INSPECTOR GENERAL

U.S. Department of Defense

Top DoD Management Challenges

Fiscal Year 2018

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

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

TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE DEPARTMENT OF DEFENSE

Public Law 106-531, the "Reports Consolidation Act of 2000," requires each Inspector General (IG) to prepare an annual statement that summarizes what the IG considers to be the "most serious management and performance challenges facing the agency" and also requires the IG to assess the Agency's progress in addressing those challenges. The law states that "agency head may comment on the IG's statement, but may not modify the statement." By statute, the IG's statement must 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 challenges outlined in this statement were identified based on a variety of factors, including DoD OIG oversight work, research, and judgment; oversight work done by other DoD components; oversight projects conducted by the GAO; and input from DoD officials. While we also 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 as a research and planning tool to identify areas of risk in the DoD operations. It is forward looking and outlines the most significant management and performance challenges facing the DoD now and in the future.

This year's summary of challenges is for FY 2018 rather than for FY 2017. In previous years, the document's title contained the year of the DoD financial statement that included this report. While last year's report was labelled as FY 2016, this year we labelled the document as the top management challenges for FY 2018 to reflect its forward-looking orientation. Therefore, no document is labelled FY 2017 summary of management challenges, but there has been no gap in our top management challenges documents.

As reflected in this document, the FY 2018 top 10 management and performance challenges are:

1. Countering Strategic Challenges: North Korea, Russia, China, Iran, and Transnational Terrorism
2. Addressing Challenges in Overseas Contingency Operations in Iraq, Syria, and Afghanistan
3. Enabling Effective Acquisition and Contract Management
4. Increasing Cyber Security and Cyber Capabilities
5. Improving Financial Management
6. Maintaining the Nuclear Enterprise
7. Optimally Balancing Readiness, Modernization, and Force Structure
8. Ensuring Ethical Conduct
9. Providing Effective, Comprehensive, and Cost Effective Health Care
10. Identifying and Implementing Efficiencies in the DoD

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

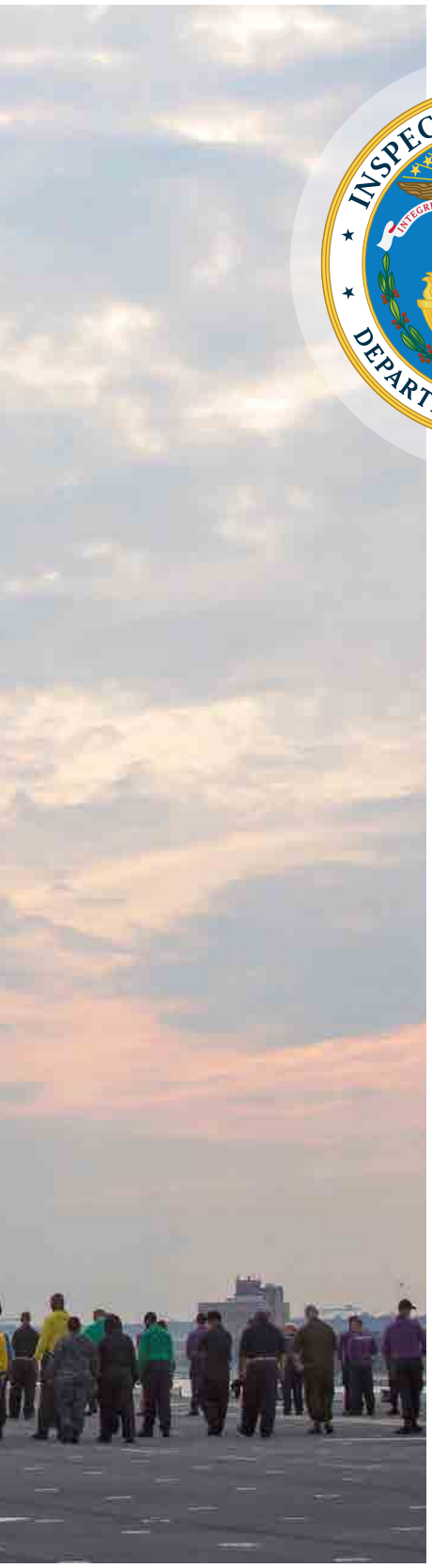
These challenges are not listed in order of importance or by magnitude of the challenge. All are critically important management challenges.

We look forward to working with the DoD to help address these important challenges.

Glenn A. Fine
Acting Inspector General


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

U.S. marines with the 26th Marine Expeditionary Unit, and sailors from the USS Kearsarge, conduct a foreign object and debris walk-down during departure aboard the Kearsarge at Naval Station Norfolk, Virginia. (U.S. Marine Corps photo)



Summary of Management and Performance Challenges Facing the DoD

FISCAL YEAR 2018

Camp Humphreys, Republic of Korea: Soldiers from 1st Battalion, 5th Cavalry Regiment, 2nd Armored Brigade Combat Team, 1st Cavalry Division, secure cargo lines to a CH-47 Chinook during sling load training. (U.S. Army photo)

Challenge 1: Countering Strategic Challenges: North Korea, Russia, China, Iran and Transnational Terrorism

Addressing evolving global threats presents a significant challenge for the Department of Defense (DoD). State and non-state actors present security challenges that have destabilized the post-Cold War international order, and the DoD must confront these challenges in close coordination with U.S. allies and DoD interagency partners.

In a recent interview, General Joseph Dunford, Chairman of the Joint Chiefs of Staff, identified five significant global strategic challenges to U.S. interests: North Korea, Russia, China, Iran, and violent extremism or transnational terrorism. General Dunford noted that the DoD does not have "the luxury today of singling out one challenge." He stated that, from a capability perspective, Russia presents the greatest mid-to-long-term threat to U.S. national security, but from an urgency perspective, North Korea poses the top challenge.

NORTH KOREA

"The most urgent and dangerous threat to peace and security [in the world] is North Korea," Secretary of Defense James Mattis said in a June 12, 2017, statement before the House Armed Services Committee, and that assessment is even more concerning today. North Korea's aggressive pursuit of nuclear weapons and ballistic missile technologies, and its role in their proliferation, presents a growing strategic threat to U.S. forces in the region and to the U.S. mainland, as well as to North Korea's neighbors, South Korea and Japan. The United States is pressuring North Korea to stop the development of its nuclear weapons and ballistic missiles programs.

However, North Korea has continued to develop its nuclear weapons and ballistic missile programs. Throughout 2017, North Korea conducted ballistic missile tests, including launching intercontinental ballistic missiles. Publicly reported analysis indicated that North Korea's intercontinental ballistic missiles have the technical capability to reach the entire State of Alaska and parts of the U.S. mainland. On September 3, 2017, North Korea claimed to have tested a thermonuclear bomb—the blast was recorded by the U.S. Geological Survey as a human-made, 6.3-magnitude seismic event, which was far larger than previous North Korean nuclear weapon tests. Moreover, the Defense Intelligence Agency stated that North Korea is capable of creating a miniaturized nuclear device to use as a missile warhead. In addition to its nuclear capability, North Korea has deployed a significant ground force along its border with South Korea, maintains a chemical and biological warfare capability, and can strike South Korea's capital, Seoul, with a formidable array of artillery and rockets.

Republic of Korea Marine Amphibious Assault Vehicles eject smoke clouds during a Korean Marine Exchange Program exercise. (U.S. Marine Corps photo)

According to the 2017 Defense Posture Statement, the DoD has developed a comprehensive set of alliance capabilities to deter and counter the North Korean threat. The DoD maintains 80,000 military personnel and a significant ground, air, and sea force capability in and around South Korea and Japan. It conducts regular joint military exercises with South Korea and Japan, with whom the United States has security treaty commitments. The United States and South Korea have also agreed to deploy a Terminal High-Altitude Area Defense missile capability to South Korea to defend South Korea and alliance forces from North Korea's ballistic missile threats.

Speaking in Seoul on August 14, 2017, General Dunford stated that the military directly supports U.S. diplomatic and economic efforts to resolve the crisis with North Korea. He also stated that the DoD provides viable military options in the event that deterrence fails. However, General Dunford noted that armed conflict with North Korea would lead to a level of casualties not experienced since World War II. Similarly, Secretary of Defense Mattis has said that a military confrontation with North Korea would be "catastrophic."

The United States continues to reach out to China, North Korea's closest ally and trading partner, to convince China to pressure North Korea to halt its nuclear program. In 2017, the United States imposed additional economic sanctions on North Korea, and China agreed to United Nations' limitations on future imports from North Korea. However, North Korea has rejected formal negotiations and expressed no intention to de-nuclearize or stop developing ballistic missiles. North Korean leader Kim Jong-un reportedly believes that maintaining North Korea's nuclear and ballistic missile capability is necessary to deter the threat that North Korea's perceived enemies, principally the United States, pose to his regime.

Given the level of concern over North Korea's statements and actions, the DoD faces several challenges: maintaining a high level of military readiness and deterrence; supporting the U.S. and allied strategy to seek diplomatic negotiations while imposing economic sanctions; and, if required, executing a military option.

RUSSIA

In June 2017, Secretary of Defense Mattis testified about a resurgent and more aggressive Russia, which objects to key aspects of the post-Cold War international order by taking multiple actions against other countries, including challenging the sovereignty of nations on its borders. In recent years, Russia has clashed with the United States over the 2014 revolution in Ukraine that ousted its pro-Russian president, the subsequent revolt of the president's supporters and Russia's intervention in Eastern Ukraine and seizure of Crimea. Russia has also opposed the expansion of the North Atlantic Treaty Organization (NATO) into the Baltic countries of Estonia, Latvia, and Lithuania, which brought U.S. and other NATO allies' military forces to Russia's border.

In the Syrian civil war, Russia intervened on behalf of the Government of Syria. As a result, U.S. forces conducting operations to defeat the Islamic State of Iraq and Syria (ISIS) in Syria operate in close proximity to Russian military forces. The Defense Intelligence Agency has reported that Russia's military intervention in Syria changed the dynamic of the conflict, bolstered the government of Syria, and ensured that resolution to the conflict is impossible without Russia's agreement.

In addition to having a formidable nuclear force, Russia has significantly advanced its conventional and unconventional military capabilities. The Russian military has enhanced its ground, sea, and air strategic and operational forces; deployed an asymmetric, unconventional warfare capability; and expanded its covert use of cyber and information operations.

In Europe, the United States and its NATO allies have reinforced their military capabilities. Through the European Deterrence (formerly Reassurance) Initiative, announced in June 2014, the DoD has sought to build its European allies and partners' capability to enable a quicker and more robust response to support NATO's common defense. The European Deterrence Initiative augmented the presence of U.S. forces in Eastern Europe through increased unit rotations and pre-positioned materiel in strategic locations. In addition, other NATO countries have deployed military units to the Baltic countries and to Romania, Poland, and Bulgaria. NATO is also enhancing its Response Force into a flexible and mobile, 40,000-troop joint force composed of land, sea, air, and special operations units, and is conducting increased training and joint exercises with partner countries' security forces. The total U.S. investment in the European Deterrence Initiative has quadrupled over the past year, from $789 million in FY 2016 to $3.4 billion for FY 2017.

However, challenges remain to the rapid deployment of U.S. and other NATO forces in response to potential Russian aggression. For example, a recently released DoD OIG evaluation noted that, according to senior U.S. European Command officials, obstacles to a timely military ground response by U.S. and other NATO forces to a Russian military attack include a lack of compatible infrastructure and movement agreements between NATO countries and experience controlling military convoys.

In Syria, the United States and Russia have established communication mechanisms to de-conflict operations and avoid conflict. On June 19, 2017, after U.S. forces shot down a Syrian fighter aircraft, the Russian defense ministry issued a statement that "all kinds of airborne vehicles, including aircraft and UAVs of the international coalition detected to the west of the Euphrates River will be tracked by the Russian SAM [surface-to-air missiles] systems as air targets." Despite the heightened tension resulting from these actions the United States and Russia have sought to deconflict air zones in Syria. To further reduce the potential for military confrontation, in agreement with the United States and other concerned countries, Russia has established and is monitoring de-escalation zones in southern Syria.

U.S. Marine Corps KC-130 J Hercules aircraft with Marine Aerial Refueler Transport Squadrons. (U.S. Marine Corps photo)

A U.S. Navy Boatswain's Mate directs an MH-60S Seahawk helicopter to the flight deck aboard the Littoral Combat Ship USS Coronado. (U.S. Navy photo)

Strategically, Russia's actions indicate that it has established an enduring presence in Syria to maintain its warm-water naval port and to project power regionally. As a United Nations Security Council member, Russia also influences a wide range of other international issues, including the fight against terrorism. The potential exists for military confrontation in these areas; the DoD needs to maintain an effective military deterrence capability and dialogue with the Russian military.

CHINA

Already a nuclear weapons power, China continues to further build its conventional military capacity. In recent years, China's military has improved its offensive and defensive capabilities in the areas of ballistic and cruise missiles, counter-space and offensive cyber capabilities, electronic warfare systems, surface and submarine warfare capabilities, and its air force. In 2017, Chinese military expenditures increased another 7 percent.

In recent years, China has undertaken aggressive expansionist activities in the Asia-Pacific region. In the South China Sea, China has increased tensions with its regional neighbors and with the United States by creating artificial islands in maritime territory claimed by multiple neighboring countries. China is militarizing these artificial islands, using them to gain control over the South China Sea's air and sea lanes, as well as its extensive underwater natural resources. The Chinese government refuses to accept an international arbitration tribunal ruling that China does not have the maritime territorial sovereignty it claims over the South China Sea.

In the East China Sea, China declared an air-defense identification zone in 2013 in which it requires the identification, location, and control of foreign aircraft over what it considers its sovereign airspace or water. China's self-declared air-defense identification zone extends over the Japanese-owned Senkaku Islands. Neither Japan nor the Unites States recognize China's claims. In addition, the Japanese government has expressed concern over China's almost daily intrusions into Japanese air space in 2017.

In response to China's actions, the DoD continues to fly, sail, and operate throughout the South China and East China Seas, in accordance with international law, to demonstrate its commitment to freedom of navigation and overflight. Furthermore, the DoD is working to enhance

the alliance relationships the United States has with countries in the Asia-Pacific region in support of regional stability and U.S. strategic interests. In 2014, the United States signed the Enhanced Defense Cooperation Agreement with the Philippines, which increased U.S. access to Philippine military bases, and provided for donations of U.S. maritime vessels to the Philippine military and joint training exercises. In 2015, the United States announced the Southeast Asia Maritime Security Initiative, a 5-year, $425 million project to enhance partner capabilities and collaboration among Southeast Asia countries, including the Philippines, Vietnam, Indonesia and Malaysia.

To expand its global maritime influence, China established its first overseas military base in Djibouti in the Horn of Africa. Djibouti is strategically located on the Strait of Bab el-Mandeb between the Red Sea and the Gulf of Aden where approximately 20,000 ships and 20 percent of global exports traverse yearly. China is building a facility that will house up to 10,000 Chinese military personnel and provide a logistics base for its navy.

U.S. intelligence analysts assert that this is a critical period in which China plans to test U.S. military and political resolve. The United States and its allies will need to have a clear response to protect U.S. interests.

IRAN

Iran continues to pose a significant global security threat to the United States given its regional power ambitions and potential development of a nuclear weapons capability. For example, according to the 2017 Defense Posture Statement, Iran supports the Assad regime in Syria, backs the militant Shi'a terrorist organization Hezbollah in Syria and Lebanon, and contributes to disorder in Yemen. In July 2017, Michael Pompeo, the Director of the Central Intelligence Agency, described Iran's use of proxy forces—Hezbollah in Lebanon and Syria and Shiite militias in Syria and Iraq—to establish

U.S. Marine Corps joint terminal attack controllers communicate with an MV-22 Osprey during takeoff. (U.S. Marine Corps photo)

Iranian dominance along the newly forming Shiite Crescent stretching from Beirut to Tehran. Iran's ally Hezbollah claims it is "close to achieving this goal." These actions directly threaten Israel and other U.S. allies in the Middle East.

In 2015, Iran, the P5+1 (China, France, Russia, the United Kingdom, the United States, and Germany), and the European Union agreed to the Joint Comprehensive Plan of Action, which seeks to ensure that Iran's nuclear program is exclusively peaceful in exchange for the United States, the European Union, and the United Nations lifting economic sanctions. Under U.S. law, the State Department must notify Congress every 90 days of Iran's compliance with the Joint Comprehensive Plan of Action.

Because of Iran's continued testing of ballistic missiles and direction of hostile actions in the region, Congress passed legislation in 2017 imposing new economic sanctions against Iran. The State Department also stated Iran has expanded activities that undermine stability, security, and prosperity in the Middle East, such as supporting the terrorist groups Hezbollah, Hamas, and Palestinian Islamic Jihad. Iran also supports the government of Syrian President Bashar

al-Assad, despite his atrocities against his own people. In Yemen, Iran has provided the Houthi rebels with advanced weaponry, which the rebels have used to attack Saudi Arabia, that threatens freedom of navigation in the Red Sea. Iran is also testing and developing ballistic missiles, in defiance of U.N. Security Council Resolutions.

In response to the new economic sanctions, President Hassan Rouhani of Iran warned that it could start its nuclear program "within hours." Iran's parliament also responded by voting overwhelmingly in favor of legislation to increase the budget for the country's ballistic missile program and the Revolutionary Guard's external operations arm, the Quds Force.

The United States is working with its allies in the Middle East to contain Iranian aggression and influence. In May 2017, the State Department announced a large arms package—$110 billion of defense equipment and services—for Saudi Arabia and other U.S. allies in the Gulf region to support their long-term security "in the face of the malign Iranian influence and Iranian-related threats." The State Department re-designated Iran 2 months later as a State Sponsor of Terrorism, a designation it has held since 1984.

Meanwhile, Iran has taken significant steps to increase its influence in Iraq. Speaking at the Aspen Security Forum in July 2017, Iraq's Ambassador to the United States praised Iran's provision of critical supplies in the fight against ISIS. He stated that Iran has enhanced its influence today in Iraq because other Arab nations were missing when Iraq needed their support against ISIS. Recently, however, Saudi Arabia has initiated talks with Iraq pursuant to an economic agreement to help reconstruct the country post-ISIS.

Notwithstanding its current support of Iraq to defeat ISIS, Iranian influence in Iraq could make it more difficult for Iraq to assert its sovereignty and maintain its independence as it attempts to reconcile competing sectarian interests and establish stable governance. Currently, Iranian-backed Shia Popular Mobilization Forces of considerable size and reach operate in Iraq to support the anti-ISIS campaign. The Government of Iraq has officially incorporated some of these Shia Popular Mobilization Forces into the Iraqi Security Forces. Iran has warned the Iraqi government not to weaken these Iranian-backed Shia forces, which, so far, have avoided conflict with U.S military personnel.

A U.S. Marine Corps humvee enters the beach to board a Landing Craft Utility 1651 in order to transfer personnel and equipment. (U.S. Navy photo)

TRANSNATIONAL TERRORISM

Countering transnational terrorism remains a key U.S. national security challenge. Despite heightened U.S., European, and other allies' focus on combatting terrorism following al-Qaeda's attack on the United States on September 11, 2001, terrorist organizations have proliferated throughout the world and present a global threat.

These terrorist organizations include Boko Haram in Nigeria and Chad; al-Shabab in Somalia; al-Qaeda in Syria, Yemen, and Afghanistan; the Islamic Maghreb in North Africa; and ISIS in Iraq, Syria, Libya, Afghanistan, Egypt, and the Philippines. Tens of thousands of young Muslims have migrated across nation-state borders to join the terrorist organizations, especially into Syria and Iraq, with an estimated 3,000 – 5,000 from Western Europe and the United States alone.

These terrorist organizations continue to pose a significant destabilizing force. ISIS, in particular and those it has inspired, has carried out multiple terrorist attacks in Europe and in the United States.

ISIS recently directed its adherents to attack tourists anywhere in the world using a SUV or truck as its principal weapon.

While each terrorist organization has a unique history, procedures, and motivation based on local grievances, the common thread linking them is adherence to interpretations of extremist versions of Islam that justify violence.

However, the so-called Islamic Caliphate established by ISIS in Iraq and Syria is on the verge of defeat. In June 2017, after a 9-month battle, Iraqi Security Forces, backed by U.S. and Coalition air and special operations forces, liberated Mosul, Iraq's second largest city. In August 2017, Kurdish and Arab military forces, supported by U.S. and Coalition air and special operations forces, entered Raqqa, Syria, the "capital" of the so-called Islamic Caliphate.

However, the military success against ISIS in Syria and Iraq is driving some of the surviving ISIS fighters into other ungoverned spaces around the world, fueling the spread of transnational terrorism. The prospect of radicalized foreign fighters returning to their home countries to further spread ISIS influence and stage attacks poses a significant challenge to the United States and its allies.

Special Presidential Envoy for the Global Coalition to Counter ISIS, Ambassador Brett McGurk, stated that the long-term key to preempting ISIS and other terrorist attacks after the military phase of defeating the so-called Islamic Caliphate in Iraq and Syria is to share information among the U.S. coalition of 69 countries. He noted that this will require increased emphasis on law enforcement and intelligence gathering to build a global database of known terrorists.

In addition to Iraq and Syria, the DoD is conducting military operations with allies against terrorist groups throughout the world, especially in several fragile or failed states. For example, General Raymond A. Thomas III, Commander, U.S. Special Operations Command, recently stated that forces under his command, along with local proxies, eliminated approximately 1,500 ISIS terrorists in Libya after ISIS established a presence there in 2015. He said that his teams operate globally against terrorists, anywhere a significant threat exists. In addition, U.S. forces are providing critical support and assistance to the Philippine Security Forces as they combat ISIS in the southern region of Mindanao.

The DoD is also undertaking increased security cooperation initiatives in the Middle East and in other regions to enhance our alliances and build our partners' military capability to defend themselves against Islamist extremist terrorist attacks. For example, on May 15, 2017, the DoD announced a new bilateral defense cooperation agreement with the United Arab Emirates on a range of shared regional security threats, including the ongoing Iranian, Al-Qaeda, or ISIS-backed instability in Yemen and Libya, and the campaign to defeat ISIS in Iraq and Syria. The State Department also announced that the United States and Saudi Arabia are embarking on a number of new initiatives "to counter violent extremist messaging," which will include opening a new Global Center for Combatting Extremist Ideology. A recent DoD OIG evaluation reported that DoD and State Department global efforts to build partner-country counterterrorism capacity through training and equipping programs have reached over 70 nations through the congressionally funded Section 2282 program.

In summary, transnational terrorism presents a long-term global threat. International institutions and governments must work to resolve the underlying conditions that led to the rise and continued propagation of violent extremism. These conditions result from the collapse of state economies and effective governance, sectarian and religious civil wars, and political and social alienation among the young in the countries in which the ideology has taken root.

Iraqi federal police load artillery in support of the fight against ISIS near Hawijah, Iraq. (U.S. Army photo)

Challenge 2: Addressing Challenges in Overseas Contingency Operations in Iraq, Syria, and Afghanistan

The U.S. Government is engaged in two overseas contingency operations: (1) Operation Inherent Resolve (the effort to degrade and defeat the Islamic State of Iraq and the Levant [ISIS] in Iraq and Syria); and (2) Operation Freedom's Sentinel (the effort to build partner capacity within the Afghan National Defense and Security Forces [ANDSF], and to counter terrorism in Afghanistan). Conducted in the U.S. Central Command Area of Responsibility, both operations are focused on building capacity for each host nation to provide for its own security, while addressing challenges to U.S. security interests from both state and non-state actors.

The U.S. Central Command Area of Responsibility is a region of 20 nations, with more than 550 million people from over 20 ethnic groups. It lies at the intersection of sea-lanes, flight corridors, pipelines, and overland routes supporting regional and global economic networks. Many threats in the region go beyond state borders, and occur on land, sea, and in cyberspace. The region remains an epicenter for terrorism and violent extremism, and according to General Votel, the Commander of U.S. Central Command, accounts for almost 80 percent of terrorism incidents worldwide.

General Votel testified before the House Armed Services Committee in March 2017 that the root causes of regional instability include ethnic and sectarian hostility, reduced government services and lack of economic opportunity, unemployed youth populations susceptible to radical ideologies, and expanding ungoverned areas. General Votel explained that violent extremist organizations, such as ISIS and al Qaeda, exploit this instability to foment unrest, challenge governments, and threaten U.S. national interests.

The internet can facilitate the recruitment of violent extremists. Admiral Mike Rogers, Commander of U.S. Cyber Command, testified before the Senate Armed Services Committee in May 2017 that ISIS employs cyber capabilities to recruit followers and solicit contributions in the West. Closer to the Middle East, ISIS employs the internet to boost morale among its fighters, frighten opponents, and promote its false narrative of Sunni fundamentalism.

According to General Votel, the DoD and its Coalition partners are pursuing a strategy of working "by, with, and through" partners in Iraq, Syria, and Afghanistan to prevail over adversaries in the region. The DoD's challenge in this region is to contribute to a whole-of-government approach that addresses the regional and growing global threats, protects human and financial investments, and promotes the national security and foreign policy of the United States and its partner nations. General Votel stated that military operations alone cannot address the root causes of instability, but can help create necessary conditions for progress.

An F-16CM Fighting Falcon pilot assigned to the 79th Fighter Squadron returns home to Shaw Air Force Base, South Carolina, after a six-month deployment in support of Operation Freedom's Sentinel. (U.S. Air Force photo)

OPERATION FREEDOM'S SENTINEL

The DoD has been fighting in Afghanistan for nearly 16 years. The direct combat mission of Operation Enduring Freedom began in October 2001 and transitioned to the North Atlantic Treaty Organization Resolute Support mission in January 2015. According to CENTCOM, Resolute Support provides training, advice, assistance, and equipment to Afghan security forces and institutions as part of a broader engagement by the international community to ensure that Afghanistan is not a safe haven for terrorism. Under Operation Freedom's Sentinel, the DoD has two complementary missions: (1) participate in Resolute Support with North Atlantic Treaty Organization partners and allied nations to train, advise, assist, and equip the ANDSF; and (2) conduct U.S. counterterrorism operations against al Qaeda, the Islamic State of Iraq and Syria-Khorasan (ISIS-K), and their affiliates in Afghanistan.

The DoD reports that the ANDSF has shown increased capability, but the ANDSF still suffers from leadership and logistical problems, and its casualty rates remain high. Despite significant U.S. and international support to Afghanistan, DoD officials recently described the fight as a "stalemate," and have declared that "we are not winning" in Afghanistan. In August 2017, the U.S. announced a revised strategy for Afghanistan and South Asia, emphasizing preventing safe havens for terrorists and preventing terrorists from obtaining nuclear weapons and materials. The strategy relies on five principles:

- adopt a conditions-based approach;
- integrate diplomatic, economic, and military power;
- persuade Pakistan to deny safe haven to terrorists;
- partner with India to assist in stabilizing Afghanistan;
- and provide U.S. warfighters the resources and rules of engagement necessary for success.

However, the DoD recognizes the need for a regional strategy that includes Pakistan and India, as well as addresses persistent challenges with ANDSF capability gaps and long-term DoD support. The U.S. strategy also seeks to integrate various elements of U.S. power to make possible a political settlement that includes elements of the Taliban in Afghanistan.

REGIONAL INFLUENCES ON THE INSURGENCY AND AFGHAN GOVERNANCE

In its June 2017 report "Enhancing Security and Stability in Afghanistan," the DoD identified Pakistan as the most influential external actor affecting Afghan stability. According to this report, although Pakistani military operations have disrupted some militant sanctuaries, Pakistan plays a destabilizing role in Afghanistan, driven in part by its India-centric regional policy objectives and because of the support and refuge it provides to multiple militant groups within Pakistan. In addition, General John W. Nicholson, the Commander of U.S. Forces-Afghanistan, has identified the use of ungoverned sanctuaries outside of Afghanistan by terrorists and Afghan insurgents as the single greatest external factor that could cause failure of the 39-nation North Atlantic Treaty Organization-led coalition in Afghanistan. To address this concern, the DoD withheld $400 million in FY 2016 military funding intended for Pakistan, and an additional $50 million in FY 2017 funding, pending certification that Pakistan is taking sufficient action in denying safe haven to insurgent groups.

In addition, the DoD has reported that Russia, China, and Iran are seeking to develop greater relationships with the Afghan government and the Taliban. General Nicholson has criticized both Russian and Iranian support to the Taliban and rejected the "false narrative" that such engagements were in the pursuit of peace.

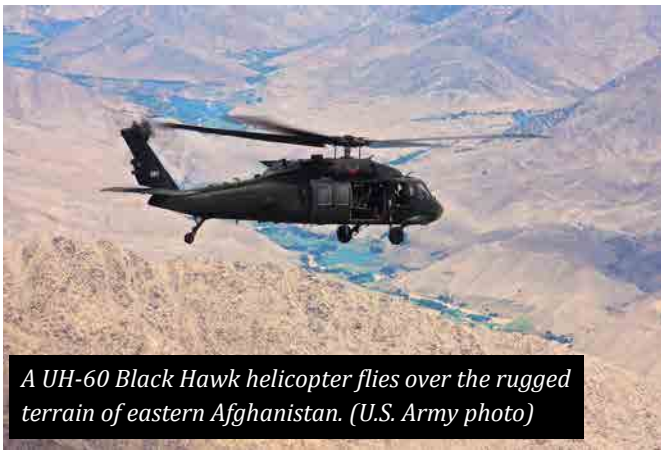
LEADERSHIP CHALLENGES AND CORRUPTION WITHIN THE ANDSF

Poor leadership and endemic corruption have weakened the fighting effectiveness of Afghan forces and adversely affected retention of personnel. This year, Afghan President Ashraf Ghani directed the development of a 4-year "Road Map" to reform and strengthen the ANDSF in the key areas of fighting capability, leadership development, unity of command, and countering corruption.

However, DoD OIG and Special Inspector General for Afghanistan Reconstruction reports have continued to identify corruption and mismanagement in Afghanistan contracting operations, failures in budgeting and execution, a lack of transparency and internal oversight, and failures in governance and rule of law. While the DoD has implemented measures, such as Conditionality Agreements and Bilateral Financial Commitment Letters, to promote improved ANDSF management practices, continued corruption plagues the ANDSF.

For example, a DoD OIG report noted that the Afghan government was not penalized for repeated commitment letter violations regarding U.S. direct assistance funding. The DoD has attempted to place the management of fuel procurement under the responsibility of the Ministry of Defense, but corruption and mismanagement of operations and facilities caused President Ghani to cancel these efforts and return full administration to the U.S. Government.

The Afghan government has taken some positive steps to attempt to address corruption issues. In June 2016, the Afghan government opened its Anti-Corruption Justice Center as an independent authority to enforce the law and prosecute corruption crimes. Since its inception, the Anti-Corruption Justice Center has completed 14 major corruption cases involving 38 defendants, including four from the Ministry of Interior, one from the Ministry of Defense, and the rest from other ministries or private sector entities.



A UH-60 Black Hawk helicopter flies over the rugged terrain of eastern Afghanistan. (U.S. Army photo)

Soldiers of the U.S. Army's 3rd Infantry Division load bags for soldiers deploying to Afghanistan in support of Operations Resolute Support and Freedom's Sentinel. (U.S. Army photo)

ANDSF CAPABILITY GAPS

In June 2017, the DoD reported that the ANDSF has progressed in planning combat operations and integrating combat enablers, such as integrating air and ground forces and intelligence collectors into those operations. However, persistent gaps in ANDSF capabilities remain, many of which require continued U.S. support. For example, according to the report Afghan intelligence collection for targeting and battle assessments is being enhanced through remotely piloted aircraft and other technical tools, but the Afghans are unable to maintain the equipment. In addition, a lack of trust between the Afghan Ministries of Defense (military) and Interior (police) inhibits intelligence sharing. Maintenance and training strategies intended for adoption by the ANDSF have not met established milestones and have faced challenges caused by Afghan illiteracy, a lack of leadership, and management shortcomings.

In addition, according to the DoD report, the Afghan Air Force is using the Super Tucano light attack (fixed-wing) aircraft to attack targets of strategic significance, although technical limitations currently limit the use of precision guided munitions. Meanwhile, the decreasing availability of non-North Atlantic Treaty Organization Mi-17 helicopters is severely limiting Afghan troop support and casualty evacuation. The planned introduction of U.S.-type helicopters presents a long-term solution but does not resolve the immediate shortfalls in aerial transport. To assess these challenges, the DoD OIG is currently conducting an assessment of U.S. and Coalition efforts to train, advise, assist, and equip the Afghan Air Force.

The DoD continues efforts to build critical capabilities and to implement technical support systems within an underdeveloped ANDSF. However, the DoD has reported that these efforts are hindered by the limited capability of the Ministry of Defense to execute resource and personnel management, as well as procurement planning. In addition, the Afghan National Police has significant shortcomings in training, equipping, and employing its personnel and is several years behind the Army in its development.

LACK OF RELIABLE DATA TO MEASURE PROGRESS IN ANDSF DEVELOPMENT

In its June 2017 report, the DoD stated that the coalition relies largely on ANDSF reporting for all metrics. As such, the DoD's assessments of progress in the Afghan Ministries of Defense and Interior rely on data provided by the Afghan ministries. However, much of this information cannot be verified because Afghan operations occur beyond the reach of Coalition advisors who face security restrictions on their travel.

To help address these weaknesses, the DoD is attempting to modernize Afghan ministerial functions, which includes the introduction of three automated systems:

- Afghan Human Resource Information Management System to validate ANDSF personnel numbers and salaries;
- Afghan Personnel Pay System to facilitate unit strength accountability and personnel verification; and
- Core Information Management System to improve accountability of equipment inventories.

These automated systems seek to provide ANDSF leadership and their advisors the tools to evaluate personnel and resource management in a more accurate way.

Nevertheless, the DoD OIG has found that the Combined Security Transition Command – Afghanistan needs to strengthen controls over U.S. direct assistance funding. For example, a DoD OIG audit found that the Afghans could not ensure the accuracy of reports detailing fuel delivery and consumption by the Ministry of Defense. Similarly, a 2017 Special Inspector General for Afghanistan Reconstruction audit found that the DoD spent over $400 million to build ANDSF intelligence capacity but lacked performance metrics to assess progress.

The DoD is emphasizing the need for Afghanistan to implement reforms to address illicit activity and patronage networks within security organizations in order to reduce corruption and increase ANDSF effectiveness. The DoD OIG is currently conducting a summary audit of its previous reports on direct assistance that will make recommendations to address any systemic issues identified. Future DoD OIG oversight will assess U.S. and North Atlantic Treaty Organization efforts to enable the Ministry of Interior to develop its own oversight and internal control capabilities.

ANDSF CAPACITY AND LONG-TERM DOD AUGMENTATION

The United States and the North Atlantic Treaty Organization have relied heavily on contract support for the ANDSF, with the long-term goal that the ANDSF would establish its own capabilities for many of these functions. As of April 2017, around 25,000 personnel served under DoD contracts in Afghanistan, which included support to the ANDSF.

A previous DoD OIG evaluation of Afghan National Police maintenance sustainment capability found that the Afghan National Police lacked a sustainable logistics planning capability, failed to adequately capture consumption and demand data, lacked funding and experience to sustain existing infrastructure, and delayed the transition to an organic maintenance capability. In the long-term, the DoD strategy is for U.S. and North Atlantic Treaty Organization advisors, along with ANDSF leadership, to commit to implementing the National Maintenance Strategy and its goal of ANDSF self-sustainability by 2021.

In summary, the DoD's progress in Afghanistan faces continuing challenges in security, governance, and capacity-building. The ANDSF faces an intensified Taliban insurgency, Islamic State affiliates maintain the ability to conduct suicide attacks and regenerate forces, and Afghan-Pakistan relations remain contentious. After 16 years of U.S. engagement, the challenges in Afghanistan are persistent.

OPERATION INHERENT RESOLVE

Operation Inherent Resolve began on August 8, 2014, when U.S. airstrikes attacked ISIS as it threatened the Iraqi city of Erbil. On September 10, 2014, the United States announced the creation of the Global Coalition to Defeat ISIS, which seeks to use diplomatic, economic, informational, and military power to degrade and ultimately defeat ISIS.

The DoD efforts to train, advise, assist, and equip local forces in Iraq and Syria remain a cornerstone of the U.S. strategy to defeat ISIS. The United States and its 72 Coalition partners support and advise Iraqi Security Forces, Kurdish Peshmerga, Syrian Democratic Forces, and vetted Syrian opposition forces in military operations against ISIS. Iraqi forces' liberation of the city of Mosul demonstrates their increasing security capabilities and the eroding ISIS physical caliphate in Iraq.

INFLUENCE OF RUSSIA AND IRAN IN SYRIA

In March 2017, General Votel testified that Iran poses the greatest danger to long-term peace in the Middle East. He also stated that Iran seeks to take advantage of the war against ISIS and the civil war in Syria to pursue regional dominance. Iran sends fighting forces into Syria in support of the Syrian regime forces of President Bashar al-Assad, and Iran has influence over several of the militias in the Popular Mobilization Forces in Iraq.

The DoD's Defense Intelligence Agency has reported that Russia's military intervention in Syria in 2015 changed the dynamic of the conflict, bolstered the Assad regime, and ensured that no resolution to the conflict is possible without Moscow's agreement. Fighting has also divided the country into zones of influence. As of July 2017, the Syrian regime and pro-regime forces backed by Russia and Iran controlled most of the west of the country, which includes an array of major population centers. In addition, Iran has taken significant steps to increase its influence, mainly through its support for Shia militias operating in both countries, and has warned the Iraqi government not to weaken Iranian-backed Shia Popular Mobilization Forces operating in Iraq.

THE FUTURE OF ISIS

In June 2017, the DoD reported that ISIS was transitioning from a state-like entity in control of territory to an insurgency. The 9-month battle to liberate Mosul illustrated the growing competence of Iraqi Security Forces, but also demonstrated the tenacity and durability of ISIS as a dangerous enemy. ISIS will remain a physical threat within the region in some form, and its viral nature makes it a global threat.

In response to a congressional request, in June 2017, Secretary of Defense James Mattis submitted to Congress a report on the U.S. strategy to defeat ISIS. The report described a new framework for coordinating whole-of-government activities to defeat the global reach of ISIS, while accelerating and intensifying the Operation Inherent Resolve mission in Iraq and Syria. The new strategic framework directs simultaneous pressure across ISIS's global organization, increases focus on non-lethal efforts, seeks to improve interagency collaboration and implementation, and

Iraqi soldiers assigned to the 1st Battalion, 73rd Brigade, 16th Division, run through a breach in a berm. (U.S. Army photo)

streamlines decision-making processes. As part of the framework, the DoD collaborates with the Departments of State, Treasury, and Homeland Security; the Office of the Director of National Intelligence; the Joint Chiefs of Staff; and senior Administration officials to develop the U.S. strategy.

The framework to defeat ISIS described, in part, that intelligence collaboration among partner nations has helped hinder ISIS's attempts to export terror. A recent classified DoD OIG report determined whether the DoD allocation process for intelligence, surveillance, and reconnaissance capability effectively supported the intelligence requirements of the Combined Joint Task Force–Operation Inherent Resolve Commander, while managing the global availability of forces. Future DoD OIG oversight will evaluate DoD policies and procedures for sharing intelligence with allied Coalition forces supporting Operation Inherent Resolve.

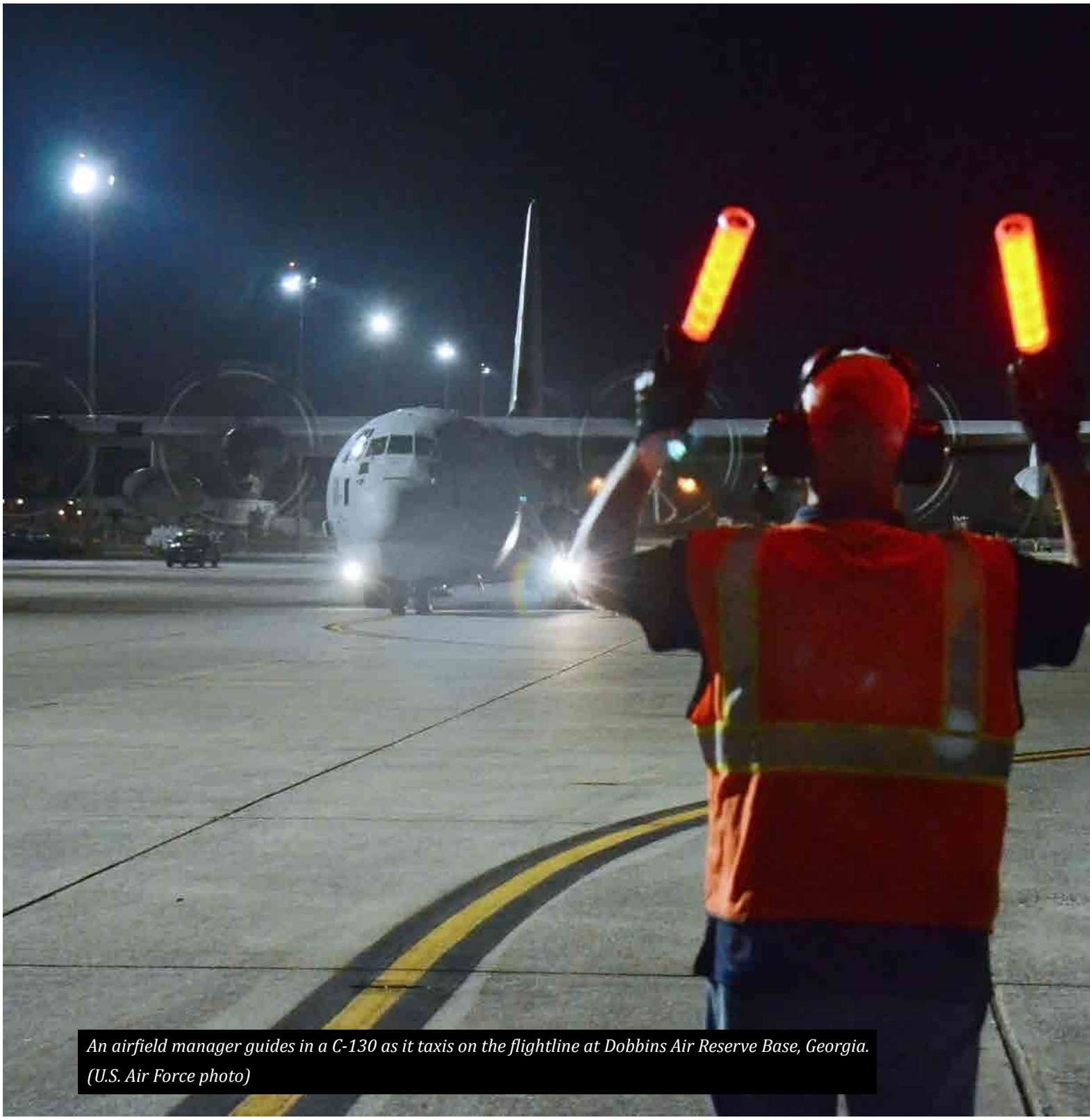
HUMANITARIAN CRISIS IN IRAQ AND SYRIA

The United Nations Office for the Coordination of Humanitarian Affairs reported that Iraq's humanitarian crisis is severe and rapidly expanding. The conflict has displaced over 3 million Iraqis who are living in 3,700 locations across the country. Additionally, more than 1 million displaced people and refugees have fled to areas controlled by the Kurdistan Region Government. According to the United Nations Office for the Coordination of Humanitarian Affairs, because of the intensity of fighting in Mosul, Hawija and Tal Afar, as many as 1.1 million additional civilians may be forced from their homes. As Iraq's campaign transitions to rebuilding the governing, economic, and social structures in areas liberated from ISIS, the humanitarian crisis places immense burdens on the Iraqi central government, regional governments, and host communities.

Similarly, Syria remains one of the most complex and dynamic humanitarian crises in the world today. According to the United Nations Office for the Coordination of Humanitarian Affairs 2017 humanitarian response plan for Iraq, an estimated 13.5 million people, including 6 million children, continue to be in need of humanitarian assistance. Of these, 5.47 million people are in hard-to-reach areas, including nearly 600,000 people in 18 besieged areas. Humanitarian access to individuals in need remains constrained by ongoing conflict; shifting frontlines; administrative and bureaucratic hurdles; violence along access routes; and general safety and security concerns in contravention of international law, particularly international humanitarian and human rights law.

The DoD coordinates with the Department of State and the U.S. Agency for International Development to address humanitarian assistance needs. The DoD uses Overseas Humanitarian, Disaster, and Civic Aid funding to address humanitarian assistance projects and help meet the basic needs of civilian populations. This funding allows for valuable civilian-military cooperation, capacity-building of partner nations, and strengthening of regional stability and security, while promoting U.S. national security interests.

In summary, while the U.S-led Global Coalition to Defeat ISIS has trained and supported Iraqi and Moderate Syrian Opposition forces in significantly reducing ISIS's control of territory and in liberating major population centers, significant challenges remain. DoD officials have stated that ISIS is transitioning to an insurgency with the ability to conduct asymmetric attacks in government-controlled territory with minimal to no warning. Iraqi Government is also challenged in its efforts to incorporate the Popular Mobilization Forces under its control, as some government factions and Iran seek to retain influence. While key major cities have been liberated from ISIS, the transformation of ISIS from a pseudo-state to a trans-regional insurgency will present continued challenges to the DoD and the Global Coalition.



An airfield manager guides in a C-130 as it taxis on the flightline at Dobbins Air Reserve Base, Georgia. (U.S. Air Force photo)

Challenge 3: Enabling Effective Acquisition and Contract Management

Acquisition and contract management have remained high-risk areas for the DoD for many years, and delivering weapons and technology systems on time and within budget continues to pose major management challenges for the DoD. Although Congress and the DoD have initiated reforms designed to improve the acquisition of major weapon systems, many DoD programs fall short of cost, schedule, and performance expectations. As a result, the DoD regularly pays more than anticipated, buys less than expected, and in some cases, delivers less capability than its contracts require. In addition, the Defense Acquisition System often focuses on near-term costs, schedule, and performance trade-offs to the detriment of long-term costs. Yet, more than 70 percent of the life-cycle costs of a weapon system are incurred in the operation and sustainment of the weapon system.

In total, the DoD obligates more than $273 billion annually on contracts for goods and services, including support for military installations, information technology, consulting services, and commercial items. In these areas, the DoD faces challenges in overseeing the contracting officer's representatives, making contract payments, and assessing and reporting on contractor performance. In addition, DoD decision makers sometimes lack information on past and anticipated future contracted services and sometimes focus more on processing the contract action than evaluating the underlying need for the service.

Compounding the acquisition and contracting challenges is the external threat targeting U.S. technologies—specifically, foreign attempts to obtain sensitive or classified information and technologies. The DoD must prevent the illegal transfer of operational and defense technologies.

ACQUISITION AND SUSTAINMENT

As of April 2017, the DoD portfolio of Defense Acquisition programs included 1,667 programs. In the FY 2018 Presidential Budget, the DoD requested $208.6 billion to fund these acquisition programs. Over the past year, the number of programs in the DoD portfolio of Major Defense Acquisition programs grew from 79 to 85, increasing the total planned investment in these programs from $1.64 trillion to $1.75 trillion.

A U.S. Air Force contracting specialist from the 20th Contracting Squadron reviews a contract. (U.S. Air Force photo)

In 2010, the DoD launched the Better Buying Power initiatives in an effort to strengthen the DoD's buying power; improve industry productivity; and provide an affordable, value-added military capability to the warfighter. The Better Buying Power initiatives were based on a set of fundamental acquisition principles, such as:

- eliminating redundancy,
- mandating affordability,
- building stronger partnerships with the requirements community to control costs,
- using the technology development phase for true risk reduction,
- emphasizing competition strategies,
- creating and maintaining competitive environments,
- eliminating requirements imposed on industry where costs outweigh benefits,
- increasing the use of Performance-based Logistics,
- enforcing open system architectures, and
- effectively managing technical data rights.

Congress has also enacted acquisition reforms designed to simplify the procurement process, reduce unnecessary paperwork and regulatory burdens, and enable the development of clearer and more agile acquisition strategies. Through the National Defense Authorization Act, For Fiscal Year 2017, Congress reorganized the acquisition authority within the Office of the Secretary of Defense. The National Defense Authorization Act for FY 2017 also created the position of the Chief Management Officer of the DoD, effective February 1, 2018. The Chief Management Officer will be responsible for improving the quality and productivity of the DoD's business operations, and reducing the costs of those operations, which could enable the DoD to reallocate resources from business operations to readiness and recapitalization of the combat force. The reforms also seek to streamline and modernize DoD's acquisition system, empower better decision making, and encourage investment earlier in acquisition programs. The ultimate goal of the reforms is to provide better technology faster and more efficiently to the warfighter.

While DoD OIG audits determined that the DoD has made progress in acquisition reform, program personnel have not always adequately defined, validated, funded, and executed requirements or delivered weapon systems that meet performance requirements. For example, in 2017, a DoD OIG audit found that the Navy did not effectively establish capability requirements and execute testing to procure the Surface Mine Countermeasure Unmanned Undersea Vehicle (Knifefish). Specifically, the Knifefish requirements developer did not fully define requirements to support the communication interface and launch and recovery operations between the Knifefish system and the Littoral Combat Ship, which is a fast, agile ship designed for operations in environments near the shoreline. Additionally, the Knifefish program office did not effectively plan and execute testing because of funding shortfalls, which resulted in a 14-month delay in meeting program milestones.

The DoD OIG has found that sometimes capability requirements have not been adequately defined and tested and that test community recommendations or deficiencies have not been adequately addressed and, in some cases, have been ignored. For example, the DoD OIG evaluated the Navy's management of waivers and deferrals from operational test requirements for nine major weapon systems. The DoD OIG review of waiver requests at the Naval Air Systems Command found that Navy program managers and system sponsors did not fully implement Navy policies for requesting waivers and deferrals before certifying that the programs were ready for Initial Operational Test and Evaluation to support the final production decision. As a result, six of nine programs reviewed had completed Initial Operational Test and Evaluation with unresolved deficiencies that negatively impacted the warfighter's primary missions. The Navy took corrective actions by issuing interim guidance to address the gaps in the testing and identification of deficiencies caused by program offices' unchecked use of the waiver and deferral process. Additionally, the Vice Chairman of the Joint Chiefs of Staff updated the Manual for the Operation of the Joint Capabilities Integration and Development System to include a requirement that program managers notify the Joint Requirement Oversight Council when a program is not meeting its primary mission requirement.

In addition, DoD OIG audits have determined that the DoD continues to exceed cost and schedule baselines and still does not consistently define performance metrics. Between October 2016 and March 2017, the DoD OIG identified $909.7 million in questioned costs and funds recommended to be put to better use during acquisition audits. For example, the DoD OIG reported in August 2016 that Army officials could have managed the schedule, affordability, and quantity requirements of the XM25 program more effectively. The XM25 is a semiautomatic, shoulder-fired weapon system that fires 25-mm high-explosive, air-bursting ammunition to allow soldiers to fire at hidden enemy targets. The initial production decision for the XM25 has been delayed since the first quarter of FY 2012. In April 2017, the Army terminated the XM25 contract with the prime contractor after it failed to deliver the weapons as specified by the terms of the contract.

An assistant product manager for Soldier Protective Equipment shows the Acting Principal Deputy for the Assistant Secretary of the Army (Acquisition, Logistics and Technology) how hard armor saves soldiers' lives. (U.S. Army photo)

An HH-60 conducting rescue operations in the Beaumont, Texas, area after Hurricane Harvey. (U.S. Air National Guard photo)

The DoD OIG also continues to identify challenges with the sustainment of weapon systems. For example, in 2017 the DoD OIG determined that the DoD did not consolidate its purchase of 2.9 million H-60 spare parts to maximize its market leverage. The H-60 is a twin-engine helicopter that has been in service since 1979. The Army, Navy, Air Force, and U.S. Special Operations Command all fly different versions of the H-60. The DoD used at least 2,136 different contracts and purchase orders from February 2015 through January 2016 to purchase H-60 spare parts valued at $394.9 million. These contracts and purchase orders were awarded to at least 590 different contractors. The DoD procured the same H-60 spare parts on different contracts, often at different prices. As a result, the DoD missed the opportunity to use quantity discounts to lower spare parts prices and administrative costs.

Overall, as of March 2017, the DoD OIG was tracking 245 open recommendations on 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 are related to issues such as support for the procurement of weapon systems and automated information systems and obtaining fair and reasonable contract pricing. We believe the DoD needs to examine best practices to integrate critical requirements, resources, and acquisition decision-making processes.

CONTRACT MANAGEMENT AND OVERSIGHT

As noted above, the DoD spends more than $273 billion each year on contracts for supplies, such as furniture and services, support for military bases, support for contingency operations in Southwest Asia, and general 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 also critical to ensuring that contractors provide quality services and supplies in a timely manner, within cost; mitigating contractor performance problems; and ensuring that the Government receives the best value for the warfighter. However, DoD OIG audits have found deficiencies in contract

U.S. sailors and marines with Special Purpose Marine Air-Ground Task Force – Crisis Response – Central Command carry a marine to a UH-60L Black Hawk in the Middle East. (U.S. Marine Corps photo)

oversight. For example, DoD OIG audits have determined that DoD contracting officers do not always appoint contracting officer's representatives (CORs), appointed CORs are not always adequately trained, contracting officials do not always develop adequate quality assurance surveillance plans or never developed them at all, quality assurance surveillance plans do not reflect current contract requirements, and CORs did not always maintain supporting documentation. Moreover, the CORs did not use the oversight procedures established in the quality assurance surveillance plans to monitor contractor performance.

In addition, the DoD OIG determined that Defense Logistics Agency (DLA) Land and Maritime did not adequately process product quality deficiency reports or pursue appropriate restitution for a projected 267 contracts for which contractors supplied defective parts. In addition, DLA Land and Maritime did not account for the defective parts in the DoD supply chain, including all parts on a contract for a critical safety item for which DoD customers submitted product quality deficiency reports.

DoD OIG audits also identified problems with the management of contract requirements. For example, the DoD OIG determined that for the contracts used to provide commercial transportation in the Middle East, the Army did not analyze asset usage or continuously evaluate transportation requirements so that it could increase or decrease orders based on operational needs. As a result, the Army ordered an average of 39 percent more transportation assets than it needed throughout the life of the contracts. Further, excessive guaranteed minimum payments were paid to each of the four contractors, which prompted the Army to order services to meet the guaranteed minimums rather than what was actually required within that period of performance. The audit concluded that the Army wasted $53.6 million throughout the life of the contracts on services that it did not require.

The DoD also must seek to reduce improper payments. Improper payments are overpayments or underpayments that should not have been made, payments made in an incorrect amount, payments made to ineligible recipients or for ineligible goods or services, and payments made with missing or insufficient documentation. Improper payments are often caused by unreliable data or inadequate internal controls that increase the likelihood of fraud. The DoD reported that it made $973.77 million in improper payments for FY 2016; however, a DoD OIG audit found problems with the completeness and accuracy of the DoD improper payment review and the information the DoD reported.

Recent DoD OIG reports highlighted improper payments related to service fees for on-time delivery for deliveries that were late, as well as ineligible travel-related expenses. These reports focused on specific areas of concern related to improper payments, such as unidentified improper billings by vendors and lack of adequate controls to pay for eligible services or supplies received by the DoD.

The DoD OIG has also identified significant problems with the reporting of contractor past performance in the Contractor Performance Assessment Reporting System across the DoD. The

Federal Acquisition Regulation requires contractor performance information be collected in the Contractor Performance Assessment Reporting System and used in source selection evaluations. Contractor past performance information is critical to ensuring that the U.S. Government only does business with companies that provide quality products and services in support of DoD missions.

However, DoD officials have not always evaluated contractor performance in accordance with Federal guidance. In addition, DoD OIG audits identified an internal control weakness in the Contractor Performance Assessment Reporting System that allowed incomplete evaluations of contractor performance to be submitted. As a result, Federal source selection officials did not have access to timely, accurate, and complete past performance assessment information needed to make informed decisions related to contract awards.

As of March 2017, the DoD OIG made and tracked 131 open recommendations related to issues such as assessment of contractor performance through performance assessment reports, management of energy savings performance contracts, cost-reimbursement contract issuance, and management and identification of defective spare parts. In FY 2018, the DoD OIG plans to perform additional audits on oversight of various contracts in Africa and Southwest Asia, DoD integration of operational contract support into force development and training, privatization of DoD utilities, improper payments, and use of past performance information in the source selection process.

ILLEGAL TECHNOLOGY TRANSFER AND COUNTERFEIT

The DoD spends billions of dollars each year to develop and acquire sophisticated technologies that provide an advantage for the warfighter during combat or other missions. Many of these technologies are also sold or transferred to other countries to promote U.S. economic, foreign policy, and national security interests. However, sensitive DoD technology is also a target for unauthorized transfer, such as theft, espionage, reverse engineering, and illegal export.

A U.S. Army soldier with the 5th Special Forces Group (Airborne) demonstrates an Australian rappel. (U.S. Army photo)

Each year, the Defense Security Service publishes a report, "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting," providing a compilation and analysis of the suspicious contact reports received from cleared industry, which are industry partners that must meet specific requirements to safeguarding critical technologies in their possession. The report stated that the threat posed by illegal transfer of DoD technology "shows no sign of waning, and securing our cutting-edge technology remains key to maintaining our military and economic advantage."

To address the threat of illegal technology transfers, the DoD has also published agency-wide policies and worked to strengthen programs to identify and protect technologies critical to U.S. interests. The Defense Security Service administers the National Industrial Security Program for DoD and 30 other Federal agencies, which seeks to ensure that DoD contractors properly safeguard classified information and information associated with critical technologies. The guidance requires cleared contractors to remain vigilant and report suspicious contacts to the Defense Security Service.

The final brigade-level exercise to enhance readiness to deter aggression in Europe while serving in support of Operation Atlantic Resolve. (U.S. Army photo)

While these measures help to protect critical technologies, illegal transfer of sensitive technologies still occurs. As the criminal investigative arm of the DoD OIG, the Defense Criminal Investigative Service (DCIS) conducts counter-proliferation investigations that seek to deter the illegal transfer of sensitive DoD technologies and hold accountable those who do so. DCIS Counter-proliferation investigations resulted in 19 criminal charges, 19 convictions, 1 suspension and 11 debarments from Government contracts in FY 17.

For example, a DCIS investigation resulted in the guilty plea and sentencing of Fuyi Sun, a citizen of the People's Republic of China, for violating the International Emergency Economic Powers Act. Sun was sentenced to 3 years in prison for a scheme to covertly bypass U.S. export laws to obtain M60JB-3000-50B carbon fiber, which has applications in aerospace technologies, unmanned aerial vehicles and other military applications. This highly protected material is export-controlled and requires a license to export to China.

In another example, a Chinese businessman, Guan Ying Li, also known as "Henry Li," pleaded guilty and was sentenced to 10 years in Federal prison for attempting to provide military equipment to a Peruvian terrorist organization. Li brokered several deals with a purported Chicago-area businessman, knowing the items would be used to harm Peruvian and U.S. Government personnel. The equipment included thermal batteries designed for use in man-portable air-defense systems, very high frequency radios and night-vision systems.

In addition to illegal technology transfers, the DoD is also at risk of counterfeit parts being used on DoD weapons systems. For example, with many manufacturing steps being performed off-shore, sophisticated adversaries can exploit vulnerabilities to introduce kill switches, back doors, or viruses to render systems ineffective or to leak sensitive information. In particular, the use of counterfeit parts can affect the integrity of systems and ultimately endanger the lives of service members. Many systems face risks of being counterfeited, including microelectronics used in fighter jets, ground combat systems, and missile guidance systems.

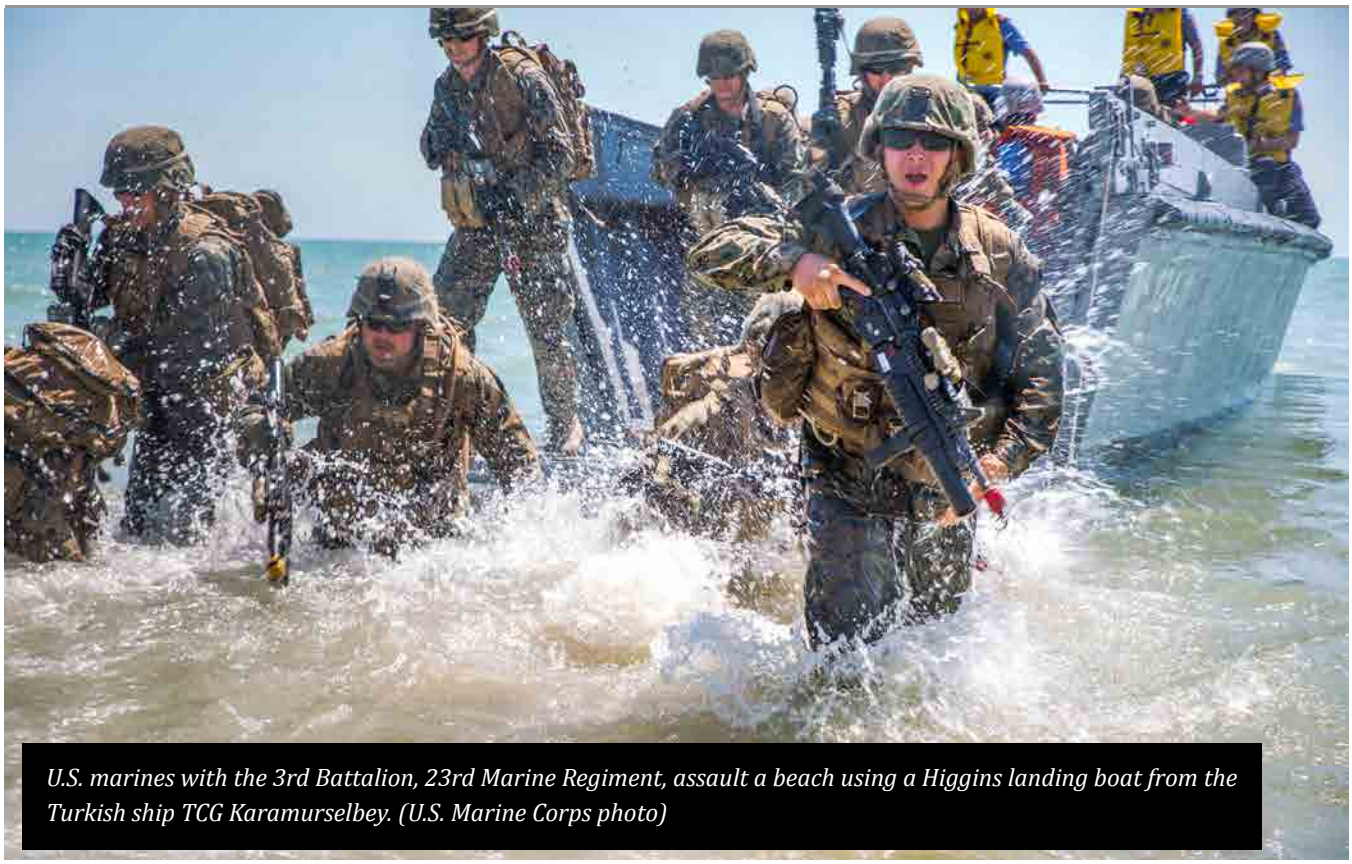
The GAO reviewed the DoD's efforts to address vulnerabilities from counterfeit parts in the DoD supply chain. The GAO found several aspects of the DoD's implementation of its mandatory reporting

A U.S. Army soldier checks targets through a spotting scope during the Squad Designated Marksman Course. (U.S. Air National Guard photo)

for suspect counterfeit parts to have limited its effectiveness as an early warning system. The GAO also concluded that, without proper oversight ensuring that the reporting requirement was consistently applied, the DoD could not ensure it effectively managed the risks associated with counterfeit parts.

The DoD OIG has also identified gaps in the DoD's supply chain management process that have increased the risk that an adversary could infiltrate the supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of systems. For example, the DoD OIG determined that the Missile Defense Agency had established several initiatives to manage supply chain risk for the Ground-based Midcourse Defense system. The Missile Defense Agency is piloting a DoD software assurance program to improve the supply chain security for its critical software. However, the Missile Defense Agency did not fully implement the DoD supply chain risk management policy for the Ground-based Midcourse Defense system. As a result, there was an increased risk to the Missile Defense Agency's supply chain security for the Ground-based Midcourse Defense system's critical hardware, software, and firmware.

The DoD OIG is also planning to conduct reviews addressing key risk areas regarding counterfeit parts and the industrial base. For example, the DoD OIG is planning to review whether the controls governing the Commercial and Government Entity Code process are adequate and effective. The Commercial and Government Entity Code is a five-position code that identifies contractors conducting business with the U.S. Government, North Atlantic Treaty Organization member nations, and other foreign governments. The Commercial and Government Entity code allows contractors access to a variety of mechanized systems throughout the Government and provides for a standardized method of identifying a given legal entity at a specific location.



U.S. marines with the 3rd Battalion, 23rd Marine Regiment, assault a beach using a Higgins landing boat from the Turkish ship TCG Karamurselbey. (U.S. Marine Corps photo)

DoD OIG investigations of product substitution, including counterfeit, defective, or substandard products, are also one of DCIS's investigative priorities. Product substitution can disrupt readiness, waste economic resources, and threaten the safety of military and Government personnel and other end users. DCIS coordinates with the DLA to react to anomalies and threats affecting the DoD supply chain. As of September 6, 2017, product substitution investigations resulted in 19 criminal charges, 3 convictions, 8 suspensions, and 16 debarments from Government contracts in FY 2017.

For example, a DCIS investigation determined that a DoD contractor, Boggs & Associates, Inc., was selling nonconforming parts to the DLA for military aircraft, vehicles, and vessels. The majority of these parts were considered critical application items and had to meet certain military specifications to ensure weapon system performance and the safety of operating personnel. Testing of parts provided by Boggs & Associates revealed that the company provided DLA nonconforming parts on 46 different purchase orders. Specifically, the parts were made from unauthorized substituted material or did not pass specified testing requirements. As a result, Stephan D. Boggs, president of Boggs & Associates, was sentenced to 24 months in prison and debarred from Federal contracting.

In summary, with the prospect of slowly-growing or flat DoD budgets for years to come, 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. In addition, the DoD needs to better manage and oversee contracts for goods and services and to prevent the illegal transfer of sensitive technology.

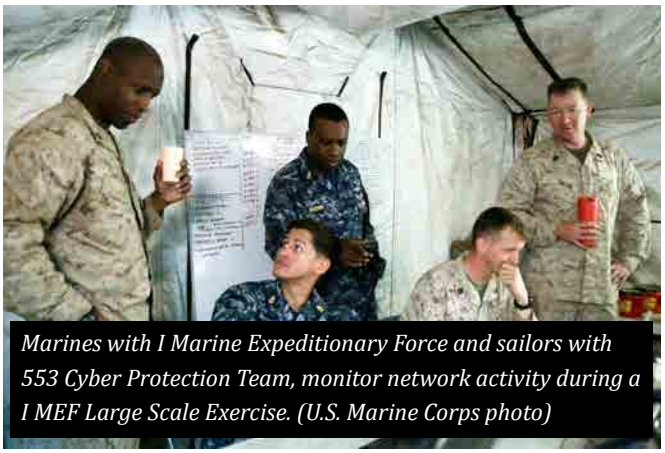
A U.S. Army soldier, assigned to the 4th Infantry Division, and soldiers from Romania and Bulgaria work at the International Help Desk during exercise Saber Guardian. (U.S. Army photo)

Challenge 4: Increasing Cybersecurity and Cyber Capabilities

Cyber threats to the United States are unpredictable, rapidly changing, and widespread. Adversaries are becoming more sophisticated and strategic-minded, and cyber threats and exploitable vulnerabilities will continue to grow. Since 2013, the Director of National Intelligence has identified cyber threats as the top strategic global threat facing the United States. During the same period, the GAO identified cybersecurity of Federal information systems and networks as a high-risk area because all sectors of the Government—energy, transportation systems, communications, financial services, and defense of the homeland—are dependent on information systems and electronic data to perform operations.

Since the beginning of 2016, well-publicized cyberattacks, such as those against the Democratic National Committee, state voter databases and software systems during the 2016 U.S. presidential election, and private industry have compromised national security and had significant economic impacts.

Cyberattacks can also affect DoD missions. The DoD relies heavily on cyberspace to perform the full spectrum of its military, intelligence, and business operations. While cybersecurity is the responsibility of all DoD Components and personnel, several Components are assigned specific responsibility for DoD cybersecurity programs. The DoD Chief Information Officer must develop strategies and policies for operating and defending the DoD Information Network (DoDIN) and building the DoD cybersecurity workforce, manage the DoD information technology architecture, and maintain inventories of DoD mission-critical and mission-essential systems. This is a challenging responsibility because the DoDIN is composed of thousands of DoD networks and systems worldwide, including DoD-owned and leased communications, software, data, security devices, and other associated services. 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. The Joint Force Headquarters–DoDIN Commander also serves as the Director of the Defense Information Systems Agency.



Marines with I Marine Expeditionary Force and sailors with 553 Cyber Protection Team, monitor network activity during a I MEF Large Scale Exercise. (U.S. Marine Corps photo)

Each Military Service and Defense agency is responsible for protecting its networks and systems. The Military Services also staff and equip the Cyber Mission Force. The Cyber Mission Force is composed of the:

- National Mission Force, which defends national interests against cyberattacks of significant consequence;
- Combat Mission Force, which generates integrated cyberspace effects and develops cyberspace capabilities to support combatant commanders in meeting command plan objectives; and
- Cyber Protection Teams, which support the DoD's cyber workforce in performing traditional defensive measures and defends priority DoD networks and systems against specific threats.

In May 2017, the President issued Executive Order 13800, which stated that a "whole-of-government" approach is needed to protect information technology and data from unauthorized access and other cyber threats. Many Government organizations and the private sector contribute to securing U.S. and DoD networks because no one agency or organization has the capability to do it alone. For example, USCYBERCOM supports a portion of the whole-of-government effort to defend America's critical infrastructure by working with other Government agencies, such as the Departments of Homeland Security and Justice, to help protect national critical infrastructure and to prepare for scenarios in which U.S. military action is required to defend against cyberattacks. In addition, USCYBERCOM and other Federal agencies are increasingly sharing information about cyber threats and working to clarify their roles to assist the private sector in responding to cyberattacks and recovering from cyber incidents.

In 2017, the Director of National Intelligence testified that adversaries from nation states (Russia, China, Iran, and North Korea) and non-nation states (terrorists, criminals, and "hacktivists") were investing heavily in developing cyberspace capabilities and becoming more adept at using cyberspace to threaten U.S. national security interests. The Director also stated that nearly all information, communication networks, and systems are at risk because of supply chain operations that insert compromised hardware or software, malicious actions by trusted insiders, and mistakes by system users. Additionally, the Director stated that cyber threats pose an increasing risk to public health, safety, and the economy as technology is integrated with critical infrastructure in sectors that support American society.

The cybersecurity risks identified by the Director, as well as the DoD's ability to develop strong partnerships with U.S. allies, international partners, and other private organizations, are critical challenges for the DoD. To address these challenges, the FY 2017 National Defense Authorization Act required the DoD to establish a Unified Combatant Command for cyber operations forces. In addition, the Act prohibited the Secretary of Defense from separating the "dual-hatted" relationship between the USCYBERCOM Commander and the National Security Agency

A U.S. Air Force E-3 Sentry Airborne Warning and Control System takes off from Nellis Air Force Base, Nevada. (U.S. Air Force photo)

Director until specific conditions are met.[1] In August 2017, the President directed the Secretary of Defense to begin elevating USCYBERCOM to a Unified Combatant Command, consistent with the 2017 Act requirements.

DEFENDING THE DOD INFORMATION NETWORK FROM INSIDER AND EXTERNAL THREATS

The DoD must defend the DoDIN against cyberattacks, recover quickly if security measures fail, and operate in a degraded environment if a system or network is compromised. While the DoD will have difficulty defending every network and system against every kind of intrusion, it must take steps to identify, prioritize, and defend its most critical networks from insider and external threats.

The President's May 2017 Executive Order notes that known but unmitigated vulnerabilities—such as using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance—are among the highest cybersecurity risks faced by the U.S. Government. The 2017 Executive Order also states the majority of malicious activity on Federal systems and networks are perpetrated by exploiting known vulnerabilities and could be prevented by mitigating those vulnerabilities. However, the DoD OIG and the GAO have both found in recent years that DoD leadership did not address vulnerabilities consistently or in a timely manner.

One measure the DoD has initiated to reduce cybersecurity risks is the consolidation of DoD information technology systems. In 2010, the DoD began migrating to a Joint Information Environment to reduce the DoDIN attack surface by establishing a single security architecture, optimizing identity and access management, and migrating to cloud computing. A major component of that architecture is the Joint Regional Security Stacks, which is a suite of equipment with network applications that provide data processing platforms and network

1 The National Defense Authorization Act for FY 2017 identifies specific conditions that needed to be met before terminating the dual-hatted relationship—sufficiency of tools, capabilities, and infrastructure to meet the unique cyber mission needs of each agency; establishing command and control systems and processes to plan, de-conflict, and execute military cyberspace operations; and the CMF achieving full operational capability.

capabilities, such as firewalls, intrusion detection and prevention, and enterprise risk management solutions. However, the DoD OIG and the GAO have identified challenges the DoD has faced in implementing the Joint Information Environment, such as implementing an effective cloud strategy and defining the scope and cost of key initiatives of the Joint Information Environment program. In the coming year, the DoD OIG intends to determine the progress of the DoD's implementation of Joint Information Environment initiatives specific to the Joint Regional Security Stacks.

The DoD must 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.

The Government and the DoD have taken steps to attempt to mitigate insider threats. For example, in response to the Wikileaks disclosures in 2010, the President issued Executive Order 13587 establishing an insider threat detection and prevention program in 2011. In 2012, the President issued a Presidential Memorandum to establish minimum standards for Executive Branch insider threat programs. In 2013, the DoD issued a strategy to defend its networks, systems, and data, which included goals to:

- enhance security through good cyber hygiene, which is general user, administrator, and leadership compliance with laws, regulations, Federal and DoD policies and standards critical to protecting systems and networks against cyber threats;
- identify and detect insider threats through increased monitoring of high-risk roles; and
- increase focus on industrial control systems, which are systems used to operate infrastructure such as base utilities, dams, and nuclear facilities within the DoD.

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 and the DoD Component Insider Threat Records System to analyze, monitor, and audit insider threat information derived from DoD insider threat programs. In an upcoming audit, the DoD OIG intends to assess whether the Defense

U.S. Army soldiers assigned to the 44th Expeditionary Signal Battalion, 2nd Theater Signal Brigade, monitor the network at Lightning Ops. (U.S. Army photo)

Insider Threat Management and Analysis Center has implemented effective controls over the collection, analysis, and dissemination of information related to insider threats.

Yet, although the DoD has made progress defending against insider threats, more progress is needed. Despite efforts to limit insider risks, two contractors working for the National Security Agency removed classified information in 2017, and in at least one instance disclosed classified information detrimental to national security. The DoD OIG also intends to determine whether DoD intelligence community agencies have secured access to and monitored user activity affecting classified enclaves within their agencies.

In a review completed in August 2016, the DoD OIG determined that the National Security Agency's processes and technical controls to limit insider threats from privileged users to its networks, systems, and data were ineffective. In a followup audit, the DoD OIG is examining whether the National Security Agency implemented effective security configuration controls and processes to monitor user activity within its enterprise, identify and authenticate connected devices, and disable removable media.

The U.S. Marine Corps fielded its first tactical information system to be issued standard with Windows 10. (U.S. Marine Corps photo)

In July 2017, the DoD OIG also identified weaknesses in Army and Defense Health Agency efforts to protect their networks and systems that process, store, and transmit patient health information. The DoD OIG is examining whether the Navy and Air Force implemented sufficient security protocols to protect electronic health records and patient health information from unauthorized access and disclosure. The DoD OIG is also determining whether Missile Defense Agency contractors implemented controls and processes to protect ballistic missile defense system data. The DoD OIG also intends to assess whether the Military Departments have mitigated cybersecurity vulnerabilities in major acquisition programs identified during operational testing, and whether DoD Components implemented effective cyber hygiene programs.

In July 2017, the DoD OIG published a Compendium of Open Recommendations that identified all open recommendations from prior reports. These open recommendations included more than 100 recommendations, which if implemented, would improve the DoD's efforts to reduce its risks of insider threats and protect the DoDIN. For example, the USCYBERCOM Commander, the Chiefs of Staff for the Army and Air Force, the Chief of Naval Operations, and the Commandant of the Marine Corps have not yet developed a comprehensive framework that reduces the DoD's risk to fully meeting current and future Cyber Mission Force resourcing requirements. In addition, the Army has not fully identified the owner of each Secret Internet Protocol Router Network that is responsible for managing and securing those circuits. Further, the Under Secretary of Defense for Acquisition, Technology, and Logistics has not developed and issued a policy requiring program offices to implement applicable software assurance countermeasures throughout the lifecycle of DoD programs. These actions would help the DoD to build and sustain its cyber workforce, improve its ability to conduct offensive and defensive cyberspace operations, and protect its systems and networks from cyber threats.

In summary, the DoD continues to take steps to defend its vast architecture of cyber systems, networks, and devices from insider and external threats, but significant challenges to protecting the networks remain. In pursuing this challenge, the DoD must accurately identify the composition of its networks; 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; and improve the effectiveness of its cyber hygiene programs to ensure fundamental cybersecurity practices are followed. These are not easy or short-term tasks, but they are critical to many aspects of the DoD's mission.

PROTECTING DOD CRITICAL INFRASTRUCTURE

Heightening the importance of the cybersecurity challenge, the nation's critical infrastructure has become much more interdependent, transitioning to an operating environment interconnected through multiple platforms, such as cloud computing, mobile devices, the Internet, and wireless connectivity. 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, nuclear reactors, and communication networks.

The risks threatening critical infrastructure are complex, uncertain, and constantly evolving. Critical infrastructure that has been subject to risks associated with physical threats and natural disasters is increasingly exposed to cyberspace risks. The DoD relies on a global network of critical infrastructure and the systems used to operate the assets to protect, support, and sustain its forces, and to conduct operations worldwide.

In January 2017, the Director of National Intelligence and USCYBERCOM Commander stated that adversaries were developing capabilities to compromise U.S. critical infrastructure, as well as consumer and industrial devices known as the "Internet of Things," which are everyday physical objects that are able to connect to the Internet and identify themselves to other devices within a network. The Commander stated that several countries have disrupted or remotely accessed critical infrastructure systems of the United States

A U.S. Air Force aircraft metals technology journeyman from the 20th Equipment Maintenance Squadron, welds a portable deployment trailer at Shaw Air Force Base, South Carolina. (U.S. Air Force photo)

and its allies. For example, the "Black Energy" malware affected energy-sector systems worldwide and caused a malicious cyberattack against Ukrainian power systems in 2015, which resulted in widespread, unplanned, and lengthy power outages across western Ukraine.

The DoD OIG has issued several reports about DoD cybersecurity weaknesses affecting critical infrastructure. In 2013 and 2014, the DoD OIG issued a series of reports that determined that the U.S. Army Corps of Engineers did not adequately protect critical infrastructure, such as locks and dams and the industrial control systems used to operate those structures, from unauthorized access and cyberattacks. More recently, the DoD OIG determined that the Air Force did not implement basic cybersecurity controls to protect, detect, counter, and mitigate potential cyberattacks on industrial control systems that provide essential services such as those generating or providing electricity, distributing and treating potable water, and heating and cooling computer rooms and data centers. The DoD OIG is currently determining whether the Air Force adequately plans for the recovery of information systems and data after emergencies, system failures, or disasters and whether the DoD has effective programs to detect, report, and respond to security incidents on mission-critical control systems.

In summary, the DoD continues to face challenges in protecting critical infrastructure and supporting other Government agencies in protecting critical infrastructure. To mitigate these risks, the DoD needs to fully identify physical and cybersecurity risks affecting each asset, identify all industrial control systems used to operate the assets, adequately fund security improvements, and enable staff with expertise to operate and secure the industrial control systems.

INCREASING SUPPLY CHAIN RISK MANAGEMENT PRACTICES

Federal agencies also face constant risks associated with information technology products that may contain malicious functionality, are counterfeit, or are vulnerable to compromise because of poor manufacturing and development practices within the supply chain. In 2008, National Security Presidential Directive-54 and Homeland Security Presidential Directive-23 made supply chain risk management a national priority. Supply chain risks include acts by an adversary or trusted 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 a subset of the supply chain risks. Examples of cybersecurity supply chain risks include:

- third-party service providers and vendors with physical or logical access to information systems, software code, or intellectual property;
- poor information security practices;
- compromised software or hardware purchases;
- counterfeit software or hardware with embedded malware; and
- third-party data storage and software security vulnerabilities in the supply chain process.

Cybersecurity risks in the supply chain are especially challenging to the DoD when it develops and acquires weapon systems or any system that relies on technology. However, cybersecurity in the supply chain cannot be viewed as solely an information technology problem. Ensuring DoD warfighting mission capabilities are not impaired by vulnerabilities introduced through the supply chain process by foreign intelligence, terrorists, or hostile actors, whether an insider or external adversary, is essential to ensuring uncompromised

An M270 Multiple Launch Rocket System fires an MGM-140 Army Tactical Missile. (U.S. Army photo)

weapons and information systems. For example, in 2015, the supply chain was compromised when a third-party vendor installed adware known as "Superfish" in Lenovo notebook computers. Superfish tampered with the user's computer security in such a way that cyber attackers could see all communications, including banking transactions, passwords, and e-mails. In 2016, the DoD's Joint Staff warned the DoD against using equipment, such as computers and handheld devices, made by Lenovo, a Chinese manufacturer, amid concerns that the technology could be used to spy on DoD networks.

To combat and manage these risks throughout the life cycle of a program requires robust systems engineering, supply chain risk management, hardware and software assurance, and information systems security.[2] In April 2016, the DoD OIG determined that the DoD had not issued procedures for applying software assurance countermeasures across all Major Defense Acquisition programs, and the Navy did not perform all software assurance countermeasures in the program protection plan for the Navy Littoral Combat Ship, a type of ship designed to operate close to shore to counter shallow-water mine, surface, and submarine threats. Additionally, the DoD OIG reported in April 2017 that the Missile Defense Agency did not fully implement the DoD supply chain risk management policy for the Ground-based Midcourse Defense System, a critical system used to detect, track, and destroy intermediate and long-range ballistic missiles during the midcourse phase of flight. The DoD OIG is currently examining whether the Air Force Space Command has implemented an effective supply chain risk management program for critical strategic systems, which are systems so vital that their loss or degradation would prevent the Air Force from providing resilient space and cyberspace capabilities to meet Joint Force and national objectives.

In summary, while the DoD is taking steps to reduce its supply chain risks, more must be done in this area to manage the risks associated with acquiring assets containing technology. The DoD needs to develop and consistently implement software assurance countermeasures across all major acquisition programs; coordinate with other agencies and the private sector to improve cybersecurity over products for which the DoD has limited to no direct control within the manufacturing process; and identify susceptibilities, vulnerabilities, and threats throughout the DoD supply chain and develop mitigation strategies to combat those threats.

PLANNING AND CONDUCTING DEFENSIVE AND OFFENSIVE OPERATIONS

Defensive and offensive cyberspace operations, whether conducted individually or simultaneously, are critical for defending the U.S. and supporting combatant commanders. Presidential Policy

2 Hardware and software assurance is the level of confidence that hardware and software will function as intended and be free of vulnerabilities, either intentionally or unintentionally designed or inserted, throughout the component's life cycle.

Directive-20 gives the DoD authority to conduct offensive and defensive cyberspace operations. Defensive cyberspace operations include activities to discover, detect, analyze, and mitigate prioritized threats against cyber key terrain to ensure mission success. In military doctrine, cyber key terrain includes the physical location where routers, switches, cables, and other devices are located, as well as the logical configuration of a network and the users and administrators (cyber persona) of an architecture. Offensive cyberspace operations include activities and the use of cyberspace capabilities to project power and achieve a specific objective in and through cyberspace.

To conduct successful offensive and defensive cyberspace operations, the DoD requires detailed, predictive, and actionable intelligence about global networks and systems, adversary capabilities, and malware to develop its intelligence, warning, and cyber capabilities. However, the DoD continues to face challenges in developing or acquiring unique cyber capabilities to conduct defensive and offensive operations. Cyber capabilities include the infrastructure, such as computers, cables, antennas, switches and routers; the electromagnetic spectrum, such as datalink, cellular, and wireless frequencies; and the content, such as data, algorithms, and applications needed to conduct cyberspace operations. USCYBERCOM, the Military Services, and the Defense Information Systems Agency are now focused on identifying, prioritizing, and developing Service-specific and joint infrastructure and cyberspace capabilities. Specifically, the DoD continues to build a Unified Platform that provides an extended network of cyber capabilities to the Cyber Mission Force to conduct full-spectrum cyberspace operations, but the platform will not be operational for several years.

In January 2016, the USCYBERCOM Commander stated that the DoD needed to work with its allies and international partners to develop cybersecurity capabilities and build on the global investments in cyber-related capabilities, technologies, and

An HH-60G Pave Hawk refuels from an HC-130P/N King enroute to rescue two German citizens in distress at sea. (U.S. Air Force photo)

strategies because "no single group, nation, segment, or entity has all the answers." The 2015 DoD Cyber Strategy, which is consistent with the National Military Strategy, includes a goal to build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. It states that the DoD must work with its interagency partners, the private sector, and allied and partner nations, such as those in the Middle East, Asia, and Europe, to deter and if necessary defeat a cyberattack of significant consequence to the United States and U.S. interests.

USCYBERCOM and the Cyber Mission Force are also executing cyberspace missions to support operations against violent extremists, especially across the U.S. Central Command's area of responsibility and in U.S. Special Operations Command missions. However, building alliances and maintaining partnerships to develop combined capabilities that support combatant command objectives are difficult and require continual focus, particularly given rapidly shifting and dynamic military and strategic alliances.

Since 2011, the Secretary of Defense has issued two 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. However, the DoD continues to struggle to implement these strategies. For example, in December 2014, the DoD OIG determined that combatant commands

had insufficient resources and guidance from the Joint Staff to adequately plan and conduct cyberspace operations in their areas of operations. The DoD OIG is currently determining whether the U.S. European Command has integrated offensive and defensive cyberspace operations into its command plans.

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

BUILDING, RETAINING, AND GROWING DOD'S CYBER WORKFORCE

Despite Federal policies and strategies designed to grow the DoD cybersecurity workforce, the DoD and the U.S. Government continue to struggle in attracting, growing, and retaining its cyber workforce. Addressing the growing cybersecurity challenges requires a capable workforce that has the necessary cybersecurity knowledge, skills, and competencies to counter increasingly sophisticated and ever-changing threats.

A U.S. Army network operations noncommissioned officer configures a router. (U.S. Army photo)

In 2017, the GAO again identified the shortage of cybersecurity professionals in the U.S. Government as a high-risk area. Recognizing significant gaps in the Government's cybersecurity workforce, the Office of Management and Budget issued Memorandum M-16-04 to support Government efforts to recruit, develop, and maintain cybersecurity talent and to address existing challenges in understanding key capabilities and capacity gaps affecting the cybersecurity workforce.

The DoD cyber workforce includes personnel who build, secure, operate, and defend DoD and U.S. cyberspace resources, and conduct related intelligence activities and operations in or through cyberspace. According to the USCYBERCOM Commander, to attract, build, retain, and grow the DoD cyber workforce, the DoD is:

- expanding training capacity by tapping into previously unused resources and building new partnerships with academia, other Federal agencies, and the private sector;
- developing and refining specific career tracks within the Military Services;
- identifying specific cybersecurity roles and responsibilities instead of categorizing the entire workforce as a single group;
- instituting selective re-enlistment bonus programs; and
- offering enlistments at higher ranks for personnel entering the service with cybersecurity-related certifications.

In November 2015, the DoD OIG determined that the USCYBERCOM and Military Services needed to develop a defined process to determine the acceptability, suitability, and feasibility of a proposed force design change that addresses

A U.S. Army soldier checks signal connection strengths. (U.S. Army photo)

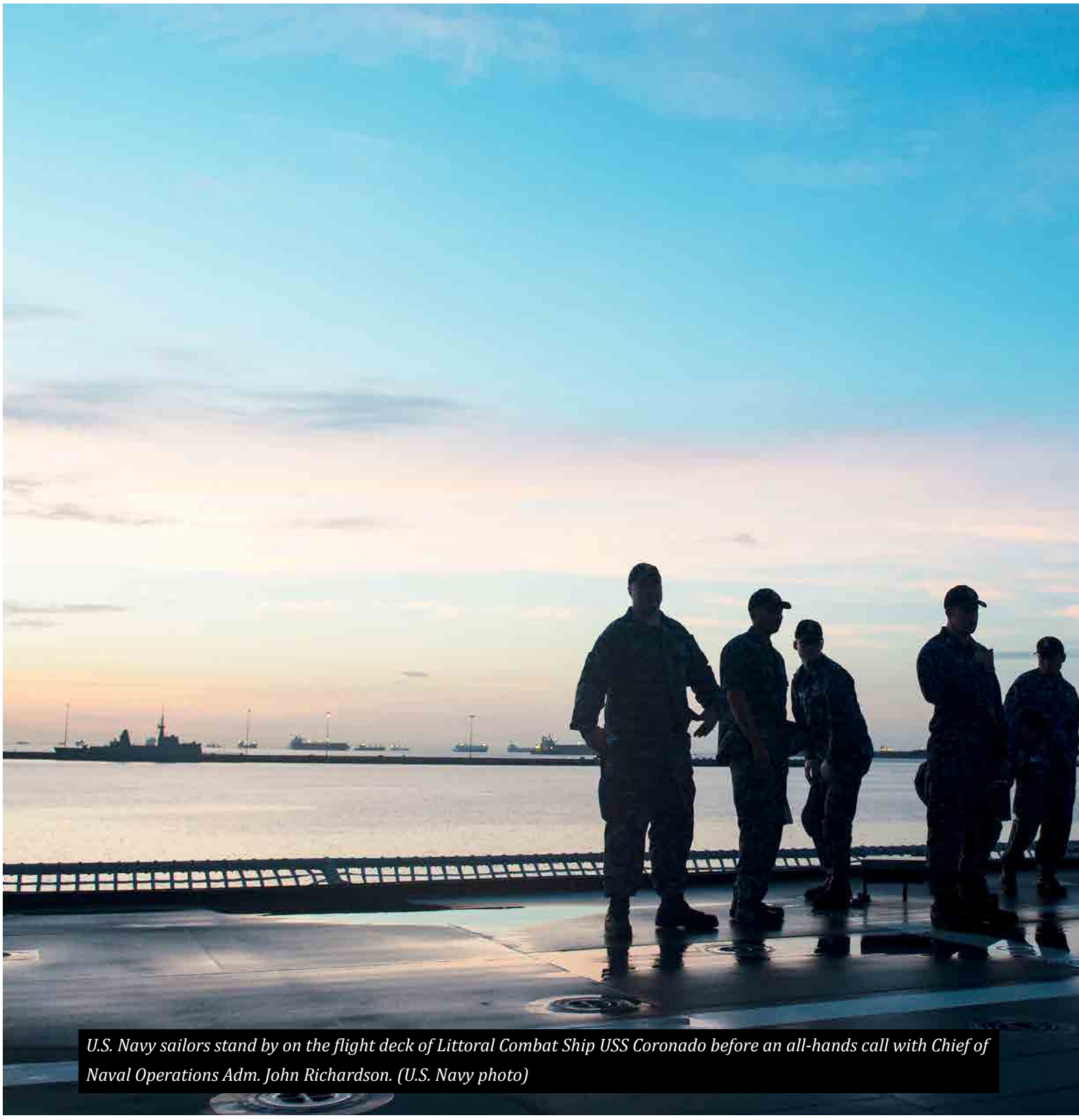
strategies to build, grow, and sustain the Cyber Mission Force. As of October 2016, the DoD reported that all 133 Cyber Mission Force teams had achieved initial operating capability and expected the teams to reach full operating capability by the end of FY 2018. As of June 2017, approximately 5,000 of the 6,200 personnel needed to fully execute critical cyberspace missions within the Cyber Mission Force were staffed.[3]

The shortage of cybersecurity staff directly affects the DoD's efforts to protect its networks from malicious cyber attacks. Although the DoD has made gains in growing 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 the National Guard and, when applicable, integrating them into the DoD's cybersecurity workforce, and expanding partnerships and relationships with Government agencies, as well as the private sector.

In summary, malicious actors will continue to seek unauthorized access to compromise DoD networks, systems, and data. The cybersecurity challenge is that adversaries and defenders constantly innovate and adapt capabilities, and the DoD will need to continually focus attention and resources to protect its networks and information technology assets from increasingly sophisticated cyberattacks. Technological changes will accelerate the intersection of cyber and physical devices, therefore, creating new and more serious risks.

While the DoD continues to take steps to improve security over its systems and networks, significant challenges remain. The DoD needs to continue to evolve its tactics, techniques, and technologies to defend DoD systems, networks, and infrastructure 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, develop and use cyber capabilities to perform offensive and defensive operations, and build and maintain a skilled cyber workforce.

3 USCYBERCOM defines meeting initial operating capability as all CMF teams reaching a minimum threshold of capability to perform their fundamental missions.



U.S. Navy sailors stand by on the flight deck of Littoral Combat Ship USS Coronado before an all-hands call with Chief of Naval Operations Adm. John Richardson. (U.S. Navy photo)

Challenge 5: Improving Financial Management

The DoD is the only Federal agency that has never undergone a full financial statement audit. Moreover, the lack of a favorable audit opinion on the DoD financial statements is the major impediment to a successful audit of the U.S. Government. Long-standing financial management challenges continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information to support reported financial statement balances. Additionally, the lack of reliable financial information prevents its full use in operating, budgeting, and policy decisions.

The DoD's financial management challenges involve a complex array of issues, including maintaining documentation that supports recorded transactions, recording timely and proper accounting entries, maintaining a valid universe of transactions, operating with many decentralized and noncompliant information technology systems, accurately documenting business processes, implementing strong internal controls over accounting data and business operations, and eliminating the need for journal vouchers to force agreement of budgetary, financial, and accounting transactions and balances.

The DoD is required by the Chief Financial Officers Act of 1990 to undergo a full financial statement audit covering its budget, assets, and liabilities. In addition, the National Defense Authorization Act for 2010 specifically requires the DoD to have audit-ready financial statements by September 30, 2017.

In the past, DoD OIG and independent public accounting firm auditors have not conducted a full-scope, detailed audit of the DoD financial statements because the DoD's supporting records have not been suitable for audit. Since the DoD began preparing financial statements in the early 1990s, the DoD Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Military Departments have consistently acknowledged that weaknesses exist with respect to financial reporting. In addition to process design weaknesses and insufficient accounting policies, the DoD could not previously assert that it was able to provide auditors with sufficient evidence to complete a timely financial statement audit.

IMPORTANCE OF STRONG FINANCIAL MANAGEMENT

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. Having sound financial management practices and reliable, useful, and timely financial information is also

important to ensure accountability over the DoD's budgets and assets, and to allow 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.

A key component of sound financial management is an agency's network of internal controls. Strong internal controls include the procedures, requirements, instructions, and checks designed to ensure that agency resources are used effectively and safeguarded properly. For example, within the DoD, key financial management internal controls include leadership commitment to auditability, automated system security, policies and procedures that ensure compliance with accounting standards, checks to ensure adherence to asset or fiscal accountability, documented data reconciliations, performance measurement, and tracking corrective actions to audit findings.

Internal controls are also vital to effective financial management. For example, sound internal controls over asset quantities, asset cost information, item movement, customer requirements, and product ordering help ensure that property location, movement, and costs are known and accurate. Internal controls help prevent waste and even fraud, minimize costs, and allow timely decision making. For example, accurate quantity and cost information is essential to making informed procurement decisions. In addition, when managers can trust that financial data is accurate, improved buying and inventory decisions will result.

With respect to internal control over asset accountability, recent DoD OIG audits had determined that the DoD needs improvements in this area. Specifically, the DoD continues to struggle to provide auditors with detailed asset cost information and to maintain accurate asset quantity information when assets are tracked in multiple property systems. Better internal controls, such as detailed reconciliations and research of quantity discrepancies, would improve the accuracy of financial reports and could improve budgeting decisions because the financial system data would match actual quantities on-hand. When internal controls are strong and on-hand quantities and costs of physical assets are known and accurate, the DoD is able to make the most cost-effective buying decisions. Internal

The U.S. Marine Corps Silent Drill Platoon executes the 'bursting bomb' during a Friday Evening Parade at Marine Barracks Washington, D.C. (U.S. Marine Corps photo)

controls over asset accountability, such as periodic inventories, also minimize the risk of buying more stock than needed.

Unreliable financial information also makes it difficult to accurately develop and execute budgets and to determine the effectiveness and efficiency of military operations. DoD financial management challenges hinder the ability to see potential waste, mismanagement, and cost overruns when certain data is either untimely, unavailable, or inaccurate. For example, auditors of the Military Department's budgetary financial statement have recently concluded that adequate supporting records were not available to complete the audit. The findings demonstrate the difficulty that the DoD has in maintaining accounting control of the hundreds of thousands of transactions that occur all over the world every day.

Yet, internal control weaknesses and noncompliance continue to exist within the DoD's financial feeder systems. Feeder systems contain information that the DoD provides to its accounting agency (the Defense Finance and Accounting Service) to support dollar values reported in DoD financial statements. The feeder systems are decentralized and consist of over 200 significant systems that process millions of transactions reported in DoD financial statements. Independent public accountants have issued hundreds of findings to the DoD related to the lack of internal controls and noncompliant information technology processes in these feeder systems.

Improving financial feeder systems and controls by correcting weaknesses identified by auditors may be the most demanding challenge related to DoD financial management and audit readiness. For example, the DoD reported in its May 2017 Financial Improvement and Audit Readiness Plan Status Report that each Military Department will have uncorrected information technology weaknesses when the FY 2018 financial statement audits begin. As part of improving financial management, the DoD must eliminate outdated

A U.S. Army soldier adjusts the aim of an M777 towed 155 mm howitzer. (U.S. Army photo)

systems and continue to develop and document adequate controls that comply with accounting standards and improve system security.

The DoD also needs to expedite its plan to retire legacy systems while ensuring that remaining systems interface with each other without the need for manual processes to validate that data is transferred accurately. The remaining systems should record, maintain, and disseminate timely and accurate transaction data that decision makers can rely on for financial reporting and for assurance that programs are working and funds are being used properly.

Characteristics of strong financial management include routine and documented reconciliations without the need for thousands of journal vouchers and other adjustments. Sound process improvements would also significantly reduce the current effort being made to reconcile transactions between DoD business partners and minimize the need for processing thousands of journal vouchers.

FINANCIAL AUDITABILITY

Throughout FY 2017, DoD senior leadership has been clear regarding their commitment to undergoing full financial statement audits beginning in FY 2018, as required by statute. For example, in a May 2017 memorandum, Secretary of Defense Mattis stressed the challenge of achieving a clean audit opinion, as well as the importance of improving financial management. The Secretary stated that DoD leadership would

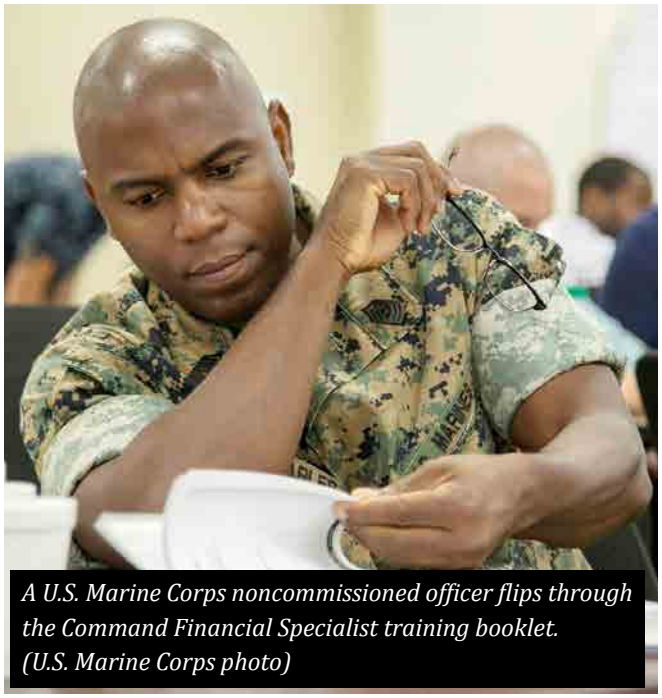
be held accountable for achieving a positive audit opinion in the shortest timeframe possible. He also indicated that undergoing a full financial statement audit is the best tool to improve controls and strengthen business processes and systems.

On September 27, 2017, Secretary Mattis and DoD Comptroller Norquist asserted to the DoD Acting Inspector General that the DoD is ready for a financial statement audit. They added that the DoD was not expecting an unmodified audit opinion on its agency-wide consolidated financial statements, and it was not a certification that the DoD financial statements or components' financial statements are reliable. Rather, they were asserting that the DoD has the capabilities to allow an auditor to scope and perform a full financial statement audit that results in actionable feedback on various financial processes, systems, and documentation.

At the same time, Secretary Mattis notified Congress that the DoD will begin full financial statement audits in FY 2018. He wrote that it will take time for the DoD to go from being audited to passing an audit. He noted that "Direct feedback from auditors keeps audit remediation in the forefront of our day-to-day work and helps us to be accountable to DoD decision-makers as well as responsive to you and other stakeholders."

In addition, Deputy Secretary of Defense Shanahan wrote a memorandum to all DoD employees stating the DoD's support for the FY 2018 financial statement audits. He wrote that he expected everyone to make it a priority to correct problems identified in these audits. He noted "This Department is the last federal agency to not have a clean agency-wide financial opinion. This must change. We must lead and not lag behind." He added that the audits will give DoD leaders and commanders the reliable information they need to exercise judgment and accomplish their mission.

Other DoD leaders have also initiated actions to obtain buy-in from all personnel involved in the recording and reporting of financial data. For example, Army leaders have stressed the importance of audit readiness in an Army-specific publication for functional components to support audit readiness.



A U.S. Marine Corps noncommissioned officer flips through the Command Financial Specialist training booklet. (U.S. Marine Corps photo)

In addition, the DoD pursued initiatives to support audit readiness or improve overall financial management. For example, the Financial Improvement and Audit Readiness Directorate continues to work toward improving the quality of DoD financial information with a positive audit opinion as the desired outcome. The Financial Improvement and Readiness Directorate provides DoD reporting entities the key tasks and requirements that should be followed to become audit ready. The DoD has also created working groups to ensure that solutions to its financial management challenges comply with accounting standards and can pass auditor testing. The groups are working to address long-standing accounting weaknesses, including Fund Balance With Treasury reconciliation, property valuation documentation, and a full account of billions of dollars in payments to DoD contractors. Further, the DoD continues to update the Financial Management Regulation and issue policy memorandums designed to improve accounting operations and establish standard and sustainable processes.

U.S. Air Force explosive ordnance disposal technicians assigned to the 99th Civil Engineer Squadron walk onto a range for training. (U.S. Air Force photo)

The DoD's definition of "audit ready" and the DoD Comptroller's position that a clean audit opinion is not expected immediately demonstrates that, while progress has been made, the magnitude of what remains to be done to achieve a favorable opinion is significant. Even if the DoD does not obtain clean audit opinions immediately, the DoD OIG agrees that performing full financial statement audits can provide benefit to the DoD. Financial statement audits can help DoD leadership ascertain where financial and other business processes are working as intended, and where specific deficiencies need to be corrected.

CURRENT STATUS OF DOD FINANCIAL STATEMENT AUDITS

The DoD continues to award financial statement audit contracts for entities that have asserted audit readiness. In FY 2016, the DoD contracted for seven financial statement audits and three Military Department budgetary statement audits. The U.S. Army Corps of Engineers, the Military Retirement Fund, and Defense Health Agency-Contract Resource Management all passed FY 2016 audits with unmodified audit opinions. In addition, the results of the Defense Information Systems Agency financial statement audit were generally favorable in that one of its two business segments attained a clean opinion. Other FY 2016 audits were not as successful. Independent public accountants determined that the Military Department budgetary financial statements were not audit-ready and thus the auditors disclaimed opinions.

In FY 2017, the Defense Logistics Agency (DLA) and the Marine Corps underwent a full financial statement audit. However, the independent public accountants determined that DLA and Marine Corps personnel were not able to provide sufficient documentation to the auditors to perform a full audit. In addition, independent public accountants continue to perform audits of FY 2017 Army and Air Force budgetary records. Recently, these independent public accountants notified Army and Air Force leadership that the auditors were not provided sufficient documentation to perform a full audit and that the auditors plan to issue disclaimers of opinion on the budgetary financial statement.

Other audit contracts continue to be awarded, including those for the FY 2018 financial statement audits of the U.S. Special Operations Command, the U.S. Transportation Command, and the Defense Health Program. In addition, actions have been taken to award contracts or exercise

A U.S. Army soldier with Assassin Troop, 1st Squadron, 11th Armored Cavalry Regiment, scans the battlefield. (U.S. Army photo)

options so that independent public accountants can perform FY 2018 financial statement audits of the Military Departments. The CFO Act requires that the DoD OIG either perform or contract for DoD financial statement audits. To fulfill this responsibility, the DoD OIG performs oversight of the contractors to ensure that the independent public accountants follow auditing standards, comply with DoD security policies, and meet contract requirements.

DoD OIG audits have found a lack of supporting documentation for account balances and system data that are not reliable, accurate, or timely. In addition, asset information, such as certain inventory and equipment balances, continue to lack sufficient valuation documentation, and sometimes lack accurate location and quantity information. These deficiencies have consequences. For example, inaccurate inventory and equipment counts can result in DoD personnel placing orders for new parts or equipment even though there are sufficient supplies in stock. Likewise, inaccurate asset information limits the DoD's ability to ensure material and equipment are available for operational readiness if actual on-hand balances are lower than balances in the property system.

Other DoD OIG financial management audits continue to identify the need for improved financial management controls and reporting. In FY 2017, the DoD OIG issued reports that highlighted problems with Fund Balance With Treasury reconciliations, ineffective financial management system strategies, and inaccuracies in reported costs of programs. As of July 2017, 172 open DoD OIG recommendations related to DoD finance and accounting topics, such as management of DoD suspense accounts, transactions that support financial statements and budget submissions, and DoD financial management and accounting systems.

Implementing the necessary actions to close these recommendations has proven challenging for the DoD because business processes and accounting policies need to be reviewed, improved, and monitored. For example, the DoD's implementation of new integrated logistics and accounting systems that include proper internal controls, such as compliant and timely accounting entries, has been slow and costly. When the property systems of record include accurate account balances, reliance on these balances, such as physical asset counts or cost information, can result in efficient buying decisions

WHAT'S LEFT TO DO — AN AUDITOR PERSPECTIVE

Although the DoD plan to conduct its full financial statement audits beginning October 1, 2017, as required by law, numerous key challenges continue to face the DoD when preparing for the FY 2018 and subsequent financial statement audits. According to the DoD, a key indicator of its FY 2018 audit readiness will be its ability to respond to auditors' requests for supporting documentation. This indicator is very different from the normal objective of a financial statement audit, which is to determine whether the agency's financial statements are fairly presented in all material respects in accordance with U.S. Generally Accepted Accounting Principles. For the FY 2018 financial statement audits, the DoD needs to clearly demonstrate the extent to which it has remediated the material weaknesses previously identified. Remediating these weaknesses requires improved internal controls, systems, and data reliability. Evidence that these weaknesses have been corrected will contribute to auditable financial

statements that contain complete, reliable, timely, and consistent data for financial management decision making.

The major impediments to auditability require the DoD to improve, and in some cases change, its way of doing business. Long-standing business processes that have supported DoD missions are not always sufficient for an audit. For example, audits conducted by independent public accounting firms of the Military Department's FY 2016 budgetary financial records cited more than 700 combined findings and recommendations that revealed individual and systemic issues that prevented the auditors from opining on the Military Department budgetary statements. These audit results demonstrate that current DoD business practices need to be redesigned to support Federal accounting policies and information technology requirements.

DoD OIG and independent auditors have consistently found that the DoD needs to develop sustainable and repeatable processes to better respond to audit requirements and provide timely and sufficient supporting documentation for transactions.

To achieve and sustain reliable financial data, the DoD must also focus on other high-risk areas, such as the ability to eliminate the use of journal vouchers as a means of addressing unsupported or unreconciled accounting transactions. DoD accountants use journal vouchers for various reasons, such as to adjust errors identified during financial statement compilation; record accounting entries that, due to system limitations or timing differences, have not been otherwise recorded; or for month and year-end closing purposes. For decades, DoD accountants have prepared journal vouchers as a means to complete financial reporting requirements and force balances to agree without detailed reconciliation processes to fully support and explain the accounting adjustment. Unsupported journal vouchers and unresolved differences between the DoD and the Department of the Treasury have contributed to unfavorable audit results on prior DoD financial statements.

Another area of significant concern that delays an auditor's ability to opine on financial statement balances is the lack of a verifiable universe of transactions from the outset of the audit. The DoD recognizes the need for detailed transactions and continues to work internally with stakeholders to develop a complete universe of transactions that reconciles from feeder systems to its financial statements.

Further, the DoD must be able to account for the assets reported on its balance sheet, including adequate support for how much assets cost, how much the DoD owns, and where the assets are located. These challenges must be addressed as the DoD pursues its plan to reduce the number of financial and feeder systems.

With the heightened level of review and scrutiny of full financial statement audits, the DoD should anticipate additional independent public accountant audit findings and recommendations. The DoD needs to be prepared for this additional workload and have the capability to prioritize the current and new weaknesses and recommendations into an efficient plan for success. The need for corrective actions to address current and newly identified material weaknesses and deficiencies will compete for tight resources in the future.

In summary, the DoD plans to have its largest agencies under financial statement audit in FY 2018, including the Military Departments and many Defense agencies. DoD leaders have acknowledged that there are still corrective actions to be implemented and remediation efforts to be completed before unmodified audit opinions can be achieved. Without these corrections, the DoD financial statements will continue to remain unreliable and affect the DoD's ability to make important financial, management, and resource decisions.

U.S. Army soldiers with the 20th CBRNE Command's CBRNE Leaders Course bound forward during a squad movement training exercise. (U.S. Army photo)

Challenge 6: Maintaining the Nuclear Enterprise

Maintaining a secure and effective nuclear deterrent is a key priority, and an important challenge, for the DoD. U.S. nuclear weapons serve as a deterrent to attacks by adversaries armed with nuclear weapons or other weapons of mass destruction. A credible and capable U.S. nuclear force also provides security for U.S. allies and reduces pressure for them to field their own nuclear weapons.

GLOBAL THREAT OF NUCLEAR WEAPONS

In April 2017, General John Hyten, the Commander of U.S. Strategic Command and the individual responsible for overseeing U.S. nuclear forces, stated that the global security environment has changed—the United States' adversaries are developing advanced nuclear and conventional weapons that rival U.S. capability. As noted above, Secretary of Defense Mattis identified five entities that present the greatest challenges for the DoD: Russia, China, Iran, North Korea, and violent extremist organizations. Of the five, Russia, China, Iran and North Korea are actively modernizing or expanding their nuclear and strategic strike capabilities. The extremist threat, on the other hand, can be unpredictable, and requires vigilance in monitoring their efforts to obtain a nuclear weapon or other weapon of mass destruction.

In a June 12, 2017, written statement, Secretary Mattis testified that the most urgent and dangerous threat to global peace and security is North Korea. Secretary Mattis stated that North Korea's continued pursuit of nuclear weapons and the means to deliver them has increased in pace and scope. He also stated, "The regime's nuclear weapons program is a clear and present danger to all, and the regime's provocative actions, manifestly illegal under international law, have not abated despite United Nations' censure and sanctions."

Comparatively, Russia has well-developed nuclear capabilities. According to the Defense Science Board, Russia's nuclear doctrine is publicly stated as "escalate to de-escalate," based on Russia's assumption that its first use of low-yield nuclear weapons against a conventionally superior North Atlantic Treaty Organization forces would result in a halt to further aggression.

China, on the other hand, has maintained a "no first use" policy, stating that it would use nuclear forces only in response to a nuclear strike against China. The DoD's May 2017 Annual Report to Congress on the military and security developments of the People's Republic of China noted that some People's Liberation Army officers have written publicly of the need to specify situations when China might need to use nuclear weapons first. The People's

Liberation Army officers stated an example of first use could be if an enemy's conventional attack threatened the survival of China's nuclear force or the regime itself.

Iran's development of nuclear capabilities is a significant risk, notwithstanding the Joint Comprehensive Plan of Action, signed on July 14, 2015, by China, France, Germany, Russia, the United Kingdom, the United States, the European Union, and Iran, which established monitoring and verification of Iran's nuclear program. In July 2017, the State Department criticized Iran's successful launch of a rocket that can carry satellites into orbit. The State Department stated that the launch appeared to violate United Nations Security Council Resolution 2231, tied to the 2015 Iran nuclear deal, prohibiting Iran from conducting activities related to the development of ballistic missiles capable of carrying nuclear warheads.

In addition, extremist organizations, such as ISIS, continue to threaten the United States, and express the desire to obtain nuclear weapons. To deter the nuclear threat, the United States must ensure that its nuclear weapons, weapon systems, and command and control needed to use those weapons are capable and effective.

SIMULTANEOUS SUSTAINMENT AND MODERNIZATION OF THE U.S. NUCLEAR TRIAD

Since the early 1960s, the United States has maintained a nuclear triad consisting of three systems capable of delivering strategic nuclear weapons. The first consists of long-range bombers, which can launch and be recalled if the identified threat subsides. The second consists of Intercontinental Ballistic Missiles, which are strategically placed in large enough numbers that an attack against them would have to be massive and unambiguous. The third consists of the submarines that carry Submarine Launched Ballistic Missiles. By staying submerged and undetected, these submarines are survivable even if the other two systems of the triad are destroyed through a massive nuclear attack.

The triad of delivery systems has been modernized twice, once in the early 1960s and again in the 1980s. The average warhead is now over 29 years old. According to General Paul Selva, Vice Chairman of the Joint Chiefs of Staff, every system, including elements of the Nuclear

A B-52 Stratofortress waits to approach a 908th Expeditionary Air Refueling Squadron KC-10 Extender for refueling over Syria. (U.S. Air Force photo)

Command, Control, and Communications system, is nearing a crossroads and will require significant modernization or replacement.

In March 2017, General Selva testified that the DoD is at a point where it must concurrently recapitalize each component of the nuclear deterrent. He also stated that nuclear modernization can no longer be deferred and any disruption to future acquisition plans will introduce significant risk to the U.S. nuclear deterrent. General Hyten also testified during the same hearing that Russia and China have modernized and upgraded their nuclear forces.

In January 2017, Secretary of Defense Ashton Carter wrote an exit memorandum that discussed the progress the DoD had made in its efforts to recapitalize the nuclear triad. The memorandum stated that:

- The DoD had initiated the program to build the Columbia-class nuclear ballistic missile submarine to replace the Ohio-class submarine.
- The DoD selected a designer for the B-21 Raider long-range strike bomber, which will ensure that the United States maintains a bomber capable of penetrating a sophisticated air defense system.
- The DoD is developing the Long-Range Standoff cruise missile, which will replace the air-launched cruise missile starting in 2030.
- The Air Force is continuing production of the F-35 Joint Strike Fighter, which will be updated to assume the role of dual-capable aircraft and provide the United States and its allies with continued non-strategic nuclear capabilities.
- The Air Force has begun the process for replacement of the Minuteman III Intercontinental Ballistic Missile system to continue providing a stable and responsive deterrent capability.

The DoD's efforts to modernize and sustain the nuclear triad require adequate funding. The February 2017 Congressional Budget Office estimated that the DoD will need to spend $267 billion for strategic nuclear delivery and command and control systems over the next 10 years. The Congressional Budget Office projects that the estimated cost, by function, will be:

- $80 billion for the new ballistic missile submarine
- $39 billion for the new intercontinental ballistic missile
- $34 billion for the new bomber
- $6 billion for tactical nuclear delivery systems and weapons
- $14 billion for nuclear command and control
- $20 billion for nuclear-related communications systems
- $24 billion for early-warning systems
- $13 billion for nuclear-related research and operations support activities by the DoD that the Congressional Budget Office could not associate with a specific type of delivery system or weapon

Even if adequate funding is provided, modernization and sustainment of the nuclear triad will be not be assured. The DoD OIG has regularly assessed the DoD's efforts to sustain current components of the nuclear enterprise and found significant challenges. The DoD OIG issued six

An unarmed U.S. Air Force Minuteman III intercontinental ballistic missile launches during an operational test. (U.S. Air Force photo)

evaluations between 2014 and 2017 that identified significant parts obsolescence and manufacturing shortages due to closure of many small companies that provided support for the parts. Additionally, the DoD OIG evaluations determined that Air Force and Navy senior leaders were not aware of the identified sustainment challenges or the operational practices at the unit level that drove some of the obsolescence and shortage challenges.

According to DoD OIG reports issued in 2014 and 2016, the Air Force has made progress by initiating more robust quality assurance processes to identify mission-essential parts and suitable substitutes for the Minuteman III Intercontinental Ballistic Missile (ICBM) and the Integrated Tactical Warning and Attack Assessment's Ground Based Radars. Furthermore, Air Force Global Strike Command developed metrics tailored to the Minuteman III system, these metrics include measures related to infrastructure support, helicopter security-response capability, and communications. The development of these metrics provide an enduring and standardized measure of effectiveness of the supply chain support to the Minuteman III ICBM.

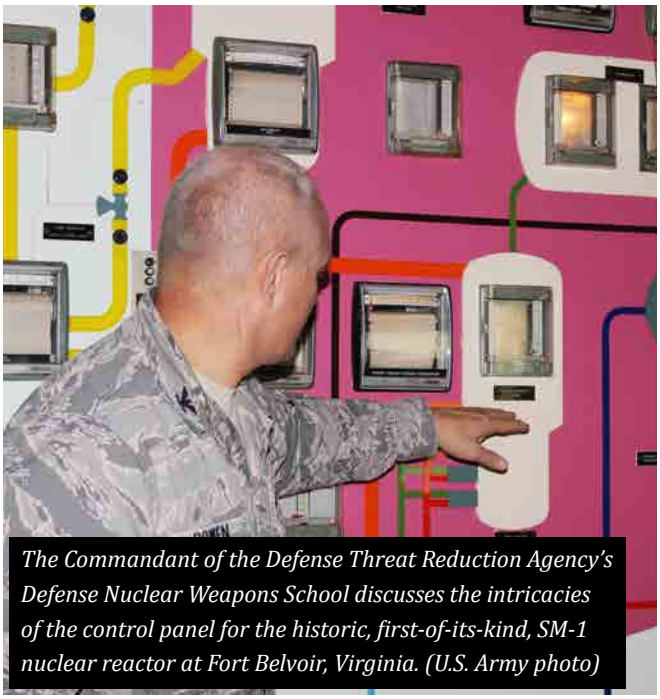
Yet, additional progress is required. For example, a 2012 DoD OIG report recommended that the Air Force acquire a new helicopter to support ICBM field operations. As of 2017, the Air Force has still not implemented this recommendation. As a result, the Air Force continues to use the UH-1N, which lacks the range, capacity, and endurance to meet current requirements. Air Force UH-1N helicopters have been performing the nuclear support mission since 1969. The helicopter airframes suffer from age-related cracks in rotor hubs, the lift-beam area, and tail-boom assemblies. As far back as 2011, the Commander, Air Force Global Strike Command, stated that it is a "Herculean effort to keep the Vietnam-era helos in the sky."

A 2014 DoD OIG report determined that the Navy has also made significant progress in addressing sustainment challenges with its nuclear command and control facilities. The Navy implemented actions to improve its preventive maintenance

U.S. Army soldiers with the 51st Chemical Biological Radiological Nuclear Company, prepare to treat victims at a decontamination field site. (U.S. Army Reserve photo)

procedures, improve its deficiency reporting, and strengthen its inspection system related to backup power systems and other supporting infrastructure. The Navy reinvigorated maintenance and material management for the Fixed Submarine Broadcast System, a global network of very low frequency antennae. By developing standard operating procedures and power plant maintenance plans, the Navy improved material readiness and sustainment of the 1950s-era system.

Despite efforts to sustain nuclear delivery platforms, nuclear support infrastructure, and Nuclear Command, Control, and Communications systems, the DoD OIG evaluations determined that those systems are deteriorating at a faster pace than their scheduled replacement. To assess these challenges, the DoD OIG plans to evaluate whether the Ohio-class nuclear ballistic missile submarine can be sustained until the Columbia-class nuclear ballistic missile submarine is operational. Planned maintenance actions for the Ohio-class have become increasingly longer, which reduces the number of available submarines for patrol. This is due to increased deterioration of the submarines and incorporating upgrades to meet current threats. Based on the commission date of the Ohio-class submarine, its 30-year projected life



The Commandant of the Defense Threat Reduction Agency's Defense Nuclear Weapons School discusses the intricacies of the control panel for the historic, first-of-its-kind, SM-1 nuclear reactor at Fort Belvoir, Virginia. (U.S. Army photo)

cycle would have ended between 2017 and 2030. However, some of the submarines will reach up to 42 years of service by the time the first Columbia-class submarine is fielded.

Overall, DoD senior leaders agree that nuclear modernization can no longer be deferred and any disruption to future acquisition plans will increase risk to the U.S. nuclear deterrent. Simultaneously modernizing the triad and elements of nuclear command and control while sustaining legacy platforms and systems remains a top DoD challenge.

NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS

In addition, the U.S. nuclear deterrent is only as effective as the command and control network that enables it to function. Nuclear Command, Control, and Communications systems must be reliable and resilient because they are essential for providing time-critical early warning information to the President and Secretary of Defense for decision-making, as well as effective direction of the nuclear forces in response to a strategic crisis. The magnitude of Nuclear Command, Control, and Communications systems is reflected in the combined $34 billion annual proposed costs over the next 10 years for their modernization. However, any cancellation or delay of Nuclear Command, Control, and Communications modernization programs increases the risk to the critical communication capability and potentially degrades the U.S. Government's ability to respond to a nuclear threat.

The DoD needs to transition Nuclear Command, Control, and Communications from outdated analog systems that transmit simple coded messages from point to point. The President, Secretary of Defense, and all levels of leadership, down to individual units, rely on video conferencing and large amounts of near real-time data to conduct conventional warfare. Yet, decisions on the use of nuclear weapons are communicated through a totally different nuclear communications network that is antiquated and often unfamiliar to leadership. However, using new technologies, such as IP-based networks, to upgrade nuclear communication systems for senior leaders increases the risk of exploitable vulnerabilities and disruptions.

The DoD OIG issued five reports between 2013 and 2017 assessing the DoD's efforts in improving Nuclear Command, Control, and Communication infrastructure. By resolving findings and implementing recommendations from these five reports, the Air Force and Navy have made progress in improving the readiness or effectiveness of the National Airborne Operation Center, early warning radars and communication systems, and the security of data passing through multiple communication systems.

To improve its ability to manage Nuclear Command, Control, and Communication, the Air Force established the U.S. Air Force Nuclear Command, Control and Communication Center in April 2017. The Air Force also designated its portion of the Nuclear Command, Control, and Communications system as a weapon system, which the Air Force believes will improve sustainment and modernization efforts by establishing a

Sailors stand topside aboard the Virginia-class, nuclear-powered, fast-attack submarine USS Missouri as the boat approaches the pier at Naval Submarine Base New London, Connecticut. (U.S. Navy photo)

foundation to address the weaknesses identified in DoD OIG evaluations. The Navy also increased its focus on Nuclear Command, Control, and Communications. For example, in 2015 the Navy took actions to resolve Nuclear Command, Control, and Communication recommendations from an evaluation report on the Navy's Fixed Submarine Broadcast System. The Navy revised the organizational structure to enhance accountability, appointed a single authority for Fixed Submarine Broadcast System issues, increased inspections, and funded recommended system upgrades.

While the DoD has made progress in protecting the security of the Nuclear Command, Control, and Communications infrastructure, deferred maintenance and schedule delays affect sustainment and modernization of the infrastructure. For example, DoD OIG reports have determined that:

- programs did not meet system requirements or lacked configuration control;
- personnel inappropriately waived preventive maintenance on nuclear support equipment, such as generators and backup power supplies; and
- system sustainment planning was inadequate, forcing continued reliance on old technology, such as vacuum tubes, punch cards, floppy disks and other outdated systems

The DoD OIG is planning additional reviews in this area, such as an evaluation of U.S. European Command's ability to effectively direct, control, and execute the non-strategic nuclear mission.

Modernizing Nuclear Command, Control, and Communications to provide leadership with a reliable, secure communication system is vital to ensuring a continued credible nuclear deterrent.

MAINTAINING ROBUST INTELLECTUAL CAPACITY

Federal advisory committees, the Defense Science Board, the GAO, and the DoD OIG have all identified the reduction in the number of DoD personnel with nuclear expertise as a challenge. The DoD is faced with an aging civilian nuclear workforce coupled with difficulties in recruiting and retaining new personnel.

For example, as DoD nuclear civilian experts retire, the DoD is challenged to find qualified replacements. A contributing factor to this

challenge is that the DoD lacks a formal career progression path for the civilian nuclear workforce. Furthermore, junior personnel entering the DoD workforce are not trained on 1950s- and 1960s-era vacuum tubes or other early technology used in the nation's nuclear weapons and command and control systems.

Also, in part, DoD OIG evaluations determined that some nuclear command and control sites cannot fill critical technical positions because of the austere work locations. Site managers have stated to the OIG this challenge is "two-fold." First, the technical positions require advanced education and certifications, but the organizational size and locality only allows for lower general schedule salaries not commensurate with the qualifications needed. Second, site managers have found that the lack of large local retail establishments hurts recruitment.

In recent years, the DoD has taken steps to improve capabilities of nuclear personnel through partnerships with universities. U.S. Strategic Command has established an academic alliance program focused on developing a community of interest on deterrence in the context of national security, with 20 universities and military higher-education institutes.

Despite these steps, challenges remain for the DoD to ensure that critical nuclear positions are filled. The DoD should pursue targeted recruitment and provide an appropriate career path to build the depth of experience and knowledge needed to replace the retiring nuclear experts. This pool of talent needs sufficient incentives to take on critical functions in some of the austere locations.

GOVERNANCE

Over the last decade, the lack of an effective DoD governance structure to maintain a secure and effective nuclear deterrent has been documented in various federal advisory reports, DoD internal assessments, and DoD OIG reports. For example, the DoD does not assign a person or organization to ensure that nuclear capabilities are planned, resourced, modernized, or sustained in an integrated fashion by all DoD Services and organizations involved in nuclear operations. Multiple committees, with overlapping memberships, address governance issues in the nuclear enterprise, but many of these committees are merely advisory or coordination committees and cannot commit resources. In December 2015, the President directed the DoD to establish and chair a Security and Incident Response Council to manage a whole-of-government approach to securing and responding to incidents that may occur in the U.S. nuclear weapons stockpile. However, the DoD has not yet established this Council, making it one of our most critical unresolved DoD OIG recommendations.

In addition, at the program or system level, the DoD OIG has noted instances when the lack of funding or programmed sustainment was a governance issue. For example, the Nuclear Detonation Detection System has many stakeholders, but they do not have a venue to decide on programmatic adjustments based on changes in threats, presidential guidance, or funding challenges. Agreements for cost sharing have expired, and some stakeholders have unilaterally dropped their funding contributions, forcing other organizations to budget for the additional funding.

In summary, the DoD has focused on the critical task of modernizing its nuclear force. However, the DoD must balance the risk between sustainment of the current nuclear force and the modernization and acquisition of future nuclear capabilities. The DoD needs to make additional progress on the governance of the nuclear force and identify a means for attracting and retaining a skilled civilian nuclear workforce. U.S. adversaries are committed to developing and adapting nuclear capabilities, which increases the importance of continual progress by the DoD in this area.

The guided-missile destroyer USS Porter conducts strike operations against a target in Syria while in the Mediterranean Sea. (U.S. Navy photo)

Challenge 7: Optimally Balancing Readiness, Modernization, and Force Structure

Balancing readiness, modernization, and force structure is a significant and enduring challenge for the DoD. It must build and maintain readiness across the current force to meet today's requirements, while also modernizing and transforming the force to meet future demands.

In a June 2017 hearing before the Senate Appropriations Committee, Secretary of Defense James Mattis outlined five priorities for the DoD:

- continue to improve upon war fighter readiness initiatives started in 2017,
- increase capacity and lethality while preparing for future investment,
- reform how the DoD does business,
- keep faith with service members and their families, and
- support overseas contingency operations.

The priorities help the DoD balance its resources and initiatives to meet global demands across the range of military operations while investing in modernizing the force for the future.

READINESS

Readiness is the ability of military forces to fight and meet the demands of assigned missions. Manning, training, and equipping are the three elements of readiness. Rebuilding and maintaining readiness after more than 16 years of continuous conflict competes with the need to modernize and to adjust force structure. Increasing the size of the military, its force structure, without corresponding investments in readiness risks the creation of a "hollow force" that is insufficiently manned, trained, or equipped to defend the nation's interests.

MANNING

The DoD is the largest employer in the United States with over 2.1 million active duty, National Guard, and Reserve members serving in uniform, and over 800,000 civilian personnel. DoD leadership recognizes that the strength of the DoD is its people. All Services must remain competitive in their efforts to recruit, develop, and retain the right mix of talented and skilled people willing and able to serve.

Maintaining a force with the right mix of skills and experience for an ever-changing, globally deployed force is a challenge across the DoD. For example, in June of 2017, Army Chief of Staff Mark Milley testified before the Senate

Appropriations Committee that the Army did not have enough soldiers to accomplish its assigned missions. The Chief of Staff further stated that the active component size of the Army should be between 540,000 and 550,000, the National Guard between 350,000 and 355,000, and the Army Reserve between 205,000 and 209,000. The Active Army currently has 476,000, the National Guard has 343,000, and the Army Reserve has 199,000 uniformed personnel.

In May of 2017, the Government Accountability Office (GAO) found that reductions to crew sizes the Navy made in the early 2000s were not analytically supported and may now be creating safety risks. The GAO also found that the work-week standard used by the Navy did not reflect the actual time sailors spent working and did not account for in-port workload—both of which have contributed to some sailors working over 100 hours a week. The GAO concluded that until the Navy changes its factors and policies used in determining manpower requirements, its ships may not have the right number of skilled sailors to maintain readiness. Additionally, the Navy may not have the ability to reduce the 100-hour, per-week demand, and the manning issue may become more prevalent as the Navy seeks to increase the size of its fleet.

The Air Force identified shortages of skilled maintenance personnel and pilots as that service's principal readiness challenge. As a result, the Air Force continues to prioritize maintenance personnel in its training pipeline as the Air Force requests to grow its active duty end strength to 325,100 in FY 2018. At the start of FY 2017, the Air Force reported a deficit of 1,555 pilots across all mission areas. This shortage resulted from high operational tempo and the civilian airline industry's demand for former Air Force pilots. To address this shortage, the Air Force plans to use bonuses and other initiatives to retain pilots. In addition, the goal of an ongoing Air Force personnel review is to reduce the number of pilots serving in non-flying positions.

These are only a few examples of the challenges faced by the DoD with regard to manning. However, manning is only part of the readiness equation — to be ready, troops must be trained.

TRAINING

Across the Joint Force, the high operational tempo is impacting the training that is required to maintain military readiness. The lack of funding or time for training presents a serious concern for the U.S. military's ability to remain a ready force. The DoD must find innovative ways to meet the operational demands on the force and while continuing to conduct adequate training. Training to meet requirements across the range of military operations, while sustaining an unrelenting operational tempo and balancing competing demands for resources, is a challenge common to each Service.

In January of 2017, the President ordered a 30-Day Readiness Review of the Armed Forces. This review initiated the development of the "DoD Request for Additional Fiscal Year 2017 Appropriations" that identified the issues requiring additional funding. Training to improve near-term readiness was one of these issues.

For example, the DoD requested additional funding for the Army to increase training and readiness for operating and generating forces. The DoD reported that this increase would provide more realistic training at the National Training Center, mitigating safety and maintenance issues, and enabling the National Training Center to replicate the tactics and capabilities of potential nation-state adversaries. The goal of the funding request was to increase ground operational tempo and flying hours, enabling both Active and Reserve Component units to train to higher levels, thereby building readiness and making more units ready and available for global contingencies. This training is designed to improve readiness levels and to assess readiness. In FY 2018 the DoD OIG plans to review whether Army and Air National Guard units are accurately reporting personnel readiness levels.

The Ticonderoga-class guided-missile cruiser USS Lake Champlain is moored pier side in Singapore with the Carl Vinson Carrier Strike Group. (U.S. Navy photo)

The DoD also requested funding for the Navy to support maintenance and upgrades to 14 additional surface ships in FY 2017. The additional funding seeks to help the additional ships to begin training on time for their next deployments with improved material condition and modernization to combat systems, communications, and engineering systems. The increased funding would also enable the Navy to add 14,000 flying hours to support tactical training for 5 carrier air wings and 33 non-carrier squadrons.

Recent collisions involving Navy ships are an example of a potential readiness shortfall due to training deficiencies. In response to these collisions, Admiral Philip Davidson, Commander of Fleet Forces, is leading a 60 day comprehensive review to examine training, individual development, and certifications.

In March of 2017, the Maine Corps Times reported that the Marine Corps is facing a critical gap in scout snipers due to lower than anticipated graduation rates for scout sniper schools over the past several years. To address this gap, the Marine Corps is considering dividing sniper training into two sessions, then assigning students to an operational unit between sessions to provide more on-the-job experience.

As part of a request for additional appropriations, the Air Force sought funds for military construction to improve its training environment and infrastructure and to strengthen facility operations through sustainment and restoration. The Air Force stated that its number one readiness priority is funding 4,000 airmen in joint critical mission areas: maintenance; aircrew; intelligence, surveillance, and reconnaissance; cyber; and battlefield airmen. The funding would also expand training and recruiting capacity to support end-strength growth to fill these capability gaps.

Additionally, during his Senate Armed Services Committee testimony on June 6, 2017, the Air Force Chief of Staff David Goldfein stated that the shortage of key personnel and the focus on providing support for the fight against extremist groups is preventing training designed to confront other major adversaries. He attributed the driving factor for this readiness shortfall as the current size of the Air Force in relation to the expanded mission requirements and the increased capabilities of U.S. adversaries.

In September 2017, a GAO report found that select Marine Corps personnel had limited capacities to perform training missions for amphibious operations and other related priorities. The GAO

U.S. marines with Bravo Battery, 1st Battalion, 10th Marine Regiment, 2nd Marine Division, provide security during a CH-53 day battle drill. (U.S. Marine Corps photo)

report stated that the decline in the number of active Navy amphibious ships also affected the Marine Corps training capacities for priority areas, such as recurring training for home-station units. While the Navy and the Marine Corps have begun to address the challenges related to amphibious training, the GAO recommended that the Navy and the Marine Corps increase coordination and implement collaborative practices to aid the naval integration of amphibious operations.

EQUIPPING

The ability to efficiently "reset" equipment after deployment is a persistent challenge for the DoD. Equipment reset consists of the actions taken to reconstitute units and equipment to a desired level of combat capability required for future missions. In his testimony before the Senate Armed Services Committee regarding the FY 2018 budget, Secretary Mattis stated that 16 years of continuous conflict has "exhausted our equipment faster than planned." The cost associated with maintaining equipment further adds to the DoD challenge in balancing investments to sustain existing equipment with investments in the development and acquisition of new equipment.

The Chairman of the Joint Chiefs of Staff General Joseph Dunford, Jr. articulated this challenge in his statement at the same hearing with Secretary Mattis, stating:

> Since 9/11, an extraordinarily high level of operational tempo has accelerated the wear and tear of our weapons and equipment. Meanwhile, budget instability and the Budget Control Act have forced the DoD to operate with far fewer resources than required for the strategy of record. As a consequence, we prioritize near-term readiness at the expense of replacing aging equipment and capability development. We also maintain a force that consumes readiness as fast as we build it. We lack sufficient capacity to meet our current operational requirements while rebuilding and maintaining full spectrum readiness.

Secretary Mattis added that units back at home station are "unable to train as equipment is sent forward to cover shortfalls or returned for extensive rework." One of the DoD's strategies to address equipping issues it to reuse equipment that is no longer needed by one unit by repairing and reissuing it to another unit. In FY 2018, the DoD OIG plans to determine whether the Defense Logistics Agency-Disposition Services is properly reutilizing and disposing of equipment in Kuwait.

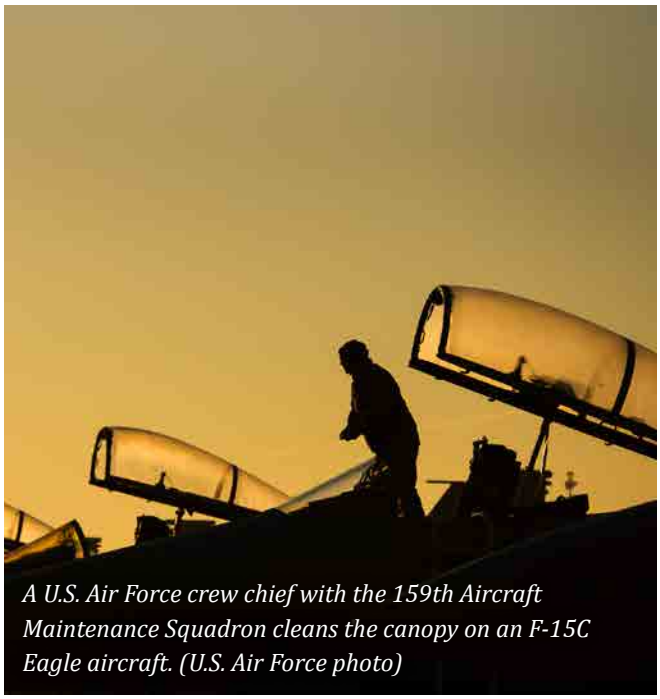
MODERNIZATION

Over 16 years of continuous conflict, current readiness has necessarily been a higher priority than modernization. However, DoD's capacity for technological innovation remains integral to its ability to dominate any enemy. Realizing that the U.S. technological advantage was declining, the 2014 Quadrennial Defense Review established innovation as a central effort of the new Third Offset Strategy. Now in its second year of implementation, the strategy seeks to combine

new technological innovations with supporting doctrine describing how to effectively employ new equipment and formations in combat. Recent initiatives include the F-35 Joint Strike Fighter, the emerging B21 Bomber, the Aegis Ballistic Missile Defense and Theater High Altitude Area Defense missile systems, counter drone technologies, and directed energy weapons. In an effort to produce a balanced and lethal force, the DoD plans to combine these newly acquired technologies with short-term modernization programs that are designed to enhance the lethality and survivability of existing U.S. weapons systems.

Determining whether to divest or retain existing capabilities is another aspect of the modernization challenge. The DoD's divestiture decision process relies on the analysis of current needs compared to anticipated future requirements. This analytical decision process also identifies any identified gaps in capabilities associated with a transition. For example, the Air Force plans to remove the A-10 ground attack aircraft from its inventory by 2022 in order to support modernization through fielding the F-35 program. However, removal of the A-10 from service creates a potential capability gap because the Air Force would no longer have a dedicated aircraft for close air support. Determining if the monetary savings gained through divestiture of the A-10 is worth the loss in ground support capacity remains a subject of DoD analysis.

In 2016, the GAO found the Air Force did not have quality information on the full implications of removing the A-10 from service. The GAO recommended that the Air Force fully identify modernization gaps, risks, and mitigation strategies, in addition to refining cost estimates of the savings before the Air Force removes the A-10 from its inventory. The GAO also recommended that DoD establish requirements to guide the removal of future weapon systems as the challenge to balancing modernization with the retention of existing equipment will increase as current weapon systems age.



A U.S. Air Force crew chief with the 159th Aircraft Maintenance Squadron cleans the canopy on an F-15C Eagle aircraft. (U.S. Air Force photo)

In the 2017 Defense Posture Statement, Former Secretary of Defense Ash Carter detailed the plan for Navy modernization. The statement attempted to balance investments in readiness and modernization to generate the force presently needed, as well as the anticipated force required for future naval superiority. It took into account the maritime threats posed by China, North Korea, and Russia.

However, in 2017 the Navy reduced the number of Littoral Combat Ships originally forecasted in 2016, in order to acquire additional capabilities in submarines, surface ships, and aircraft. During a Congressional hearing in May 2017, the Commandant of the Marine Corps noted that the Marine Corps fleet of Landing Craft Air Cushion, a hovercraft that ferries Marines, vehicles and supplies from ship to shore, has been in service for 25 years while the Landing Craft Utility, a medium-sized vessel capable of transporting personnel, cargo, and vehicles entered service in 1959.

Army modernization efforts include a 30-mm cannon upgrade for the Stryker combat vehicle to counter similar systems used by Russia and China over the past 5 years. The Army also upgraded the 155-mm ammunition for the M777 Howitzer that doubled its effective range and is replacing the

The guided-missile submarine USS Ohio arrives at Naval Magazine Indian Island, Washington. (U.S. Navy photo)

aging M113 Armored Personnel Carrier and High Mobility Multipurpose Wheeled Vehicle. Improved aircraft turbine engines for the AH-64 Apache and UH-60 Black Hawk are in development to increase platform capability in high altitude locations such as Afghanistan.

As current systems age and the pace of operations remains high, all Services will be challenged with finding the right balance between funding replacement of aging and worn existing equipment and investing in next-generation systems to counter evolving threats. Secretary of the Navy Richard Spencer stated, "We have been at war for the past 16 years with the operational tempo of the various conflicts in which we are engaged denying us the needed time and resources for modernization and maintenance."

FORCE STRUCTURE

Force structure consists of DoD organizations, both military and civilian, that comprise and support the Armed Forces. The DoD's force structure challenge is to design a force that can optimally meet a broad range of global requirements across the range of military operations, over time, within the end strength authorized by and funding appropriated by Congress. The force structure challenge is multi-faceted: achieving the right mix of capabilities across all Services; balancing the mix of Active, National Guard, and Reserve forces; and designing organizations within each Service that can be sufficiently manned, trained, and equipped to provide the capabilities that the Services need to fulfill their global requirements, when and where needed.

Many factors influence force structure decisions, including strategy, technology, funding, politics, and current and future operational requirements.

- **Strategy.** At the highest levels, the National Security Strategy, Defense Strategic Guidance, National Military Strategy, and Quadrennial Defense Review all shape decisions on what the military builds for the nation. The first three of these documents date from 2015, and the most recent QDR report was published in 2012.

U.S. Army soldiers of 1st Battalion, 4th Infantry Regiment role-play as enemy combatants while conducting an offensive operation training exercise. (U.S. Army photo)

- **Technology.** This factor is advancing at an accelerated rate. New technologies are combined with doctrine, people, and organizational design to produce new capabilities in the DoD's force structure.
- **Funding.** This factor influences force structure as the Services modernize over time to evolve their force structure at an affordable rate.
- **Politics.** From the international to the local level, this factor influences decisions on where to assign units and whether to increase or decrease force structure, affecting jobs in those communities and relations with allies.
- **Current Operational Requirements.** High demand for certain capabilities over the last 16 years of conflict drove changes in organizational design and growth in the number of high demand formations. For example, the Army's transformation from a Division-centric structure to a Brigade-centric structure, and its growth in Brigade Combat Teams at the height of Operation Iraqi Freedom.
- **Future Operational Requirements.** This is the greatest challenge in developing the future force for an unknown and unknowable future. The DoD's force structure changes continuously over time, through the disciplined application of a variety of processes, as DoD leaders seek to manage the known risks of today with the anticipated risks of tomorrow.

In summary, readiness and modernization come together in force structure. Meeting the immediate demands of global operations while developing a lethal future force is a fundamental challenge for the DoD. A sustained high-operational tempo, a broad range of evolving threats, rapid technological change, and uncertain funding complicate this challenge. These conditions have become the norm in today's environment. Optimally balancing readiness, modernization, and force structure to meet current and future military requirements will remain a difficult challenge for the DoD.

Members of the U.S. Army Band, "Pershing's Own," participate in a full honors wreath laying ceremony at the Tomb of the Unknown Soldier in Arlington National Cemetery, Virginia. (U.S. Army photo)

Challenge 8: Ensuring Ethical Conduct

Ensuring ethical conduct throughout the DoD is a critical and continual responsibility for DoD leaders. Ethical failures by DoD officials, public corruption investigations, and misconduct by a few DoD employees can undermine public confidence in the DoD, as well as foster an unwarranted perception about the overall character, ethics, dedication, and sacrifice of all DoD employees. At its core, ethical misconduct violates DoD core values and tarnishes the high standards of integrity expected of DoD personnel. Therefore, DoD leaders must continually strive to deter and prevent ethical lapses and misconduct, and hold accountable those individuals who violate the law, the standards of conduct, or other ethical requirements.

EFFORTS TO ENSURE ETHICAL CONDUCT

The responsibility for ensuring ethical conduct starts at the top of any organization. In this regard, on August 4, 2017, the Secretary of Defense emphasized the importance of ethical conduct by issuing a brief and direct memorandum to all DoD employees. This memorandum, "Ethical Standards for All Hands," states "those entrusted by our nation with carrying out violence, those entrusted with the lives of our troops, and those entrusted with enormous sums of taxpayer money must set an honorable example in all we do." The Secretary emphasized that employees should focus on the essence of ethical conduct: "doing what is right at all times, regardless of the circumstances or whether anyone is watching."

In addition, in March 2017 the Secretary of Defense, responding to reports of military misuse of social media sites, issued a statement that such conduct represented "egregious violations of the fundamental values" of the DoD and that "lack of respect for the dignity and humanity of fellow members" of the DoD is unacceptable and will not be tolerated.

In a memorandum dated February 12, 2016, "Leader-Led, Values-Based Ethics Engagement," the former Secretary of Defense informed the DoD's leaders of the importance of integrity and public confidence in DoD activities and its people. The Secretary directed leaders at every level to engage personally with their subordinates and to discuss values-based decision making to foster a culture of ethics and promote accountability, respect, and transparency throughout the DoD.

There are other examples of DoD leadership setting the tone at the top. In April 2016 the Chief of Naval Operations released a message he had provided to Naval Flag officers and Senior Executive Service (SES) members emphasizing the Navy's core values of honor, courage, and commitment and

A warrant officer with the 383rd Military Police Detachment (Criminal Investigation Command), of Lakeland, Florida, poses with a blue forensic light on a staged crime scene wall. (U.S. Army photo)

its core attributes of integrity, accountability, initiative, and toughness. This message was issued in part because of the Glenn Defense Marine Asia (GDMA) corruption scandal (also known as the "Fat Leonard" case, which is discussed in more detail below). The Chief of Naval Operations emphasized to the Navy senior leaders that their personal conduct and the example it sets are essential to their credibility, as well as to the overall integrity and efficiency of the Navy.

INSPECTORS GENERAL PROACTIVE INITIATIVES

The DoD Office of Inspector General (DoD OIG), Military Service and DoD agency Inspectors General (IGs), and the Military Criminal Investigative Organizations also play an important role in addressing this challenge, by investigating allegations of ethical violations and other misconduct and also by providing proactive education and training.

For example, the Military Services IGs have implemented various proactive initiatives intended to focus DoD personnel on ethical conduct, core values, and professionalism. The IGs engage in a broad range of proactive efforts to inform their leadership and the workforce about trends in both allegations of misconduct and substantiated investigations. Sharing these trends is intended to provide lessons learned and to help senior leaders and the workforce avoid misconduct. These efforts also include issuing publications for Service-wide distribution and speaking to general and flag officers, SES members, new commanders and officers at military schools, conference attendees, and personnel during site visits.

In particular, the Army IG uses publications, briefings, and visits to educate Army personnel on relevant trends in allegations and investigative findings the IG sees across the Army. The Army IG also publishes an annual report examining the prevalence of misconduct investigated across the Army. The report is distributed to Army IGs, attendees of officer and noncommissioned officer professional military education courses, and courses for officers selected for command.

The Naval IG briefs attendees of the Navy Leadership and Ethics Course, Naval flag and noncommissioned officer professional military education courses, and courses for new flag officers and SES members. The briefings focus on ethical, legal and moral behavior using real-life scenarios of both successes and failures in ethical decision-making by Navy leaders.

The Air Force IG briefs Air Force leaders at institutional training programs, including those for commanders at all echelons of command, new flag officers and SES members at the Senior Leader Orientation Course, Air National Guard commander courses, and Air National Guard senior leader conferences. The briefings focus on potential pitfalls and misconduct trends that have been identified by the Air Force IG.

The Marine Corps IG has initiated a series of professional military education briefings to general officers, senior noncommissioned officers, and legal advisors to inform them of the factors, indicators, and conduct that could lead to an allegation of senior official misconduct.

The DoD OIG has also implemented proactive initiatives designed to increase awareness of ethical pitfalls and prevent ethical misconduct by DoD employees. For example, the DoD IG regularly briefs newly appointed SES members at the DoD's APEX training about the role of the DoD OIG, trends in senior official misconduct, conduct to avoid, and

how to respond to OIG investigations. Recently, the Acting DoD IG has begun briefing new general and flag officers at the CAPSTONE class on these topics.

ETHICAL CONDUCT TRENDS

IGs are responsible for the investigating allegations of misconduct, whistleblower reprisal, and public corruption. These investigations are critical holding individuals accountable when they commit misconduct, and also in clearing them when the allegations are not supported.

TRENDS IN SENIOR OFFICIAL MISCONDUCT INVESTIGATIONS

Despite the proactive initiatives by DoD leaders and Service IGs, the DoD continues be confronted with high-profile misconduct cases. For example, an investigation by the DoD OIG found that an Army major general misused his Government Travel Charge Card for personal expenses at off-limits and adult entertainment establishments in South Korea and Italy; made false official statements to subordinates and to Citibank regarding charges he made to his travel card for personal expenses; and engaged in inappropriate behavior that included patronizing an establishment off limits to U.S. military personnel, drinking to excess in public, and interacting improperly with women. Another investigation found that an Air Force lieutenant general engaged in an unprofessional relationship with a married colonel.

A U.S. Navy engineman works on a lube oil purifier in the main machinery room aboard the amphibious transport dock USS Green Bay. (U.S. Navy photo)

The number of allegations received by the DoD OIG against senior DoD officials has increased over the past several years. There was a 13 percent increase in complaints alleging misconduct by senior officials from FY 2015 to FY 2017 (710 to 803). The most common allegations involved personal misconduct including improper relationships, improper personnel actions, misuse of government resources, and travel violations. The substantiation rate increased from 26 to 37 percent for investigations conducted by DoD OIG and the IGs for the Military Services, Defense agencies, and combatant commands. In the category of personal misconduct, there has been a steady trend in substantiated allegations of improper relationships and sexual misconduct.

TRENDS IN WHISTLEBLOWER REPRISAL INVESTIGATIONS

From FY 2013 through FY 2016, there has been a 51-percent increase in the number of whistleblower reprisal and military restriction complaints filed under the whistleblower protection statutes administered by the DoD OIG. The DoD OIG processes whistleblower reprisal and restriction complaints filed by military personnel, nonappropriated fund instrumentality employees, DoD contractor and subcontractor employees, and DoD intelligence community civilian employees. In FY 2016, there was a 30 percent increase in the number of these complaints. The number of reprisal investigations completed by Service IGs and other DoD Components, which require DoD OIG oversight, has increased by 50 percent since FY 2013. The overall substantiation rate for military reprisal investigations has remained at 12 percent over the years, while the substantiation rate for military restriction investigations has been higher, at 50 percent.

The Patriots Jet Team performs aerial acrobatics during the 2017 Twilight Show at Marine Corps Air Station Yuma, Arizona. (U.S. Marine Corps photo)

TRENDS IN SEXUAL ASSAULT PREVENTION AND RESPONSE INVESTIGATIONS

Preventing sexual assaults, ensuring victims who report sexual assault do not suffer retaliation, and fully investigating sexual assault allegations in a timely manner remains a continuing challenge for the DoD. According to the DoD Sexual Assault Prevention and Response Office, sexual assault prevention programs are designed to reinforce mutual respect, trust, professional values, and team commitment and to create an environment where discriminatory behaviors, sexual harassment, and sexual assault are not condoned, tolerated, or ignored.

The DoD Sexual Assault Prevention and Reporting Office is responsible for oversight of the DoD's sexual assault policy. This Office works with the Military Services and other DoD Components to develop and implement prevention and response programs. One such program is the DoD Safe Helpline—a crisis support service for members of the DoD community affected by sexual assault. The Safe Helpline provides live, one-on-one specialized support that is confidential, anonymous, and secure. The helpline is designed to provide crisis response, information, and to connect survivors to needed resources, while simultaneously building confidence in the reporting process.

Reports of sexual assault continue to rise. For example, the Military Services received 6,172 reports of sexual assault involving Service members as either victims or subjects of criminal investigations throughout FY 2016, which represents a 1.5-percent increase from the reports made in FY 2015. However, as reported to the Committees on Armed Services of the Senate and the House of Representatives in May 2017, the DoD FY 2016 Annual Report on Sexual Assault in the Military documented considerable progress to address sexual assault in the military. The 2016 Workplace and Gender Relations Survey indicated that estimated instances of sexual assaults for active duty Service members decreased in FY 2016, while the proportion of Service members choosing to report a sexual assault increased. Moreover, with sexual assault being a significantly underreported crime, the DoD considers the higher proportion of reporting as an indicator that victims are continuing to gain confidence in their leaders and response personnel to provide them with the care they need and hold alleged perpetrators appropriately accountable.

A KC-10 Extender from the 76th Air Refueling Squadron, 514th Air Mobility Wing, Joint Base McGuire-Dix-Lakehurst, New Jersey, refuels an F-22 Raptor. (U.S. Air Force photo)

The DoD OIG has also implemented overarching sexual assault investigative policy guidance to ensure uniform reporting and investigations of sexual assaults within the DoD. Most recently, DoD policies were updated to allow a victim of a sexual assault to anonymously report information from a restricted report to a Military Criminal Investigative Organization without affecting the restricted nature of the report.

With respect to oversight of investigations of sexual assault allegations, the DoD OIG has conducted several evaluations of adult sexual assault investigations closed by the Military Criminal Investigative Organizations. These evaluations indicate that investigations of sexual assault cases have been thorough. In a 2017 evaluation, the DoD OIG determined that only 2 of the 378 cases reviewed (0.5 percent) had significant deficiencies that likely adversely impacted the outcome of the investigations. This is a dramatic improvement since 2013, when a similar DoD OIG evaluation determined that 56 of 501 cases (11.2 percent) had significant deficiencies.

TRENDS IN PUBLIC CORRUPTION INVESTIGATIONS

Public corruption threatens national security; compromises the safety and security of DoD operations, systems, and personnel; wastes tax dollars; and undermines the mission of the DoD. Public corruption also involves a breach of the public's trust in the Government.

In FY 2017, public corruption investigations by the Defense Criminal Investigative Service (DCIS) resulted in 31 criminal charges and 30 convictions, including 15 DoD employees charged and 14 convicted. These investigations resulted in over $16 million in recoveries for the Government and the debarment of 29 entities from Government contracting.

A troubling example of public corruption in DoD programs involves a case relating to Glenn Defense Marine Asia PTE, LTD (GDMA), a defense-contracting firm based in Singapore that provides ship maintenance and supply services. Leonard Glenn Francis, a Malaysian national, was the former President and Chief Executive Officer of GDMA. A joint DCIS/Naval Criminal Investigative Service (NCIS) 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 that GDMA 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 GDMA employees with classified U.S. Navy ship schedules, contract data, preference and assistance in Navy contracting decisions, and a corrupt U.S. Federal agent provided access and insights into criminal investigations involving GDMA.

As of October 2017, 27 individuals have been criminally charged in connection with this scheme. Of those 27 individuals, 19 have pleaded guilty, including one Navy flag officer, a former member

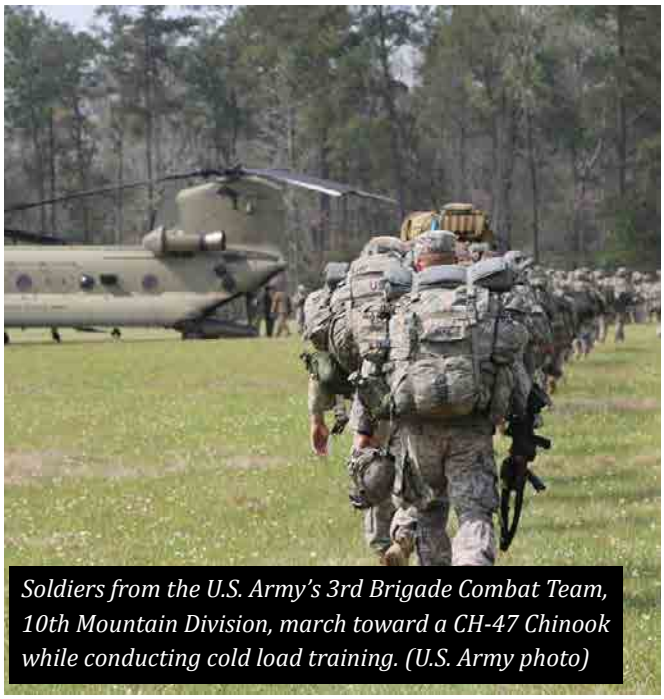
of the DoD Senior Executive Service, three Navy captains, several other Navy officers and enlisted personnel, a supervisory NCIS Special Agent, Francis, two former GDMA employees, and the GDMA corporate entity. Sentences have been imposed on 12 individuals range from 18 months to 12 years.

In addition, as a result of the active duty military personnel potentially involved in either criminal or unethical behavior involving GDMA, the Secretary of the Navy established a Consolidated Disposition Authority, headed by a four-star admiral, to review GDMA 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, to include court martial.

INITIATIVES TO IMPROVE TIMELINESS OF INVESTIGATIONS

Holding individuals accountable for misconduct, or exonerating them when they have not committed misconduct, should be done in a timely manner. The DoD OIG, Service IGs, and others investigating alleged misconduct must have a sense of urgency in accomplishing their work because of the impact investigations have on the lives of individuals and on their organizations' ability to perform effectively. However, many factors affect the timeliness of investigations, such as the complexity of the matters under investigation, the number and availability of witnesses, and the volume of complaints.

IGs have implemented several initiatives to improve the timeliness of investigations. For instance, over the last several years, the DoD OIG has standardized business processes and improved the timeliness of DoD Hotline referrals and administrative investigations. The DoD OIG also obtained funding to deploy and sustain the Defense Case Activity Tracking System Enterprise (DCATSe) through 2021. This case management system will transform the business processes and operations of



Soldiers from the U.S. Army's 3rd Brigade Combat Team, 10th Mountain Division, march toward a CH-47 Chinook while conducting cold load training. (U.S. Army photo)

the Military Services IGs and the Defense agencies by improving the efficiency and timeliness of the transmittal of investigative documents to offices located at posts, camps, and stations around the world and capturing the DoD-wide universe of complaints and investigations.

The deployment of DCATSe will also help meet the requirements of the National Defense Authorization Act for FY 2017, which requires the DoD OIG to establish uniform standards for conducting military restriction and whistleblower reprisal investigations. By standardizing the investigative processes, the DoD OIG hopes to also improve timeliness in various ways, including eliminating lengthy preliminary inquiries before opening investigations, developing consistent investigative and review timelines, and establishing uniform templates for investigative plans and reports of investigation.

At the request of the Deputy Secretary of Defense, the DoD OIG led a task force to review and improve the timeliness of senior official administrative investigations. The task force reviewed data, processes, policies, and resources and examined proposed changes to conduct more efficient and timely investigations. The task force's report, issued on November 6, 2014, included

recommendations to implement best practices for the intake and investigation processes, standardize processes, and deploy the DoD OIG's case tracking system across the DoD to increase efficiencies and timeliness throughout the entire investigative cycle. Many of the task force recommendations have been implemented. The Deputy Secretary of Defense endorsed the recommendation to deploy DCATS-e across the DoD, which is scheduled to be operational in FY 2019.

Nevertheless, timeliness of investigations, and disciplinary decisions once the investigation is completed, need further improvement. The DoD OIG will continue to focus on timeliness in investigations, as well as thoroughness and accuracy. However, a significant increase in whistleblower reprisal complaints and complaints resulting in an investigation has adversely impacted the timeliness of investigations. The volume of open cases has affected the ability of the DoD OIG and Service IGs, who conduct a majority of the whistleblower reprisal investigations, to reduce the time it take to complete investigation. This has presented a challenge for the DoD OIG and Service IGs and has prompted the IGs to seek innovative ways to promote further improvements in these areas.

In October 2016, the DoD OIG improved its process for oversight reviews of Service IG whistleblower reprisal investigations, reducing the average time from 70 to 10 days. The new approach has two stages. First, the review analyzes the report of investigation and scrutinizes the underlying documents if the report itself appears to be inconsistent, contains gaps, the conclusions are not supported by the facts presented, or appears deficient in another respect. The second stage is a programmatic assessment by the DoD OIG of the processes and overall quality of the whistleblower protection programs operated by each Service. The assessment is performed through a formal evaluation by the DoD OIG every 3 years, similar to a peer review, of the Service IGs and the Service Military Criminal Investigation Organizations. The DoD OIG has completed reviews of the Navy and Air Force IGs and will review the Army IG in FY 2018.

In addition, the DoD OIG has recently established an Alternative Dispute Resolution program to allow the parties the opportunity to settle certain types of whistleblower reprisal complaints through mediation or another Alternate Dispute Resolution process. Alternate Dispute Resolution programs can help reduce the time required to resolve complaints, typically more quickly than traditional investigative processes. The newly formed DoD OIG Alternative Dispute Resolution program will focus initially on complaints filed by employees of DoD contractors, subcontractors, grantees, and subgrantees, as well as personal services contractors; employees of nonappropriated fund instrumentalities; and employees of the DoD covered by Presidential Policy Directive 19. These types of allegations are the majority of the DoD OIG's reprisal complaints. Once fully implemented, the DoD OIG Alternative Dispute Resolution program will give contractors and employees the option of voluntarily seeking to resolve their concerns in a timely manner rather than undergo a lengthy investigation process.

In summary, timely and quality investigations require adequate resources, particularly given increasing investigative caseloads throughout the DoD. Adequate funding is necessary for DoD OIG operations, as well as for other DoD oversight entities such as the DoD agency and Service IGs, Service Auditors General, and Military Criminal Investigative Organizations to handle these increasing caseloads and provide timely and thorough investigations of misconduct. However, funding for some these DoD oversight entities has not always kept pace with the growth of the DoD, the increase in their responsibilities, or the dramatic increase in caseloads. This will continue to present a significant challenge for the DoD in its efforts to ensure ethical conduct.

A paratrooper from the U.S. Army's 173rd Brigade Combat Team re-enlists before boarding a C-130 Hercules to conduct airborne training operations. (U.S. Army photo)

Challenge 9: Providing Effective, Comprehensive, and Cost Effective Health Care

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. It includes direct and purchased care. Direct care is health care provided at military treatment facilities, primarily by military and contracted doctors. Purchased care is health 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).

In total, the Military Health System must provide health care, within fiscal constraints, for over 9 million beneficiaries, while facing increased user demand and inflation. As with any large health care system, the Military Health System must also respond and adapt to changing demographics, shifting policies, evolving standards for access and quality, advances in science and medicine, complex payment and cost considerations, rapidly evolving communications and information technology capabilities, and fluid patient expectations. As a result, providing health care at a reasonable cost without sacrificing quality remains a challenge for the DoD.

Over the last 10 years, the DoD OIG has performed audits and evaluations and made multiple recommendations related to DoD health care, many of which are still awaiting full implementation. As of March 31, 2017, the DoD had 114 open recommendations related to health care and morale issues, including recommendations to improve tracking of suicides throughout the DoD and reducing health care costs. The DoD OIG believes that fully implementing those open recommendations will help the DoD more effectively address this challenge.

QUALITY, SAFETY, AND ACCESS

In August 2014, the Military Health System Review Group published a report to the Secretary of Defense, which concluded that the Military Health System generally provided quality care that was safe, timely, and comparable in access, quality, and safety to that found in the civilian sector. However, as former Secretary of Defense Charles "Chuck" Hagel stated, "We cannot accept average when it comes to caring for our men and women in uniform and their families. We can do better; we all agree that we can do better." The Military Health System Review report indicated some areas where the Military Health System excelled and other areas where some facilities underperformed. The report

U.S. Air Force airmen transfer patients from an ambulance bus to a C-130 Hercules as part of a simulated aeromedical evacuation at Young Air Assault Strip, Fort McCoy, Wisconsin. (U.S. Air Force photo)

contained 78 recommendations to improve military health care. The report made recommendations in six major areas and recommended immediate action to improve underperformance and establish clear performance goals with standardized metrics. On October 1, 2014, the Secretary of Defense issued a memorandum, which directed the DoD to follow up on the August 2014 review results and to perform other specified tasks to improve transparency and transform the Military Health System into a High Reliability Organization.

In addition, the National Defense Authorization Act for FY 2016 added several requirements for the DoD that highlighted the importance of health care quality, safety, and access. For example, the Act included a provision requiring the Secretary of Defense to establish access standards for routine and specialty care and to ensure that TRICARE Prime beneficiaries seeking an appointment obtain appointments within those standards. The Act added requirements for the Secretary of Defense to publish on a DoD public website all measures he deemed appropriate to assess patient safety, quality of care, patient satisfaction, and health outcomes for health care provided under the TRICARE program. The Act also added requirements to detail the number of practitioners at military treatment facilities that were reported to the National Practitioner Data Bank, and to assess the accreditation status of military treatment facilities and other data related to health care quality, safety, and access.

According to Defense Health Agency personnel, the Military Health System has implemented all of the National Defense Authorization Act for FY 2016 requirements. In 2017, the DoD OIG initiated two evaluations, and plans to initiate another evaluation, to determine whether the DoD's response to the August 2014 Military Health System Review Final Report improved access to care, quality of care, and patient safety. The DoD OIG also initiated an audit to review access to care at selected military treatment facilities.

BEHAVIORAL HEALTH

Behavioral health treatment for the military continues to be a significant issue for the DoD. In recent years, the DoD has focused significant attention and resources on detecting, diagnosing, and treating mental disorders—especially those related to long and repeated deployments and combat stress. 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 addition, mental disorders accounted for the second most common reason for outpatient clinic visits by active duty service members in 2016.

In particular, proactively diagnosing and treating those with behavioral health conditions and those at risk for suicide remains a challenge for the DoD. A RAND report published in August 2017 highlighted the continuing challenges facing the DoD in providing both access and follow up to quality behavioral health care, which are key to the DoD's suicide prevention efforts. The RAND report concluded that the Military Health System continues to be a leader in achieving high rates of follow up after psychiatric hospitalization, and that the Military Health System excels at screening for suicide risk and substance use, but that follow up for service members who have already been identified as having elevated suicide risk needs improvement. The report also concluded that quality of care for post-traumatic stress disorder and depression varied by Service branch, TRICARE region, and service member characteristics, and suggested that opportunities for quality improvement may be achievable by systemic enhancements of processes across the DoD. A DoD spokesperson stated that the DoD is reviewing the report findings and recommendations and that they will be used to shape and improve the future direction of patient care.

SEPARATION FROM SERVICE OF PERSONNEL WITH MENTAL HEALTH CONDITIONS

The GAO reported in May 2017 that from 2011 through 2015, 62 percent of service members separated for misconduct were diagnosed with post-traumatic stress disorder, traumatic brain injury, or other mental health conditions within 2 years of separation. Other mental health conditions for these separated service members included adjustment disorders, alcohol-related disorders, anxiety disorders, bipolar disorders, depressive disorders, personality disorders, and substance-related disorders. Of those with mental health conditions, 23 percent received other than honorable characterizations of service, making them potentially ineligible for health benefits from the Department of Veterans Affairs. The GAO concluded that, because of policy inconsistencies and limited monitoring, the DoD had minimal assurance that certain service members diagnosed with post-traumatic stress disorder or traumatic brain injuries received the required screening and counseling before they were separated from the Service for misconduct. Additionally, the risk increased that service members may be inappropriately separated for misconduct without adequate consideration of these conditions' effects on behavior, separation characterization, or eligibility for Department of Veterans Affairs benefits and services.

The GAO recommended that the Secretary of Defense direct the Air Force and Navy to address inconsistencies in their policies with DoD policy related to screening service members and reviewing results prior to separation for misconduct, and training service members to identify mild traumatic brain injuries in a deployed setting. The GAO also recommended that the Secretary of Defense ensure that the military Services routinely monitor adherence to those policies and policies related to counseling on Department of Veterans Affairs benefits and services. The DoD agreed with the recommendations.

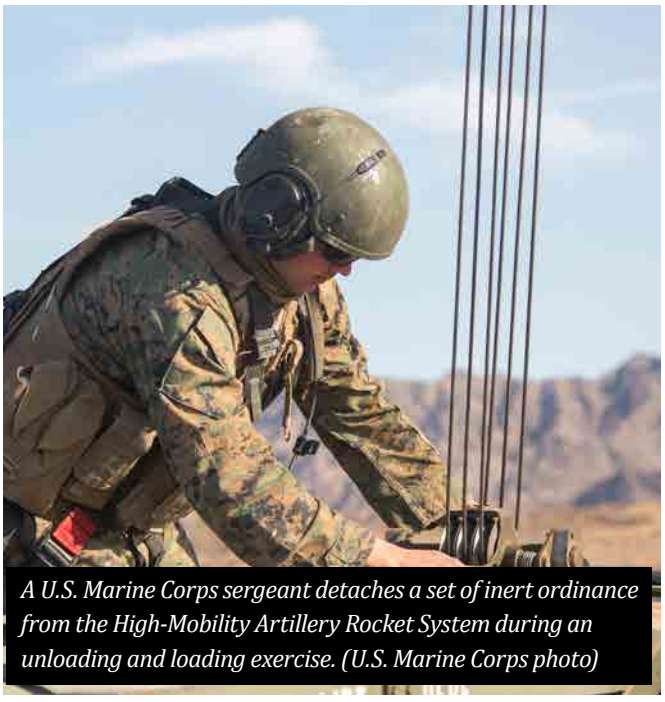
SUICIDE PREVENTION

As noted above, suicide prevention continues to be a challenge for the DoD. As of the fourth quarter of 2016, the total number of suicide deaths for DoD was 276 for the Active Component and 203 for the Reserve Component.

In response to the number of suicides, the DoD developed and promoted prevention policies, practices, and programs to attempt to reduce military suicide. For example, the Defense Suicide

Prevention Office was established in 2011 to provide advocacy, program oversight, and policy for DoD suicide prevention, intervention, and follow-up efforts to reduce suicidal behaviors in service members, civilians, and their families. It also leads working groups of representatives from the Services, the Office of the Assistant Secretary of Defense (Health Affairs), and other interested organizations, related to expanding access to behavioral health care for service members. In 2015, the Defense Suicide Prevention Office also implemented the DoD Strategy for Suicide Prevention, which is designed to guide and coordinate suicide prevention efforts across the DoD. As one part of that effort, the Defense Suicide Prevention Office published and distributed guides to military family members on suicide warning signs, risk factors, and actions to take in a crisis. The office also sponsors research initiatives and training that address gaps in suicide prevention and resilience policies and practices.

The DoD collaborated with the Department of Veterans Affairs to develop suicide prevention and intervention policy. For example, in June 2013, the DoD and Department of Veterans Affairs jointly developed the Clinical Practice Guideline, "Assessment and Management of Patients at Risk for Suicide," which recommended best practices for assessing and managing the risk of suicide among active duty military and veterans.



A U.S. Marine Corps sergeant detaches a set of inert ordinance from the High-Mobility Artillery Rocket System during an unloading and loading exercise. (U.S. Marine Corps photo)

The DoD OIG has performed several evaluations to assess DoD suicide prevention efforts. For example, in September 2015, a DoD OIG evaluation found that the DoD lacked a clearly defined governance structure and alignment of responsibilities for the Defense Suicide Prevention Program. In addition, the DoD OIG identified the lack of clear processes for planning, directing, guiding, and resourcing to effectively develop and integrate the Suicide Prevention Program within the DoD. In response to the DoD OIG's recommendations, the Defense Suicide Prevention Office issued and implemented the 2015 Strategy for Suicide Prevention, noted above, to coordinate suicide prevention efforts across the DoD. In response to another DoD OIG evaluation report in November 2014, the Defense Suicide Prevention Office developed and is in the process of issuing guidance for data collection and reporting on suicide events.

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. The DoD OIG reported this as a key open recommendation in its July 2017 Compendium of Open Recommendations. 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 to reduce suicide rates across the force.

In summary, the DoD needs to continue to pursue programs to diagnose behavioral health issues and risk factors for military personnel and its other health care beneficiaries.

INCREASING HEALTH CARE COSTS

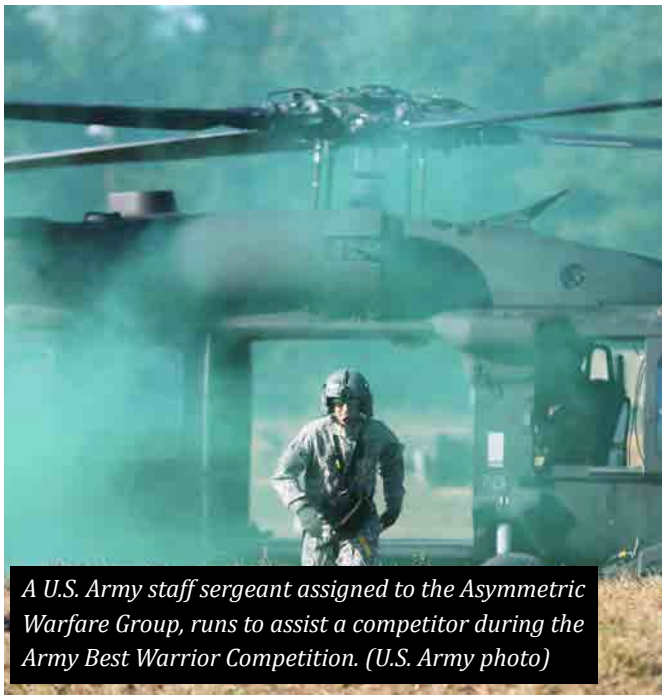
The DoD faces a continuing challenge to contain costs and prevent health care fraud. Over the last decade, health care costs in the United States have grown dramatically, and Military Health System costs have been no exception. For example, the DoD FY 2016 appropriations for health care were $32.3 billion, almost triple the FY 2001 appropriation of $12.1 billion. In its FY 2018 budget, the DoD requested $33.7 billion for the Defense Health Program.

One of the leading contributors to health care cost is fraud. Health care fraud is one of the top investigative priorities for the Defense Criminal Investigative Service (DCIS). As of July 7, 2017, DCIS had 523 open health care investigations. In FY 2016 and FY 2017 combined, DCIS health care fraud investigations resulted in 100 criminal charges and 68 convictions, the seizure of $53 million in assets, and $117 million in recoveries for TRICARE and the Defense Health Agency.

However, health care fraud schemes are constantly evolving. As one vulnerability is closed, corrupt individuals look for another vulnerability within the health care payment system to exploit. Therefore, the DoD needs to be constantly vigilant to detect health care fraud, and to establish strong internal controls to determine areas at risk for health care fraud.

PHARMACEUTICALS

The DCIS continues to vigorously investigate fraud arising from the compound pharmaceutical fraud epidemic that exploited TRICARE in 2014 and 2015. Compound drugs are developed from combining, mixing, or altering two or more ingredients to create a customized medication for an individual patient. In 2015, the Defense Health Agency experienced a dramatic increase in compounding pharmacy fraud, with $1.6 billion spent on compound medications in that 1 year alone. Much of the expenditures were fraudulent.



A U.S. Army staff sergeant assigned to the Asymmetric Warfare Group, runs to assist a competitor during the Army Best Warrior Competition. (U.S. Army photo)

For example, 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. The Defense Health Agency changed its reimbursement policy for compound drugs in response to the significant losses it realized.

As a specific example of this type of fraud, one compounding pharmacy in Florida sought reimbursement for compounding pharmaceutical prescriptions that were not medically necessary and were prescribed by physicians that had never actually examined or even seen the patients. Further, a military member involved in the scheme committed identity theft by stealing fellow military members' personally identifiable information in order to facilitate additional billings to TRICARE in exchange for kickbacks. In this case, 14 individuals have been convicted of various crimes, $31 million

has been court-ordered back to the Defense Health Agency as restitution, and approximately $10 million in assets have been seized.

In May 2015, the Defense Health Agency implemented new controls, which reduced payments for compound drugs from $497 million in April 2015 to $10 million in June 2015. In an audit report issued in July 2016, the DoD OIG found that, while the controls were effective in reducing costs for compound drugs, additional controls were necessary to prevent reimbursement for certain non-covered compound drug ingredients. The Defense Health Agency agreed with the recommendation and took actions to improve controls related to compound drugs.

Fraud and escalating costs also occur in non-compound pharmaceuticals. The DoD OIG has two ongoing audits related to pharmaceuticals, including an audit reviewing the Defense Health Agency's process for implementing controls in response to escalating costs for non-compound pharmaceuticals, and an audit to determine whether the Defense Logistics Agency Troop Support managed its Pharmaceutical Prime Vendor Program to effectively control health care costs.

AUTISM TREATMENT

One emerging fraud trend involves Applied Behavioral Analysis, 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 2017 audit, the DoD OIG determined that the Defense Health Agency made improper payments for autism services to five companies in the TRICARE South Region. Specifically, the Defense Health Agency improperly paid for services where the beneficiary was not present; the beneficiary was napping; providers were not authorized by TRICARE; documentation to support services was lacking; and the provider billed for higher qualified health care professionals than those who actually performed the services. As a result, the audit determined that the Defense Health Agency improperly paid $1.9 million of the total $3.1 million paid to the five companies in 2015.

The DCIS also investigated an Applied Behavioral Analysis therapy clinic that allegedly provided therapy using personnel who were not properly trained per Defense Health Agency guidelines, billed group therapy as one-on-one therapy, and billed for services never rendered. The investigation resulted in the indictment and conviction of the clinic owner and the reassignment of TRICARE beneficiaries from this clinic to others in the area.

PAYMENT COLLECTIONS

Another aspect of controlling health care costs involves ensuring collections are made for services provided at military treatment facilities. 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. The military treatment facilities also did not appropriately transfer funds to the U.S. Treasury for 114 delinquent accounts, valued at $13.4 million, of the 145 accounts the DoD OIG reviewed for collection. In 2017, the DoD OIG plans to perform another audit to review billing and reimbursement for health care provided to Department of Veterans Affairs patients at selected Army military treatment facilities.

While the Defense Health Agency has made progress in controlling some costs, people committing fraud will continue to look for new vulnerabilities to exploit. As internal controls are tightened in one area, those intent on committing fraud seek other vulnerabilities to exploit. For example, emerging areas of concern for fraud within the DoD health care system involve genetic and DNA testing, durable medical equipment, and opioids. The Defense Health Agency needs

to be vigilant in reviewing billing trends to look for the next fraud schemes and implement effective controls to help prevent payments for fraudulent claims.

ELECTRONIC HEALTH RECORDS

In addition, the DoD faces challenges with the security of electronic health records and integration of those records with the Department of Veteran Affairs. According to a media report, more than 115 million patient records in the United States were compromised in 2015, and more than 25 million records were "compromised" from January to October 2016. The DoD has a responsibility to protect the patient health information for its 9 million beneficiaries and transfer records as needed to the Department of Veterans Affairs.

The DoD OIG also found security weaknesses within the DoD's electronic health records. A July 2017 DoD OIG audit reported that 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. The DoD OIG began a similar audit in April 2017 of the Navy and Air Force electronic health records.

In addition to the security of health records, according to congressional testimony by a GAO official in 2016, the DoD and the Department of Veterans Affairs have failed in several attempts to integrate their respective electronic health records since 1998. The testimony noted that the Department of Veterans Affairs has undertaken a patchwork of initiatives with the DoD to allow their health information systems to exchange information and increase interoperability. These have included initiatives to share viewable data in their existing (legacy) systems, link and share computable data between their updated health data repositories, and jointly develop a single integrated system that would be used by both departments.

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 will acquire the same system as DoD. The DoD should monitor this acquisition and work closely with the Department of Veterans Affairs to ensure that the system will be interoperable with the DoD system. The DoD should work closely with the Department of Veterans Affairs to ensure interoperability between the Departments' electronic health records and ensure that sensitive patient health information contained in electronic health records are adequately protected.

In summary, providing quality, cost-effective health care to the DoD's 9 million beneficiaries will continue to be a significant challenge for the DoD. The DoD must continue to seek efficiencies to control costs without undermining timely access to quality health care. That 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. In addition, the DoD must protect patient health information within its electronic health records and work closely with the Department of Veterans Affairs to integrate electronic health records between the Departments. The DoD OIG will continue to perform reviews of high-risk health care issues and monitor progress in these areas to identify additional ways to improve health care for DoD beneficiaries.

Low Altitude Air Defense gunners with 3rd LAAD Battalion, Marine Air Control Group 38, 3rd Marine Aircraft Wing, lock onto incoming enemy aircraft during assault support tactics one. (U.S. Marine Corps photo)

Challenge 10: Identifying and Implementing Efficiencies in the DoD

In February 2017, Secretary of Defense Mattis stated that the DoD needed to field a larger, more capable, and more lethal joint force, and he also highlighted the need for the DoD to implement necessary efficiencies at the same time. In a memorandum dated February 21, 2017, the Secretary directed the establishment of cross-functional teams to seek improved mission effectiveness and efficiencies. He also encouraged cross-enterprise consolidation of business activities associated with human resource management, financial management, real property management, acquisition and contract management, logistics and supply chain management, health care management, base services, and cyber and information technology management.

In a related effort, in April 2017 the Office of Management and Budget issued a memorandum to the heads of executive departments and agencies entitled, "Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce," which addressed streamlining the Government and eliminating duplicative functions. Specifically, the Office of Management and Budget directed departments and agencies to develop comprehensive plans for reforming the Government, reducing their civilian workforces, and maximizing employee performance.

Although the DoD has some progress in identifying opportunities for efficiencies, the most challenging part of this initiative involves actually implementing identified efficiencies. The DoD, DoD OIG, GAO, and other oversight organizations regularly identify opportunities for efficiencies, but fully implementing these efficiencies has been difficult.

DOD'S REFORM PLAN TO IDENTIFY AND IMPLEMENT EFFICIENCIES

In response to the Office of Management and Budget memorandum, the DoD is developing a DoD Reform Plan in two phases. During Phase I, DoD Components must identify reform initiatives for potential inclusion in the DoD Reform Plan. In Phase II, DoD Components must provide additional information on their plans to implement the initiatives the DoD selects and the specific performance goals and measures included in the DoD Agency Strategic Plan. The DoD will also include a comprehensive DoD Workforce Rationalization Plan to fulfill the requirement for developing a long-term workforce reduction plan.

As part of Phase I, the Deputy Secretary of Defense submitted the draft Defense Reform Plan to the OMB on June 30, 2017. The DoD's Office of the Deputy Chief Management Officer developed the draft Defense Reform

A U.S. marine assigned to Kilo Company, 3rd Battalion, 1st Marines, uses a radio to support an assault during a support training exercise. (U.S. Marine Corps photo)

Plan with DoD Component input. The draft plan details proposed initiatives to improve travel, lodging, computer systems, medical, mobile communications, security, commissaries, and exchanges.

As examples of these initiatives, the DoD proposed consolidating the purchase of medical supplies and food across the DoD to take advantage of economies of scale; proposed converting the Armed Forces Retirement Home to a non-profit, private institution; and proposed consolidating all commissary and exchange systems, which would allow economies of scale in purchasing and standardization of operating policies.

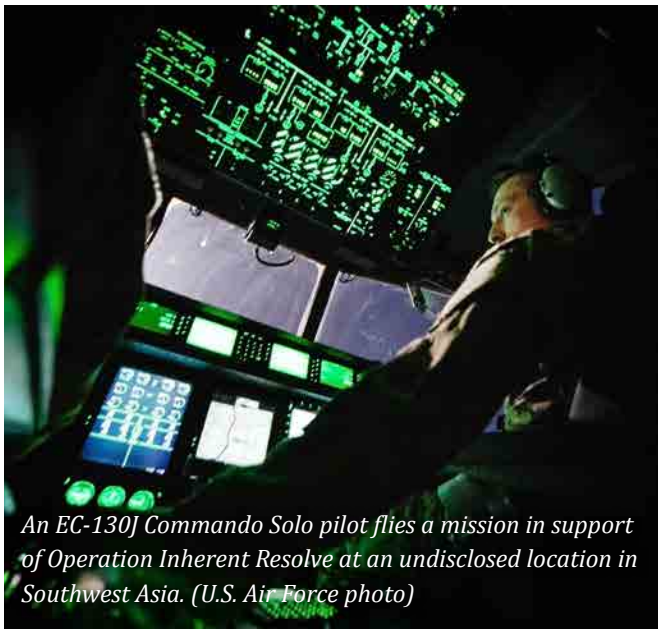
The DoD's Office of the Deputy Chief Management Officer is in the process of quantifying the savings from the proposed initiatives highlighted in the draft Defense Reform Plan and plans to incorporate the expected results into the final Defense Reform plan.

DOD OIG INPUT TO REFORM PLAN

Although not specifically identified in the DoD's draft plan, the DoD OIG provided input to the DoD reform plan, which outlined five other specific opportunities for efficiencies and enhanced mission effectiveness:

- **Logistics Systems and Spare Parts:** The DoD could achieve efficiencies by transitioning to one joint system for the procurement and tracking of spare parts. A joint system could improve the DoD's purchasing power and improve visibility of available inventory so the Services could more easily obtain spare parts, especially for shared weapon systems and platforms. In addition, with one joint system, the Services could avoid buying spare parts that another Service already has in stock or could avoid buying spare parts at unreasonable prices. The lack of a centralized logistics system also complicates identifying and removing defective parts from inventory, tracing the defective parts back to the suppliers, and recouping payment or receiving replacement parts.

- **Financial Systems:** The DoD could achieve significant efficiencies by reducing the number of financial systems related to core finance and accounting functions. Over time, DoD Components have developed separate solutions to meet their individual financial management requirements. At least some of these systems do not interface well with other systems at the Defense Finance and Accounting Service. The DoD has made progress in integrating systems; however, many inefficient processes and excess overhead exist across the DoD's financial community. For more details, see Management Challenge 5, Improving Financial Management.
- **Suspension and Debarment Offices:** The DoD could achieve efficiencies by eliminating duplication, standardizing processes, and streamlining the coordination and tracking of suspension and debarment actions. For example, the DoD currently has five primary suspension and debarment officials assigned to the Army, Navy, Air Force, Defense Logistics Agency, and Defense Information Systems Agency. Although these suspension and debarment officers operate under the same standards as each other, the different suspension and department offices are at risk of disparate decisions with regard to similar suspensions and debarments.
- **Professional Military Education and Training Schools:** The DoD could achieve efficiencies through phased consolidation of schools among the Services. The DoD maintains Service-specific schools for common professional skills and leadership training. For example, the military Services each maintain schools related to military justice, aviation, junior and mid-level officer and non-commissioned officer leadership schools, among others. Each of these schools requires manpower (instructor and overhead positions) and funding for curriculum development, travel, and installation management. The DoD should consider consolidation of these schools.
- **Military Health Care:** The DoD could achieve efficiencies by strengthening internal controls and policy related to medical billing and payments. For more details, see Management Challenge 9, Providing Effective, Comprehensive, and Cost Effective Health Care. The DoD OIG has issued several audit reports in FY 2016 related to improper payments and billing for military health care. For example, a report identified that military treatment facilities did not actively pursue collections from non-DoD beneficiaries, valued at over $11.3 million, and failed to appropriately transfer delinquent accounts to the U.S. Treasury, valued at $13.4 million. Additionally, in FY 2016, Defense Criminal Investigative Service investigations resulted in 32 criminal charges, 16 convictions, and over $380 million in recoveries related to military health care. These audits and investigations demonstrate the need for improved internal controls to help the DoD reduce the number of improper payments and allow for increased collections for health care services.



An EC-130J Commando Solo pilot flies a mission in support of Operation Inherent Resolve at an undisclosed location in Southwest Asia. (U.S. Air Force photo)

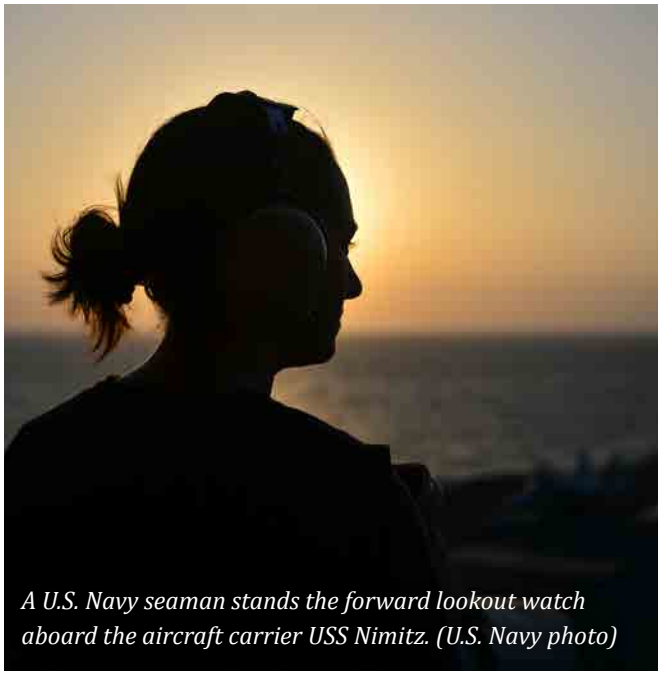
OIG OPEN RECOMMENDATIONS FOR EFFICIENCIES IN THE DOD

On July 11, 2017, the DoD OIG published a Compendium of Open Recommendations that identified all open recommendations from prior reports. These open recommendations identify potential efficiencies across the DoD that, if addressed, could help the DoD meet Secretary of Defense and Office of Management and Budget goals. The DoD should carefully consider these open recommendations as it develops its reform plan.

Specifically, DoD OIG reports provided 1,300 recommendations for efficiencies in the areas of acquisition, contract management, and financial management among others. Although the DoD has taken corrective action on many of these recommendations, it should look more broadly at DoD OIG recommendations and consider how it can implement corrective actions across the DoD.

By not implementing DoD OIG recommendations in a timely manner, the DoD is missing opportunities to improve the efficiency and effectiveness of DoD programs and operations. Each year, the DoD OIG issues an average of 150 audit and evaluation reports. These reports contain findings that identify deficiencies within DoD programs and operations, as well as recommendations for improvement. 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.

DoD management and the DoD OIG share responsibility to follow up on implementation of open recommendations. DoD managers are responsible for implementing recommendations promptly. At the same time, the DoD OIG must follow up to assess whether the DoD takes the agreed-upon corrective actions and whether those actions meet the intent of the recommendations. When DoD management does not agree to implement a recommendation and does not propose alternative corrective action to address the identified problems, the recommendation remains unresolved and open.



A U.S. Navy seaman stands the forward lookout watch aboard the aircraft carrier USS Nimitz. (U.S. Navy photo)

In the Compendium, the DoD OIG identified 1,251 recommendations that remained open despite DoD management's agreement to take corrective actions. The Compendium included listings of recommendations that best help improve the efficiency of DoD programs and operations and highlighted recommendations that the DoD OIG considered to be high priority. The Compendium also listed 47 unresolved recommendations made in reports dating back to June 2012. In addition, the Compendium listed 58 recommendations from 40 DoD OIG reports that identified billions in potential monetary benefits the DoD could achieve if the open recommendations were fully implemented.

In summary, while the DoD has taken various corrective actions on the specific recommendations contained in DoD OIG reports, the DoD should refocus attention on open recommendations and seek to implement agreed upon corrective actions across the DoD.

A U.S. Air Force weather forecaster with the 7th Operations Support Squadron reviews weather radars. (U.S. Air Force photo)

OTHER REPORTS THAT HIGHLIGHTED EFFICIENCIES

Similarly, the GAO has identified areas of needed efficiencies throughout the DoD. For example, the Director of the GAO testified to the U.S. Senate Committee on Homeland Security and Governmental Affairs on opportunities to achieve financial benefits in the Government, including opportunities to reduce overlap and duplication. This testimony provided examples in the following four DoD missions and functions:

- **Army and Air Force Virtual Training:** The Army and Air Force need to improve the management and oversight of their virtual training programs to avoid fragmentation and to more efficiently and effectively acquire and integrate virtual devices into operational training and potentially save tens of millions of dollars.
- **Construction for Military Contingency Operations:** By improving oversight of contingency construction projects, the DoD could potentially reduce duplication and save millions.
- **Defense Weather Satellites:** Establishing formal mechanisms for coordination and collaboration with the National Oceanic and Atmospheric Administration could reduce the risk of gaps in weather satellite capabilities.
- **Advertising:** The DoD should improve coordination and information sharing across its fragmented advertising programs for more efficient and more effective use of resources.

In addition to the recommendations from external reviews conducted by the DoD OIG and the GAO, DoD Components have also completed internal studies that have identified potential efficiencies for the DoD. For example, the Under Secretary of Defense, Acquisition, Technology, and Logistics 2016 Annual Report highlighted multiple areas of needed improvements across the DoD. The Annual Report stated that the DoD has significantly lowered cost growth within acquisition programs. According to the report, the DoD's efforts to improve cost performance have not adversely impacted contractor profits, but have provided a reasonable alignment of industry and government goals.

However, the 2016 report identified multiple areas where the DoD could improve, one of which related to gaining efficiencies. Specifically, the report noted that the percentage of competitive acquisitions fell each year except for one from FYs 2010 through 2015. Major drivers of this trend were high-value sole-source Foreign Military Sales, fewer new program starts, and higher percentages of the Major Defense Acquisition programs in production and thus sole or dual-sourced. According to the report, increased bid protests also forced the DoD to award sole-source contracts to bridge until the new contract awards could be let. By increasing competition, the DoD could drive costs down and realize efficiencies.

A U.S. Air Force crew chief with the 4th Aircraft Maintenance Squadron conducts a preflight check. (U.S. Air Force photo)

DoD acquisition managers could also make better use of the program assessments DOT&E provides in making production decisions. The DOT&E recommendations could save billions in unnecessary expenditures for upgrading fielded systems, provided DoD acquisition managers fully use the program assessments and recommendations. However, in a March 2017 report, the GAO estimated that the 78 DoD acquisition programs assessed by the GAO experienced $253.6 billion of cost growth after starting production. The GAO found that these significant post-production cost increases may indicate that programs start production without having demonstrated that a fully integrated, capable production-representative prototype will work as intended.

In FY 2018, the DoD OIG plans to conduct an audit to determine whether DoD acquisition managers are effectively using the DOT&E FY 2016 recommendations to better plan and execute operational testing for their programs.

In summary, although the DoD has made progress toward implementing efficiencies, many more opportunities for efficiencies exist throughout the DoD. The DoD OIG, GAO, and DoD Components regularly identify efficiency improvements. A large part of DoD's challenge is to actually implement efficiencies that have been identified and will continue to be identified. While it is important to identify opportunities for efficiencies, it is even more important to implement these recommendations. It will take continual, concerted attention and focus at all levels in the DoD to make substantial progress on implementing efficiencies.

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Protection-Ombudsman/

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

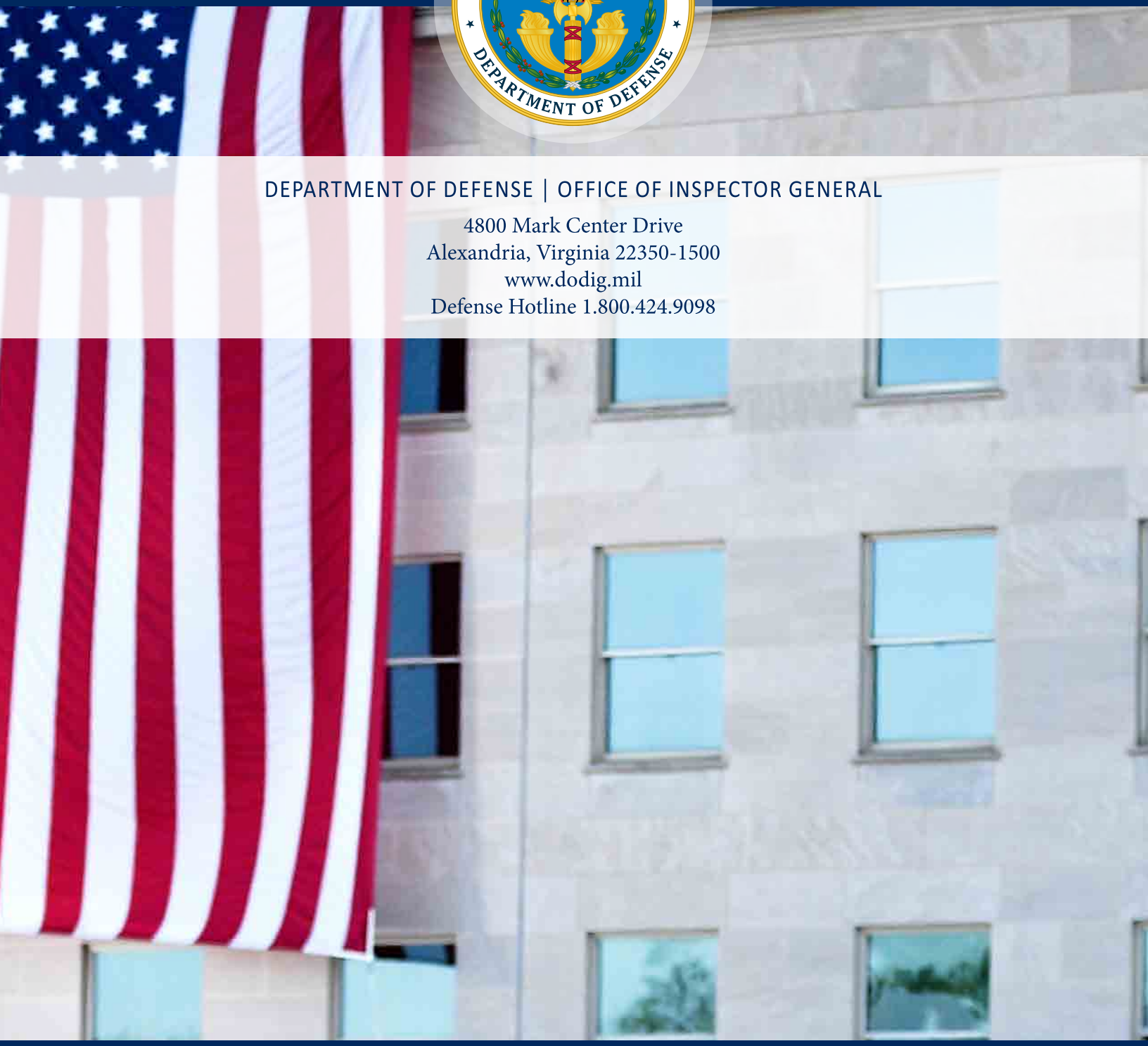
Congressional Liaison
703.604.8324

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