 2019 authorizes the DoD to procure additional weapon systems and equipment, the challenges the DoD faces to ensure readiness extend beyond the initial procurement and fielding of the equipment. The DoD also needs to ensure that all weapon systems and equipment are properly maintained throughout their planned life cycles.

In summary, with the issuance of the new National Defense Strategy and its emphasis on the reemergence of long-term, strategic competition, the DoD is focused on a variety of warfighting missions in addition to counterterrorism. As the DoD strives to improve its readiness and to organize, staff, train, and equip a more lethal force, balancing the ability of the Military Services to meet current and future threats remains a significant challenge.

[51] Report No. DODIG-2018-132, "Management of Army Equipment in Kuwait and Qatar," June 29, 2018.

[52] GAO-18-447, "Military Readiness: Analysis of Maintenance Delays Needed to Improve Availability of Patriot Equipment for Training," June 2018.

An Air Force B-1B Lancer receives fuel over the southern Pacific Ocean during a training mission with the Royal Australian Air Force as part of Exercise Black Dagger. (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. Although Congress and the DoD have sought to improve the acquisition of major weapon systems, many DoD programs still fall short of cost, schedule, and performance expectations. This can result in unanticipated cost overruns, program development spanning decades, and, in some cases, a reduction in the capability ultimately delivered to the warfighter. The 2018 National Defense Strategy states that the DoD must develop a rapid, iterative approach to capability development to reduce costs, technological obsolescence, and acquisition risk. However, the DoD has struggled with defining requirements and providing proper oversight to ensure products and services are delivered on time and at the right cost.

Acquisition and contract management have been high-risk areas for the DoD for many years. Although Congress and the DoD have sought to improve the acquisition of major weapon systems, many DoD programs still fall short of cost, schedule, and performance expectations. This can result in unanticipated cost overruns, program development spanning decades, and, in some cases, a reduction in the capability ultimately delivered to the warfighter. The 2018 National Defense Strategy states that the DoD must develop a rapid, iterative approach to capability development to reduce costs, technological obsolescence, and acquisition risk. However, the DoD has struggled with defining requirements and providing proper oversight to ensure products and services are delivered on time and at the right cost.

ACQUISITION AND SUSTAINMENT

The scope and size of acquisition programs for DoD weapon systems is enormous. In the FY 2019 Presidential Budget, the DoD requested $236.7 billion to fund acquisition programs. From December 2016 to December 2017, the number of programs in the DoD Major Defense Acquisition portfolio decreased from 87 to 83 and the total planned investment in these programs grew from $1.75 trillion to $1.93 trillion. Major Defense Acquisition programs are programs that have total research, development, test, and evaluation costs of more than $480 million or procurement costs of more than $2.79 billion.

In recent years, the DoD has sought to streamline the major weapon systems acquisition process. For example, the National Defense Authorization Act for FY 2017 mandated the split of the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics into two separate entities. In response to the guidance in the National Defense Authorization Act for FY 2017, the DoD created two new offices, the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment. According to the report to Congress in response to Section 901 of the National Defense Authorization Act for FY 2017, the Under Secretary of Defense for Research and Engineering is responsible for driving innovation and accelerating the advancement of the DoD's warfighting capability, while the Under Secretary of Defense for Acquisition and Sustainment is responsible for delivering proven technology to the warfighter more quickly and affordably. This reorganization focuses the principal role of the Under Secretary of Defense for Acquisition and Sustainment from program oversight to that of directing major DoD investments to ensure integrated, technically superior capabilities that consistently outpace enemy threats and advancements. In addition, the National Defense Authorization Act for FY 2017 provided the DoD the ability to significantly streamline the acquisition process and assign the Military Services greater responsibility and accountability for program execution and performance.[53]

Additionally, the FY 2016 National Defense Authorization Act provided the DoD with the authority to rapidly prototype and rapidly field capabilities under a new pathway, distinct from the traditional acquisition system. In April 2018, the Under Secretary of Defense for Acquisition and Sustainment issued a memorandum encouraging DoD Components to immediately develop rapid prototype and fielding processes and procedures. According to the memorandum, the Under Secretary will begin a collaborative policy development effort in January 2019 to allow DoD Components to provide input based on their prototype processes and procedures, which is expected to include lessons learned in the new DoD policy and guidance. While rapid acquisition subjects the DoD to the risk of cost growth, schedule delays, and poor program performance, acquisition officials have stated that the DoD is willing to accept the risk to keep up with innovation and technology. However, DoD officials will need to ensure proper oversight of any rapid acquisition efforts to avoid costly program delays.

SBIRS GEO Flight 4 payload mated with its Atlas V-411 rocket completed a roll out at SPacee Launch Complex-41, Cape Canaveral Air Force Base.

These initiatives and these steps seek to improve many acquisition programs that continue to exceed the cost and schedule defined in the program's strategy documents. For example, in 2018 the DoD OIG determined that the Program Executive Office for Assembled Chemical Weapons

[53] DoD, "Report to Congress Restructuring the DoD Acquisition, Technology, and Logistics Organization and Chief Management Officer Organization," August 2017.

Alternatives did not effectively manage the program's cost and schedule. Program executive officials and the contracting officers did not effectively manage contractor performance through incentive and award fee contracts, did not provide sufficient quality assurance oversight, and paid approximately $23 million extra to the contractors to correct deficiencies. As a result, program officials were 16 months behind schedule in completing destruction of all chemical weapons and may not meet the congressionally mandated deadline of December 31, 2023, for the destruction of all U.S.-stockpiled chemical weapons. Additionally, the program exceeded its cost estimate by 21.6 percent.[54]

In addition to cost overruns and schedule delays, the DoD continues to experience other acquisition challenges. Specifically, the DoD OIG regularly identifies acquisitions in which:

- program personnel did not adequately document the acquisition process to define, validate, fund, and ensure the capability requirements were met;
- programs did not meet required system performance parameters as intended; and
- planned procurement quantities were not adequately justified.

For example, in 2017, the DoD OIG reported that that Army and Navy officials determined that the Joint Air-to-Ground Missile program was unaffordable as originally designed because sufficient funding was not available to meet the Joint Air-to-Ground Missile program requirements. Therefore, program officials restructured the program to reduce program costs by lowering two primary performance requirements, using older proven technology instead of new technology still being developed, and deferred the delivery of required capabilities to future upgrades. Although these actions ensured the Joint Air-to-Ground Missile program was affordable in the near term, the DoD OIG determined that the weapon did not meet the requirements to be launched from fixed-wing aircraft; strike targets from longer distances; and increase the accuracy, lethality, and interoperability over existing air-to-ground missiles.[55]

In 2018, the DoD OIG determined that the Army did not adequately justify the planned procurement quantities of AH-64E Apaches. The Apache is a two-pilot attack and reconnaissance Army helicopter. Army officials did not conduct analyses to determine the necessary quantities to meet the Army's mission needs before approving the quantity to be produced. Therefore, Army officials could not ensure that 167 AH-64E Apaches, valued at $3.5 billion, would meet the needs of the Army. Additionally, the Army had no assurance that the AH-64E program was affordable.[56]

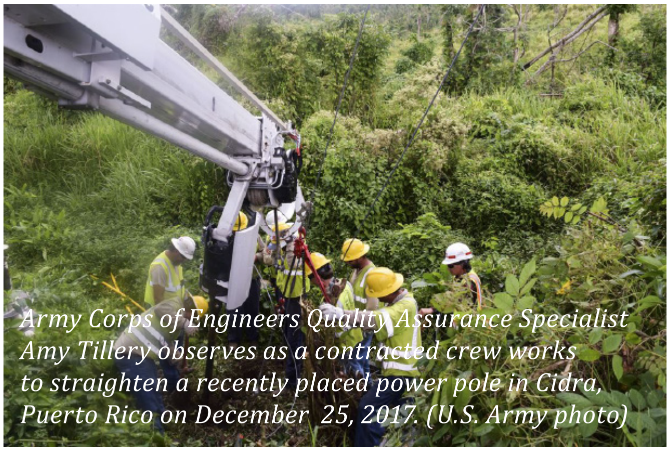
The DoD OIG also continues to identify other challenges in the acquisition process related to the pricing of spare parts and managing its contracts for weapon system support. In 2017, the DoD OIG determined that an Air Force contracting officer did not adequately determine fair and reasonable prices for 11 C-5 Reliability Enhancement and Re-Engineering Program spare parts because the contracting officer did not obtain sufficient commercial sales data for the parts. The C-5 is the largest cargo aircraft in the Air Force inventory, and the C-5 Reliability Enhancement and Re-Engineering Program is intended to reduce operating costs, improve reliability, upgrade communication and aircraft operating systems, and extend the C-5 service life. As a result of insufficient sales data, the Air Force may not have purchased the spare parts, valued at $58.8 million, at fair and reasonable prices.[57]

[54] Report No. DODIG-2018-076, "Chemical Demilitarization – Assembled Chemical Weapons Alternatives Program," February 22, 2018.

[55] Report No. DODIG-2018-038, "Joint Air-to-Ground Missile Program," December 7, 2017.

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

[57] Report No. DODIG-2017-053, "The Air Force Did Not Adequately Determine or Document Fair and Reasonable Prices for Lot 7 Sole-Source Initial Spare Parts for the C-5 Aircraft," February 7, 2017.



Army Corps of Engineers Quality Assurance Specialist Amy Tillery observes as a contracted crew works to straighten a recently placed power pole in Cidra, Puerto Rico on December 25, 2017. (U.S. Army photo)

To monitor DoD progress in addressing this challenge, the DoD OIG has two ongoing audits related to spare parts and contracts for weapon system support. One audit is examining whether the DoD is receiving ready-for-issue spare parts for the F-35 Joint Strike Fighter and whether it is paying sustainment incentive fees according to the incentive fee plan. The F-35 Joint Strike Fighter program is a multi-Service, multi-national acquisition intended to develop and field the next-generation strike fighter aircraft for the U.S. Air Force, Navy, and Marine Corps, and eight international partners. The second audit is determining whether the Air Force was inappropriately charged for MQ-9 Block 5 Reaper repairs prior to the DoD accepting the aircraft and whether the Air Force was procuring excess MQ-9 Block 5 spare parts. The MQ-9 Reaper is a single-engine turboprop, remotely piloted multi-mission aircraft designed to operate at medium-to-high altitudes for long endurance flights.

Another part of the acquisition challenge is that weapons manufacturers are incentivized to submit optimistic cost and schedule estimates to be awarded major contracts. Service officials agree with these optimistic estimates in order to remain within their acquisition budgets. However, the optimistic cost estimates can result in programs' failure to meet performance expectations after the acquisition process has started.

For example, in 2018, the DoD OIG determined that the Navy's Surface Electronic Warfare Improvement Program has experienced significant cost increases. The program provides an integrated shipboard combat system that provides early detection, signal analysis, threat warning, and protection from anti-ship missiles. However, during the engineering and manufacturing development phase, program officials did not approve a cost baseline estimate. The lack of baseline cost data prevents the DoD from consistently measuring program performance. As a result, the Navy may pay more than the original estimated cost to complete fewer deliverables than agreed to in the original contract. A deliverable is any item developed by the contractor and delivered as part of the contract. Additionally, the Navy may complete the engineering and manufacturing development phase behind schedule and may complete initial production later than planned.[58]

In FY 2017, the DoD OIG identified approximately $883 million in questioned costs and funds recommended to be put to better use during its acquisition audits related to unallowable contractor payments, requirements determination, and program management. Additionally, as of March 2018, there were 255 open DoD OIG recommendations related to the formulation and oversight of contracting strategies that support the procurement of DoD acquisition programs, automated information systems, and special interest projects for the DoD. These recommendations involve issues such as validation of procurement quantities for major defense acquisition programs, fair and reasonable contract pricing, and contracting practices that support compliance with defense acquisition program requirements.

[58] Report No. DODIG-2018-025, "Defense Hotline Allegations on the Surface Electronic Warfare Improvement Program Block 3 Costs," November 9, 2017.

CONTRACT MANAGEMENT AND OVERSIGHT

The DoD obligated $252.1 billion through the 3rd quarter of FY 2018 on contracts for supplies, equipment, materials, engineering services, and construction and sustainment of facilities, as well as other products and support services. The Government Accountability Office has stated that ensuring the DoD has the people, skills, capacities, tools, and data needed to make informed acquisition decisions is essential if the DoD is to effectively and efficiently carry out its mission in an era of more constrained resources. Oversight of Government contract surveillance is critical to ensuring that contractors provide quality services and supplies in a timely manner, within cost; to mitigating contractor performance problems; and to ensuring that the Government receives the best value in its contracts.

However, the DoD OIG has regularly identified problems with the management of contract requirements in both products and services. For example, in 2018, the DoD OIG determined that the Defense Contract Management Agency did not properly define requirements, develop an acquisition plan, or submit offers for Small Business Administration acceptance for $61 million worth of information technology contracts.[59] In another audit in 2018, the DoD OIG determined that U.S. Strategic Command did not involve other DoD organizations, such as the U.S. Army Corps of Engineers or the Defense Threat Reduction Agency, in the initial planning for the U.S. Strategic Command replacement facility military construction project. The audit determined that U.S. Strategic Command officials could have benefitted by requesting that the eventual construction agent, U.S. Army Corps of Engineers, and the Defense Threat Reduction Agency provide input on how to ensure the requirements would reflect the special uses of this facility and the additional security requirements for the construction contract.[60]

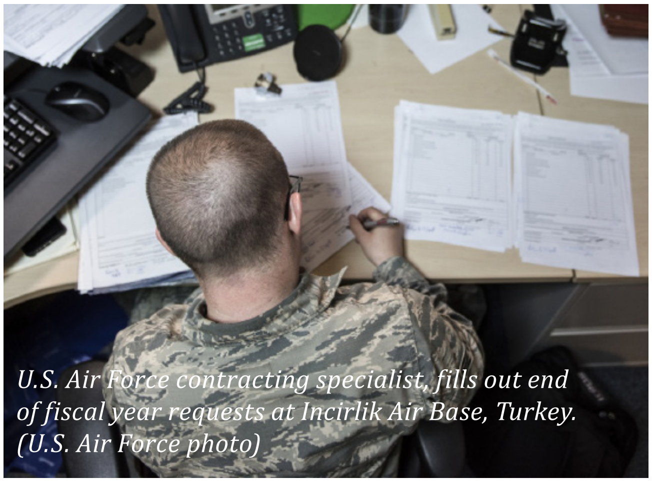
The DoD also needs to improve compliance with legal requirements such as the Berry Amendment, the Buy American Act, and contractor past performance assessments. The Berry Amendment directs DoD personnel to ensure funds appropriated or otherwise available to the DoD are not used to procure certain items if the items were not grown, reprocessed, reused, or produced in the United States. The Buy American Act requires, with certain exceptions, that only articles, materials, and supplies that were mined, produced, or manufactured in the United States are used to fulfill Federal procurement and construction contracts. Contractor past performance assessment reports must include detailed and complete statements about the contractor's performance and be based on objective data and supported by program and contract management data.

For example, in 2018 DoD OIG auditors determined that DoD contracting personnel did not comply with the Berry Amendment for 40 of the 109 contracts the auditors reviewed, with an obligated value of $211.6 million. Specifically, DoD contracting personnel did not include the required Berry Amendment clause, did not prepare award notices containing Berry Amendment exception language when procuring foreign-made items, and improperly purchased foreign-made items or item

A Marine performs maintenance work on a Humvee on the USS Rushmore in the Pacific Ocean, August 27, 2018. (U.S. Marine Corps photo)

[59] Report No. DODIG-2018-110, "Defense Contract Management Agency's Information Technology Service Contracts," April 25, 2018.

[60] Report No. DODIG-2018-122, "U. S. Strategic Command Facility Construction Project," May 31, 2018.



U.S. Air Force contracting specialist, fills out end of fiscal year requests at Incirlik Air Base, Turkey. (U.S. Air Force photo)

containing nondomestic components. Further, DoD contracting personnel did not comply with the Buy American Act for 41 of the 171 contracts reviewed, with an obligated value of $2.6 million. Contracting personnel also did not include the required Buy American Act clauses, and improperly purchased foreign-made items. To address these deficiencies, DoD contracting personnel issued a local notice to reinforce compliance with the Berry Amendment and the Buy American Act, required Berry Amendment and Buy American Act training, and updated standard operating procedures.

As a result of four previous DoD OIG reports on the Berry Amendment, the Army, Navy, Air Force, and Defense Logistics Agency contracting personnel modified 25 contracts to address the Berry Amendment requirement. In addition, Defense Procurement and Acquisition Policy personnel issued guidance reminding the DoD's acquisition community of the importance of complying with domestic procurement laws and instructing the procurement workforce to complete training on the Berry Amendment and Buy American Act.[61]

Additionally, DoD officials have not always evaluated contractor performance in accordance with Federal guidance. Accurate and timely Contractor Performance Assessment Reporting System reports that contain past performance assessment information are necessary for source selection officials, both Federal and DoD, to make informed decisions related to contract awards. The DoD OIG has reported this challenge in recent years, and it continues to be a problem. For example, in 2018 the DoD OIG determined that U.S Army Corps of Engineers Omaha District officials consistently missed reporting deadlines and eventually decided not to file past performance reports as required by the Federal Acquisition Regulation. Additionally, the DoD OIG determined that a U.S. Army Corps of Engineers Fort Worth District official did not prepare past performance reports for three design contract task orders as required by the Federal Acquisition Regulation. Contractor past performance information is critical to ensuring that the U.S. Government only conducts business with companies that provide quality products and services on time.[62]

The DoD OIG has issued four reports on oversight and management of energy savings performance contracts. An energy savings performance contract is a type of contract through which an energy services contractor designs, finances, acquires, installs, and maintains energy-saving equipment and systems for a Federal agency. Energy savings performance contracts allow Federal agencies to procure energy savings and facility improvements with no upfront capital costs or special appropriations from Congress. In the most recent report, issued in December 2017, the DoD OIG determined that Navy officials did not properly administer seven energy savings performance contracts, valued at $822.7 million. In previous reports, the DoD OIG determined that Navy and Air Force officials did not validate contractor-claimed energy savings and contracting officials did not develop quality assurance surveillance plans

[61] Report No. DODIG-2018-070, "Summary Report of DoD Compliance With the Berry Amendment and the Buy American Act," February 6, 2018.

[62] Report No. DODIG-2018-125, "The Fort Bliss Hospital Replacement Military Construction Project," June 6, 2018.

that provided specifics on how to oversee each implemented energy conservation measure. As a result of these audits, the Assistant Secretary of Defense (Energy, Installations, and Environment) agreed with the recommendations to develop and implement DoD-wide guidance to monitor energy savings performance contracts to include validating contractor-claimed energy savings. In addition, the Assistant Secretary agreed to coordinate with the Defense Procurement and Acquisition Policy Director, to ensure appropriate guidance or policy is in place to require quality assurance surveillance plans tailored to specific energy conservation measures in energy savings performance contracts.[63]

In 2019, the DoD OIG plans to conduct audits regarding statutory requirements for the use of past performance information as part of the source selection process. The DoD OIG also intends to audit undefinitized contractual actions, which are agreements that allow a contractor to begin work and incur costs before the Government and the contractor have reached a final agreement on contract terms, specifications, or prices.

Monitoring contractor performance is critical to identify the contractor's compliance or noncompliance with the terms and conditions of the contract. In response to DoD OIG recommendations, the DoD is seeking to implement additional training, improved guidance, and better quality assurance plans related to contractor oversight. Overall, as of March 2018, the DoD OIG was tracking 161 open recommendations on the oversight and integration of contractor personnel and associated equipment providing support to DoD operations. Contractor oversight includes efforts to ensure that supplies and services are delivered in accordance with the terms and conditions of the contract. These recommendations are related to contractor oversight, such as assessment of contractor performance through performance assessment reports; management of energy savings performance contracts; development of training; and quality assurance surveillance plans.

However, DoD OIG audits continue to find deficiencies in contract oversight. For example, in 2017 the DoD OIG determined that the U.S. Navy did not provide effective oversight of the base support contracts in Bahrain.[64] The contracting officer's representative relied on foreign national direct-hire or contractor performance assessment representatives to execute all quality assurance oversight of the contractors; however, the contracting officer's representative did not ensure the representatives oversaw all contractual requirements. At one base, some of the oversight tasks performed by the representatives approached inherently governmental functions.

Additionally, the DoD OIG is conducting audits related to disaster recovery response. One audit is examining contractor performance oversight of temporary emergency power contracts for the disaster recovery response to Hurricanes Harvey and Irma. Another audit is focusing on whether the U.S. Army Corps of Engineers properly monitored contractor performance, and appropriately reviewed and paid invoices for the Puerto Rico power grid repair and restoration contracts in response to Hurricane Maria.

In FY 2019, the DoD OIG plans to perform audits on undefinitized contractual actions, military construction, other transaction authorities, use of past performance information in the source selection process, Government purchase cards, TRICARE, and disaster preparedness and response for natural disasters. The DoD OIG also plans to continue auditing contract oversight of contracts in Africa and Southwest Asia.

[63] Report No. DODIG-2018-050, "Naval Facilities Engineering Command Administration of Selected Energy Savings Performance Contracts," December 17, 2017.

[64] Report No. DODIG-2018-050, "Naval Facilities Engineering Command Administration of Selected Energy Savings Performance Contracts," December 17, 2017.

In short, without effective oversight by contracting officer's representatives and other quality assurance personnel, the DoD will not have sufficient information to assure goods and services received are consistent with contract quality requirements and performed in a timely manner. Improper management of contract requirements, noncompliance with legal requirements, and deficiencies in contract oversight expose the DoD to increased potential for fraud and waste.

PROCUREMENT FRAUD AND PRODUCT SUBSTITUTION INVESTIGATIONS

Procurement fraud is also a significant risk in DoD acquisitions. In FY 2018, the DoD OIG's criminal investigative component, the Defense Criminal Investigative Service (DCIS) initiated 135 cases involving allegations of overpricing, cost and labor mischarging, and counterfeit and defective product cases. The potential financial loss is significant, and acquisition fraud can also harm the DoD's mission readiness, the safety of warfighters, and overall trust in the Government.

For example, DCIS regularly receives allegations involving Government overpayment for items and services. In some instances, contractors fail to disclose accurate pricing data, conceal actual costs, and knowingly overcharge the Government for products and labor. DCIS also investigates allegations pertaining to contractors billing for services or items the DoD never receives.

For example, DCIS investigated allegations that Telephonics Corporation overbilled the DoD on contracts to provide service and materials for the Warlock and the Light Airborne Multipurpose System. The Warlock System is installed on Army vehicles to interrupt wireless systems designed to trigger improvised explosive devices and is used in Afghanistan and Iraq. The Light Airborne Multipurpose System is a high-speed, digital air-to-ground datalink used on Navy helicopters. On November 2017, Telephonics Corporation agreed to pay $4.25 million to the Government to settle allegations that it failed to provide the Government accurate cost data. Allegedly, Telephonics overbilled the Army and Navy for services by providing inflated cost estimates and different labor rates than those specified in the contracts.[65]

Additionally, DCIS investigated Veteran Logistics, Inc. and its co-owners, Michael Mayer and Jeffrey Harrington for conspiracy to defraud the U.S. Navy using the Defense Logistics Agency's DoD EMALL, currently known as FEDMALL. FEDMALL is a web-based commerce site used by Government personnel to purchase products. Mayer and Harrington electronically submitted claims to the Defense Logistics Agency using FastPay for payment for items they knew had not been sold to the Navy and had in fact been substituted with other products they were not authorized to sell. Mayer and Harrington pleaded guilty and were each sentenced to 15 months incarceration. Also, Mayer, Harrington, and Veteran Logistics, Inc. forfeited $2.4 million in illegal proceeds. In July 2018, Mayer, Harrington, Veteran Logistics, Inc., and other associated companies were debarred from Federal contracting.

DCIS also investigates allegations of product substitution, which involves the supply of counterfeit, defective, or substandard products to the DoD. The introduction of counterfeit, defective, or substandard products into the DoD supply chain and its weapon systems can disrupt readiness, waste economic resources, and threaten the safety of military and Government personnel. As of August 2018, DCIS is investigating 34 cases involving allegations of product substitution, defective parts, or counterfeit parts in FY 2018.

For example, DCIS investigated allegations that Dennis Merkel, a former production manager at a Portland-area aluminum extrusion manufacturing facility, falsified certifications on mechanical tensile test results in connection with NASA and Missile Defense Agency Government contracts.

[65] U.S. Department of Justice press release, November 17, 2017.

U.S. Army Corps of Engineers perform recovery installation after damages caused by Hurricane Florence. (U.S. Army photo)

On April 18, 2018, the Department of Justice indicted Merkel for his alleged participation in this decade-long fraud scheme, which was allegedly carried out to conceal failing tensile test results, increase profits and productivity, and obtain production-related bonuses.[66]

In another example, DCIS investigated allegations that Toyobo, the sole manufacturer of Zylon fiber, knew that Zylon degraded quickly in normal heat and humidity, and that this degradation rendered bulletproof vests containing Zylon unfit for use. It was further alleged that Toyobo actively marketed Zylon fiber for bulletproof vests, published misleading degradation data that understated the degradation problem. Additionally, when Second Chance Body Armor recalled some of its Zylon-containing vests in late 2003, Toyobo started a public relations campaign designed to influence other body armor manufacturers to keep selling Zylon-containing vests. On March 15, 2018, Toyobo Co. Ltd. of Japan and its American subsidiary, Toyobo U.S.A. Inc. (collectively, Toyobo), agreed to pay $66 million to settle claims they used defective Zylon fiber used in bulletproof vests sold to the U.S. military and Federal, State, and local law enforcement agencies.[67]

In summary, the DoD must find ways to deliver weapon systems on time and within budget. The DoD needs to build on existing reforms by examining best practices to integrate critical requirements, resources, and acquisition decision-making processes. Furthermore, the DoD needs to ensure the reorganization of the acquisition offices brings focus to the specific functions within the acquisition life cycle. In addition, the DoD needs to focus on contract management reform to better manage and oversee contracts for goods and services. Finally, the DoD must reduce the opportunity for fraud in the acquisition process and hold accountable those who commit it.

[66] U.S. Department of Justice press release, April 19, 2018.

[67] U.S. Department of Justice press release, March 15, 2018.

A U.S. Sailor, assigned to Naval Hospital Jacksonville's Medical Home Port Purple Team, monitors an infant's heart during a checkup. (U.S. Navy photo)

Challenge 10: Providing Comprehensive and Cost-Effective Health Care

Providing health care at a reasonable cost without sacrificing quality is an ongoing challenge for the DoD. The Military Health System must provide quality health care for 9.4 million military beneficiaries, within fiscal constraints, while facing increased user demand and increasing overall health care costs. The Military Health System must also respond and adapt to changing demographics, evolving standards for access and quality, advances in science and medicine, complex payment and cost considerations, rapidly evolving information technology capabilities, and fluid patient expectations. The DoD will face challenges related to Military Health System reform as the Defense Health Agency takes responsibility this year for the military treatment facilities from the Military Services. In addition, the DoD faces challenges in providing behavioral health services to beneficiaries, including preventing suicides and preventing and treating opioid misuse. At the same time, the DoD needs to integrate medical records with the Department of Veterans Affairs and also protect the confidentiality of electronic health records.

The Military Health System 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 Military Health System provides medical care to service members, retirees, and their eligible family members. Direct care is provided at military treatment facilities by military, civilian, and contracted providers and purchased care, provided at commercial locations through the TRICARE program, which is the DoD's health care program. The Defense Health Agency manages the TRICARE program under the authority of the Assistant Secretary of Defense (Health Affairs).

The DoD OIG has performed audits and evaluations and issued recommendations covering many different areas of DoD health care, including reviews of quality and access to care and cost control, and issued numerous recommendations for improvement. Overall, the DoD has reduced the number of open recommendations related to health care and morale issues in the past year, from 114 open recommendations in March 2017 to 96 as of March 31, 2018.[68]

[68] DoD OIG, "Compendium of Open Office of Inspector General Recommendations to the Department of Defense as of March 31, 2018," July 30, 2018.

For example, the DoD has implemented recommendations related to a February 2018 evaluation report by the DoD OIG on the Military Health System Review's quality of care. Specifically, the DoD improved performance at military treatment facilities identified as outliers for three quality of care measures, developed common quality policy for the Military Services, and used a performance management system to improve quality of care as directed by the Secretary of Defense.

However, recommendations from other DoD OIG reports remain open, such as recommendations to pursue collections on improper payments to TRICARE health care providers and on delinquent medical debts, and recommendations for establishing a multidisciplinary approach for obtaining the data necessary to make comprehensive DoD Suicide Event Report submissions.

DOD MILITARY HEALTH SYSTEM REFORM

The required transfer of responsibility for the military treatment facilities from the Military Services to the Defense Health Agency will be challenging for the DoD. Historically, the Services managed and operated the military treatment facilities. 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 treatment facilities.

According to the Under Secretary of Defense for Personnel and Readiness, the optimal end state is that under the direction of the Defense Health Agency, the Military Health System should be a fully integrated system of readiness and health care delivery. The Defense Health Agency will therefore have direct control over military treatment facilities, while the Military Services will retain control over their medical uniformed personnel and certain non-health care delivery functions, such as medical readiness.

Soldiers with the 131st Field Hospital, 528th Hospital Center, assess a mock patient. (U.S. Army photo)

According to the Under Secretary of Defense for Personnel and Readiness, substantial challenges remain in implementing such a major reform, such as maintaining a ready medical force and a medically ready force. Transitioning over 457 military treatment facilities worldwide to Defense Health Agency authority, direction, and control by October 1, 2021, will be difficult.

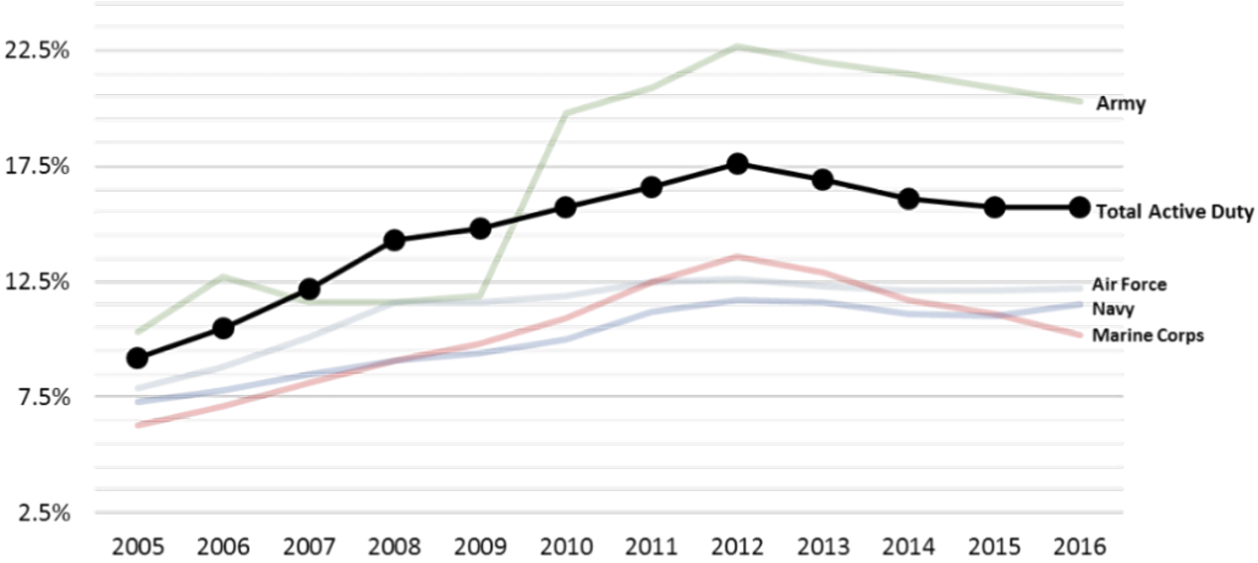
Establishing authority, direction, and control over military treatment facility health care must be carefully planned to make sure that clear authorities over Service medical personnel are properly established. For example, a May 2018 report by the DoD OIG determined that three Air Force military treatment facilities did not meet beneficiary demand for appointments because the Air Force Surgeon General did not have the authority to direct Air Force medical personnel in the military treatment facilities.[69] It is imperative that the Defense Health Agency has clear authority, direction, and control over each military treatment facility to be able to hold facility commanders accountable for providing appropriate medical care.

[69] Report No. DODIG-2018-111, "Access to Care at Selected Military Treatment Facilities," May 1, 2018.

BEHAVIORAL HEALTH

Identifying and providing care for behavioral health problems, such as suicides and opioid misuse, is a critical challenge for the DoD. As shown in Figure 7, diagnosed mental health disorders in the total population of active duty personnel increased by 6 percent from 2005 to 2016.

Figure 7. Percent of Patients with Any Mental Health Condition



Source: Military Health System Data Repository, October 2017.

Between 2012 and 2016, mental disorders were among the leading cause for hospitalization of active duty service members, accounting for between 12 to 15 percent of hospitalizations during those years. In 2017, the DoD reported that mental health disorders accounted for more hospital bed days than any other morbidity category among the active military components. In addition, mental health disorders accounted for the second most common reason for outpatient clinic visits by active duty service members in 2016.[70]

SUICIDE PREVENTION

Substance abuse, including opioids abuse, remains a significant readiness concern for the DoD, particularly due to its relationship with suicide. A recent Medical Surveillance Monthly Report study found that service members taking a combination of narcotics, antidepressants, and sedative medications have an increased risk for suicidal thoughts.[71]

Preventing suicides by DoD military personnel remains a challenge for the DoD. The DoD responded to a rise in active duty suicide deaths from 2008 to 2011 by establishing the Defense Suicide Prevention Office. This 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

[70] Defense Health Agency, "Medical Surveillance Monthly Report," Volume 25, Number 5, May 2018.

[71] Defense Health Agency, "Medical Surveillance Monthly Report," Volume 25, Number 6, June 2018.

issued DoD Instruction 6490.16, "Defense Suicide Prevention Program." The Instruction outlines processes for planning, directing, guiding, and resourcing to effectively develop and integrate the Suicide Prevention Program within the DoD.

Despite these efforts, the average suicide rate, across all Military Services, has remained consistent since 2013. The most recent Department of Defense Suicide Event Report (in 2016) shows the suicide mortality rate was 21.1 deaths per every 100,000 active duty service members. The 2016 suicide mortality rate for the Reserves, combined across all Military Services and regardless of duty status, was 22.0 deaths per 100,000 reservists. The 2016 suicide mortality rate for the National Guard, combined across the Air and Army Guard and regardless of duty status, was 27.3 deaths per 100,000 members of the Guard population. However, it is important to note that these rates are similar to the suicide mortality rate of the U.S. general population, after accounting for differences in the age and sex distributions between the U.S. general population and the military populations. The National Defense Authorization Act for FY 2015 expanded the DoD's collection of suicide data to include military family members. The DoD is now required to collect, report, and assess data regarding military family suicide. However, the current tracking systems, which are dependent on voluntary action by service members, provide incomplete mortality counts for suicides of military family members.

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.[72] However, recommendation remains open.[73] Without a comprehensive and complete DoD Suicide Event Report submission, it will be difficult for the DoD to conduct the trend or causal analysis necessary to develop effective suicide prevention policy and programs.

OPIOID MISUSE AND TREATMENT

The DoD faces also faces challenges in identifying and treating those DoD beneficiaries who are misusing opioids. Opioids are a class of drugs that include heroin, synthetic opioids such as fentanyl, and pain relievers available legally by prescription, such as oxycodone, hydrocodone, codeine, morphine, and many others.

The DoD must ensure that military health care providers prescribe opioids only to those patients who need them and adhere to guidelines that reduce the chance of addiction. 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. As a result, alternate pain relief therapies may be better long-term options for those patients. The DoD health care system must also be aggressive 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."

The DoD OIG is conducting several reviews related to opioid abuse. For example, the DoD OIG is auditing whether beneficiaries were overprescribed opioids at selected military treatment facilities.

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

[73] Compendium of Open Office of Inspector General Recommendations to the Department of Defense as of March 31, 2018, July 30, 2018.

The DoD OIG is also evaluating the DoD's management of opioid use disorder treatment, including whether the DoD has developed policies and programs to manage the treatment of opioid use disorder, identified and resolved barriers to opioid use disorder treatment, and established and implemented measures to improve opioid use disorder treatment.

DCIS, the criminal investigative arm of the DoD OIG, also conducts investigations related to opioid misuse. For example, DCIS investigated allegations that a Florida pain clinic physician illegally distributed controlled substances, including opioids and sleeping medication, from the clinic. The physician overprescribed these medications to several patients, including TRICARE beneficiaries, with no standard of care or medical necessity involved. The case resulted in the conviction of the physician and one other clinic employee for unlawful distribution of a controlled substance. Two additional clinic employees were convicted of conspiracy to distribute a controlled substance.

Additionally, DCIS investigated allegations that a physician was prescribing medically unnecessary opioid medication to his patients, including military members and their dependents. This investigation revealed a scheme between the physician, hired patient recruiters, and select patients to fraudulently prescribe opioids and then bill Government health benefit programs, including TRICARE, for the medications and associated examinations. The case resulted in the physician being convicted of multiple counts of structuring currency transactions.[74]

INCREASING HEALTH CARE COSTS

The DoD also must confront the challenges of containing health care costs and preventing health care fraud. Health care costs in the United States have grown dramatically, and Military Health System costs have been no exception. The DoD FY 2017 appropriations for health care were $33.5 billion, almost triple the FY 2001 appropriation of $12.1 billion. The DoD was appropriated $31.0 billion for the Defense Health Program in FY 2019.

HEALTH CARE FRAUD

One of the leading contributors to increasing health care costs is fraud. Health care fraud continues to be one of the top investigative priorities for DCIS. As of July 2018, DCIS had 510 open health care investigations. In FYs 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.

However, health care fraud schemes constantly evolve. As one vulnerability is addressed, corrupt individuals look for other vulnerabilities within the health care payment system to exploit. The DoD needs to be constantly vigilant to identify health care fraud schemes and ensure internal controls are in place to prevent fraudulent payments.

The DoD OIG has identified several categories of health care payments susceptible to fraud, including compound drugs and treatment for autism.

COMPOUND DRUGS

The DoD OIG continues to investigate fraud arising from the compound drug schemes that defrauded TRICARE in 2014 and 2015, before the Defense Health Agency changed its reimbursement policies for compound drugs. Compound drugs are developed from combining, mixing, or altering two or more ingredients to create a customized

[74] U.S. Department of Justice press release, November 18, 2016.

medication for an individual patient. Compound drug fraud schemes involved providers who prescribed compound drugs, including various pain and other creams, without examining or even meeting the patient; medication refills sent without the consent of the patient; kickbacks paid to providers, marketers, and patients; and grossly inflated bills for prescriptions. These schemes took advantage of a TRICARE reimbursement policy that allowed for full and immediate reimbursement of prescribed compound drugs.

For example, one compounding pharmacy and associated laboratory in Texas sought reimbursement for compounding pharmaceutical prescriptions that were not medically necessary, never received by the patient, and prescribed by physicians who had never actually examined nor had even seen the recipients of the medications. Service members were involved in the scheme by agreeing to accept kickbacks in exchange for the use of their personal identifying information to be used to facilitate additional billings to the Defense Health Agency for compound prescriptions. In this case, four individuals have been convicted of various crimes, $4.8 million is anticipated to be ordered back to the Defense Health Agency as restitution, and over $1 million in assets have been seized.

The Defense Health Agency eventually responded to rapidly increasing costs for compound drugs. In 2015, it changed its reimbursement policy for compound drugs in response to the significant fraud that occurred in 2014 and 2015. The change in policy reduced the Defense Health Agency's monthly costs for compound drugs from $497 million in April 2015 to $10 million in June 2015. As compared to payments for compound drugs of $1.6 billion in FY 2015, the DoD paid only $10.1 million for compound drugs for the entire FY 2017, demonstrating the dramatic effect of the changes in the reimbursement policy.

However, fraud and escalating costs can also occur in non-compound pharmaceuticals. A DoD OIG audit in November 2017 reported that the Defense Health Agency often took more than 6 months to implement new cost controls for drugs. The DoD OIG recommended that the Defense Health Agency implement procedures allowing expedited placement of controls to limit rapidly rising drug costs, and the Defense Health Agency took actions to implement the recommendation.[75]

FRAUDULENT AND UNSUPPORTED CLAIMS FOR AUTISM TREATMENT

The DoD OIG has also identified significant fraudulent activity and improper payments for Applied Behavioral Analysis services, which employs techniques and principles to encourage a meaningful and positive change in behavior. Applied Behavioral Analysis is a benefit offered by TRICARE for children with a diagnosis on the Autism Spectrum.

In a March 2018 audit report, the DoD OIG projected that the Defense Health Agency improperly paid $81.2 million of the total $120.1 million paid to Applied Behavioral Analysis companies in the TRICARE North Region for services provided in 2015 and 2016. The audit determined that documentation was insufficient to support the payments because the providers or companies did not provide supporting documentation or did not provide adequate details in the documentation to support their claims.[76]

The DCIS has also conducted investigations to address fraud within Applied Behavioral Analysis therapy and autism treatment. For example, one DCIS case occurring in South Carolina resulted in a provider company repaying the U.S. Government $8.8 million. The payment was made to resolve

[75] Report No. DODIG-2018-033, "Defense Health Agency Controls Over High-Risk Pharmaceutical Payments," November 16, 2017.

[76] Report No. DODIG-2018-084, "TRICARE North Region Payments for Applied Behavior Analysis Services for the Treatment of Autism Spectrum Disorder," March 14, 2018.

Filling a prescription at a Naval Branch Health Clinic Jacksonville; pharmacy. (U.S. Navy photo)

allegations that this company billed TRICARE and other Government programs for Applied Behavioral Analysis therapy services provided to children with autism in which the company either misrepresented the services provided or did not provide the services at all.

However, as the Defense Health Agency continues to make progress in controlling costs and tightening internal controls in certain areas, those intent on committing fraud seek other vulnerabilities to exploit. Emerging areas of concern for fraud within the DoD health care system involve genetic and DNA testing, vaccinations, durable medical equipment, and opioids. The Defense Health Agency needs to regularly and comprehensively review billing trends to look for the next fraud schemes and implement effective controls to help prevent payments for fraudulent claims.

PAYMENTS FOR SERVICES WITH LIMITED OR NO COST CONTROLS

The Defense Health Agency also pays for some services and products with limited or no cost containment controls. Cost containment controls could include establishing maximum allowable rates and obtaining authorizations prior to receiving the services or products. In an April 2018 report, the DoD OIG projected that the Defense Health Agency overpaid for breast pumps and parts by $16.2 million in 2016 because it had not used negotiated rates or set maximum allowable rates. For example, the Defense Health Agency paid $1,360 for a breast pump in Alaska while a local large retail store sold the same model for $221. Also, the Defense Health Agency paid more than the highest rate of Medicaid agencies for approximately 57 percent of breast pump replacement parts, including paying $138 for a single bottle, which was over 20 times the highest Medicaid reimbursement rate of $6.62.[77] The DoD OIG began an audit in March 2018 to review other items that may not have cost containment controls, such as vaccinations and birth control devices.

COLLECTIONS

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

For example, the DoD OIG issued six reports from August 2014 through January 2017 related to collections from non-DoD beneficiaries, which concluded that military treatment facilities did not actively pursue collections from non-DoD beneficiaries for 129 accounts, valued at $13.1 million, of the 145 accounts the DoD OIG reviewed.[78] The DoD OIG is performing

[77] Report No. DODIG-2018-108, “TRICARE Payments for Standard Electric Breast Pumps and Replacement Parts,” April 25, 2018.

[78] Report No. DODIG-2014-101 “Delinquent Medical Service Accounts at Brooke Army Medical Center Need Additional Management Oversight,” August 13, 2014; Report No. DODIG-2014-112 “Delinquent Medical Service Accounts at William Beaumont Army Medical Center Need Additional Management Oversight,” September 16, 2014; Report No. DODIG-2015-087 “Delinquent Medical Service Accounts at Naval Medical Center Portsmouth Need Additional Management Oversight,” March 4, 2015; Report No. DODIG-2015-179 “Delinquent Medical Service Accounts at David Grant U.S. Air Force Medical Center Need Additional Management Oversight,” September 24, 2015; Report No. DODIG-2016-079” Delinquent Medical Service Accounts at Landstuhl Regional Medical Center Need Additional Management Oversight,” April 28, 2016; Report No. DODIG-2017-045 “Medical Service Accounts at U.S. Army Medical Command Need Additional Management Oversight,” January 27, 2017.

followup work on those six reports and reviewing reimbursements for health care provided to Department of Veterans Affairs patients and collections from insurance providers.

ELECTRONIC HEALTH RECORDS

The security of electronic health records and integration of those records with the Department of Veterans Affairs also is an important challenge for the DoD. Electronic health records can contribute to improved quality of care, more efficient care, and more convenient care. These records contain sensitive medical history and information about a patient's health, including symptoms, diagnosis, medications, lab results, vital signs, immunizations, and reports from diagnostic tests, and their disclosure could have serious consequences. The security and availability of those records is critical to the patients' privacy and to health care providers' ability to treat the patients.

SECURITY OF PATIENT HEALTH INFORMATION

According to a report from the Identify Theft Resource Center, a non-profit organization that supports victims of identity theft and educates the public about identity theft, data breaches, cyber security, fraud, and privacy issues, there were 1,579 data breaches in 2017 from business, health and medical, financial, education, and Government and military institutions, exposing more than 179 million records. According to another report from the health compliance analytics company Protenus, over 5.5 million patient records were breached in 2017 across the United States.[79] According to a July 2018 article by the HIPAA Journal, the average cost of a data breach in the United States is $7.91 million, and health care data breaches represent the highest costs for breaches at an average of $408 per record.

These risks affect the DoD also. For example, the DoD OIG identified in 2017 that the Defense Health Agency and Army officials did not consistently implement effective security protocols to protect systems that stored, processed, and transmitted electronic health records and electronic patient health information. Specifically, Defense Health Agency and Army officials did not enforce the use of Common Access Cards to access five electronic health record systems and did not comply with DoD password complexity requirements for three systems. In addition, the DoD OIG reported that system and network administrators at three Army facilities did not consistently mitigate known vulnerabilities affecting Army networks, protect stored data for five systems, and grant user access to the seven systems based on the user's assigned duties.[80]

A May 2018 DoD OIG audit had similar findings for the Navy and Air Force electronic health records at five facilities. In addition to many of the problems noted in the DoD OIG report on the Army, the DoD OIG audit reported that system and network administrators did not properly configure electronic health record systems to lock after 15 minutes of inactivity and did not consistently review system activity reports to identify unusual or suspicious activities and access. In short, the DoD needs to ensure adequate controls exist on its health care systems to reduce the risk of compromising DoD patients' sensitive health care information.[81]

[79] Protenus "2017 Breach Barometer Annual Report," 2017.

[80] Report No. DODIG-2017-085, "Protection of Electronic Patient Health Information at Army Military Treatment Facilities," July 6, 2017.

[81] Report No. DODIG-2018-109, "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities," May 2, 2018.

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 2017 directed the DoD and the Department of Veterans Affairs to integrate their electronic health records and gave the departments 5 years to meet this requirement. The Secretary of the Department of Veterans Affairs announced in 2017 that the Department of Veterans Affairs would acquire the same system as the DoD. In May 2018, the Department of Veterans Affairs established a $10 billion contract to overhaul its electronic health records system to make it compatible with the DoD's records.

In FY 2019, the DoD OIG plans to review the DoD and the Department of Veterans Affairs electronic health care systems to determine whether they allow for full interoperability of health care information between DoD, Department of Veterans Affairs, and private sector health care systems.

In summary, providing comprehensive and cost-effective health care to the DoD's 9.4 million beneficiaries will continue to be a significant challenge for the DoD. The DoD must carefully plan the transfer of authority, direction, and control of the military treatment facilities to the Defense Health Agency. The DoD must also continue to seek efficiencies to control costs without undermining timely access to quality health care, which is not an easy task. At the same time, the DoD needs to address behavioral disorders and aggressively seek to reduce the number of suicides within the military while also identifying and treating patients suffering from opioid addiction. Finally, the DoD must protect patient health information within its electronic health records and work with the Department of Veterans Affairs to integrate electronic health records between the departments.

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
Defense Hotline 1.800.424.9098