United States Government Accountability Office

Testimony

Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 3:00 p.m. ET
Friday, April 30, 2021

INFORMATION ENVIRONMENT

DOD Operations Need Enhanced Leadership and Integration of Capabilities

Statement of Joseph W. Kirschbaum, PhD,
Director, Defense Capabilities and Management

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-525T

GAO Highlights

Highlights of GAO-21-525T, a testimony before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives

April 30, 2021

Information EnvirOnment

DOD Operations Need Enhanced Leadership and Integration of Capabilities

Why GAO Did This Study

U.S. potential adversaries—including near-peer competitors Russia and China—are using information to achieve objectives below the threshold of armed conflict. DOD can use information operations to counter these activities.

This testimony summarizes GAO's past work related to DOD's IO capabilities. Specifically, it discusses: (1) DOD's information operation terms and concept, and (2) DOD's actions to implement the 2016 DOD IO strategy and address oversight and integration challenges. This statement is based on GAO's August and October 2019 reports (GAO-19-510C and GAO-20-51SU) and updates conducted in April 2021.

What GAO Recommends

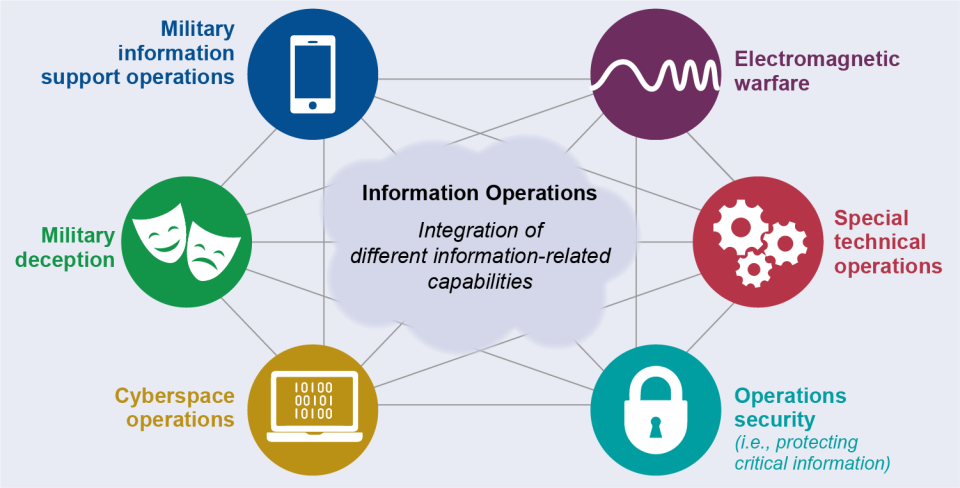
In prior work on which this testimony is based, GAO recommended that DOD take five actions to improve leadership and integration for information operations—including that the department should conduct a posture review to assess integration challenges. DOD disagreed with the recommendations. However, Section 1631 of the National Defense Authorization Act for Fiscal Year 2020 included several provisions related to our recommendations, such as one that required the Secretary of Defense to conduct a posture review.

View GAO-21-525T. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

At its core, information operations (IO) are the *integration* of information-related capabilities during military operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. (See figure.) For example, in seeking to facilitate safe and orderly humanitarian assistance, the Department of Defense (DOD) would conduct IO by influencing host nation and regional cooperation through the *integration* of public affairs activities and military information support operations.

Information Operations and Selected Information-Related Capabilities



Source: GAO analysis of Department of Defense (DOD) information. | GAO 21-525T

Text of Information Operations and Selected Information-Related Capabilities

Information Operations: integration of different information-related capabilities

- Military information support operations
- electromagnetic warfare
- special technical operations
- operations security (i.e. protecting critical information)
- Cyberspace operations
- Military deception

GAO found, in 2019, that DOD had made limited progress in implementing the 2016 DOD IO strategy and faced a number of challenges in overseeing the IO enterprise and integrating its IO capabilities. Specifically:

- In seeking to implement the strategy, DOD had not developed an implementation plan or an investment framework to identify planning priorities to address IO gaps.
- DOD has established department-wide IO roles and responsibilities and assigned most oversight responsibilities to the Under Secretary of Defense for Policy. The Under Secretary had exercised some responsibilities, such as establishing an executive steering group. However, the Under Secretary had not fulfilled other IO oversight responsibilities, such as conducting an assessment of needed tasks, workload, and resources. Instead, the Under Secretary delegated these responsibilities to an official whose primary responsibilities are focused on special operations and combatting terrorism.
- DOD had integrated information-related capabilities in some military operations, but had not conducted a posture review to assess IO challenges. Conducting a comprehensive posture review to fully assess challenges would assist DOD in effectively operating while using information-related capabilities.

Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee:

I am pleased to be here today to discuss the vital role of the Department of Defense's (DOD) operations in the information environment. In short, information environment refers to the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

As then Secretary of Defense Carter stated in the 2016 DOD *Strategy for Operations in the Information Environment,* although the term information environment is relatively new, the concept of an "information battlefield" is not. The role of information, either provided or denied, is an important consideration in military planning and operations. In fact, throughout the history of warfare, militaries have sought advantage through actions intended to affect the perception and behavior of adversaries. Information is such a powerful tool, it is recognized as an element of U.S. national power and, as such, the department must be prepared to synchronize information programs, plans, messages, and products as part of a whole-of-government effort.[1]

We are not the only global power to recognize the importance of the information environment. Competitors, including Russia and China, have made great strides in improving their capabilities and in how they use the information environment to advance their national objectives and to undermine the security and principles of the United States and its allies and partners. For example, Russia, through military intelligence units, also known as the "GRU," and Kremlin-linked troll organizations often referred to as the "Internet Research Agency," deploys information warfare operations against the United States and its allies and partners, with the goal of advancing the strategic interests of the Russian Federation.[2] Similarly, China has formed new military units to achieve dominance in the electromagnetic spectrum and centralized space, cyber, electromagnetic warfare capabilities, and potentially psychological

[1]DOD, *Strategy for Operations in the Information Environment* (June 2016).

[2]National Intelligence Council, *Foreign Threats to the 2020 U.S. Federal Elections,* ICA 2020-00078D (Mar. 10, 2021).

warfare, according to studies we reviewed for our December 2020 report focused on DOD electromagnetic spectrum operations.[3]

As recognized in DOD's 2018 *Joint Concept for Operating in the Information Environment,* information technology has significantly enhanced human interaction around the globe and elevated the importance of information as an instrument of power wielded by individuals and societies in politics, economics, and warfare. Advances in information technology have significantly changed the generation of, transmission of, reception of, and reaction to information. These advances have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms. However, our competitors and adversaries are taking advantage of the advances in information technology and subsequent effects in the information environment to offset the United States' preeminent warfighting force.

To make additional advances in this area, DOD has taken a number of actions—including issuing new or updated doctrine, establishing new leadership positions and organizations, and conducting operations. For example, in November 2012, DOD issued joint doctrine on Information Operations (IO).[4] Also, as noted earlier, DOD in 2016 issued its *Strategy for Operations in the Information Environment.* Additionally, in 2017, DOD updated its *Doctrine for the Armed Forces of the United States* to establish information as the seventh joint function of the military, along with the joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[5]

Finally, Congress addressed DOD's role in the information environment with a number of provisions in National Defense Authorization Acts—including requirements that led to DOD issuing the 2016 DOD *Strategy for Operations in the Information Environment,* the establishment of a

[3]GAO, *Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64 (Washington, D.C.: Dec. 10, 2020).

[4]Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Nov. 27, 2012, incorporating Change 1, Nov. 20, 2014).

[5]Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Mar. 25, 2013, incorporating Change 1, July 12, 2017).

DOD Principal Information Operations Advisor, and an IO posture review that the department has recently initiated.[6]

Since 2019, we have issued a series of reports assessing DOD operations in the information environment—including DOD cyberspace operations, information operations, and electromagnetic spectrum operations.[7] We have also issued reports on emerging threats to national security, threats attributed to emerging technology in the information environment (including 5G and internet-of-things devices), and units that conduct operations in the information environment.[8]

My testimony today describes (1) DOD's information operations terms and concept, and (2) DOD actions to implement the 2016 DOD strategy and address IO oversight and integration challenges.

This statement is based on our assessment of DOD documents that define and explain IO—including DOD's dictionary of military terms, DOD's IO policy directive, DOD's IO joint doctrine, and the 2016 DOD *Strategy for Operations in the Information Environment.*[9] This statement is

[6]See, for example, Pub. L. No. 113-66, § 1096 (2013); and Pub. L. No. 116-92, § 1631 (2019).

[7]GAO, *Cyberspace Operations: DOD Has Authorities and Organizations in Place, but Policies, Processes, and Reporting Could Be Improved*, GAO-20-13C (Washington, D.C.: Sept. 28, 2020); *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C.: Oct. 18, 2019); GAO-21-64; and *Electromagnetic Spectrum Operations: DOD Needs to Take Action to Help Ensure Superiority*, GAO-21-440T (Washington, D.C.: Mar. 19, 2021).

[8]GAO, *National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies*, GAO-19-204SP (Washington, D.C.: Dec. 13, 2018); *National Security: Actions Needed to Address 5G Telecommunications Risks*, GAO-21-256SU (Washington, D.C.: Mar. 5, 2021); *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Aug. 13, 2020); and *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*, GAO-19-570 (Washington, D.C.: Aug. 15, 2019).

[9]Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (as of January 2021); DOD, DOD Directive 3600.01, *Information Operations* (IO) (May 2, 2013, Incorporating Change 1, May 4, 2017); Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Nov. 27, 2012, incorporating Change 1, Nov. 20, 2014); and DOD, *Strategy for Operations in the Information Environment.*

also based on reports we issued in August and October 2019.[10] In addition, we obtained updates in April 2021. To conduct that work, we compared DOD strategy and guidance documents to actions taken by the department to determine the extent to which they had been implemented, interviewed DOD officials, and reviewed guidance documents regarding DOD oversight and integration of IO by selected DOD components. Our 2019 reports provide more details on the scope of our prior work and methodologies we used.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

IO-Related Terms and Examples of the IO Concept

Definitions for IO-Related Terms

DOD and others, including the Congressional Research Service and RAND, have IO-related terms as shown in figure 1.

[10]The report issued in August 2019 is a classified report. The report issued in October 2019 is a For Official Use Only version of the classified report. Both reports addressed the same objectives and use the same methodology. GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-19-510C (Washington, D.C.: Aug. 28, 2019) (S//NF); and GAO-20-51SU.

Figure 1: Information Operations-Related Terms Defined by DOD and Others

DOD-defined terms	Information environment	The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as the physical, informational, and cognitive (or human) dimensions.
	Information operations	The integrated employment during military operations of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.
	Information-related capability	A tool, technique, or activity employed within a dimension of the information environment that can be used to achieve a specific end. DOD does not have a definitive list of information-related capabilities because any capability could be used in a way that meets the definition, according to DOD officials. A DOD official recently told us that the term information-related capability will be retired from the common vocabulary, but for the purpose of this testimony the term will continue to be used.
Non-DOD-defined terms	Influence activities/ operations	DOD's current dictionary does not refer to the term "influence activities" or "influence operations." However, DOD's IO policy document refers to "influence activities" as an information-related capability, although the policy document does not define or describe these activities.[a] In 2009, RAND issued a study on behalf of the U.S. Army. In that study, RAND defines influence operations as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives."[b] A key difference between this definition of influence operations and DOD's definition of "information operations" is that RAND's definition includes all instruments of national power (i.e., diplomacy, information, military, and economics) whereas DOD's joint doctrine focuses on activities and operations conducted by the military.
	Information warfare	Neither the U.S. government (as a whole) nor DOD (as a department) have a definition for "information warfare." However, the Congressional Research Service notes that information warfare is a form of political warfare where targets include a nation state's government, military, private sector, and general population.[c] Taking place below the level of armed conflict, information warfare is the range of military and government operations to protect and exploit the information environment. It consists of both offensive and defensive operations: the protection and assurance of one's own information (information security), and information operations to advance interests. As noted in our 2019 report about DOD information operations, while DOD does not have a department-wide definition for information warfare, we found that several of the services were using the term.[d] For example, the U.S. Navy defines information warfare as the integrated application of capabilities to degrade, deny, deceive, or destroy an enemy's information environment or to enhance the effectiveness of friendly operations. Our report also noted that the U.S. Army has begun to use the term information warfare as well, but this change has not been made in doctrine or guidance.

Source: GAO analysis of Congressional Research Service, Department of Defense (DOD), and RAND information. | GAO-21-525T

Text of Figure 1: Information Operations-Related Terms Defined by DOD and Others

DOD-defined terms

- Information environment: The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as the physical, informational, and cognitive (or human) dimensions.
- Information operations: The integrated employment during military operations of information-related capabilities in concert with other

lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

- Information related capability: A tool, technique, or activity employed within a dimension of the information environment that can be used to achieve a specific end. DOD does not have a definitive list of information-related capabilities because any capability could be used in a way that meets the definition, according to DOD officials. A DOD official recently told us that the term information-related capability will be retired from the common vocabulary, but for the purpose of this testimony the term will continue to be used.

Non-DOD Defined terms

- Influence activities / operations:
  - DOD's current dictionary does not refer to the term "influence activities" or "influence operations." However, DOD's IO policy document refers to "influence activities" as an information-related capability, although the policy document does not define or describe these activities.a
  - In 2009, RAND issued a study on behalf of the U.S. Army. In that study, RAND defines influence operations as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives."b
  - A key difference between this definition of influence operations and DOD's definition of "information operations" is that RAND's definition includes all instruments of national power (i.e., diplomacy, information, military, and economics) whereas DOD's joint doctrine focuses on activities and operations conducted by the military.
- Information warfare:
  - Neither the U.S. government (as a whole) nor DOD (as a department) have a definition for "information warfare." However, the Congressional Research Service notes that information warfare is a form of political warfare where targets include a nation state's government, military, private sector, and general population.c Taking place below the level of armed conflict, information warfare is the range of military and government

operations to protect and exploit the information environment. It consists of both offensive and defensive operations: the protection and assurance of one's own information (information security), and information operations to advance interests.

- As noted in our 2019 report about DOD information operations, while DOD does not have a department-wide definition for information warfare, we found that several of the services were using the term.d For example, the U.S. Navy defines information warfare as the integrated application of capabilities to degrade, deny, deceive, or destroy an enemy's information environment or to enhance the effectiveness of friendly operations. Our report also noted that the U.S. Army has begun to use the term information warfare as well, but this change has not been made in doctrine or guidance.

[a]DOD, *DOD Dictionary of Military and Associated Terms*, (As of January 2021); and DOD Directive 3600.01, *Information Operations (IO)*, (May 2, 2013, Incorporating Change 1, May 4, 2017).

[b]RAND, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (2009).

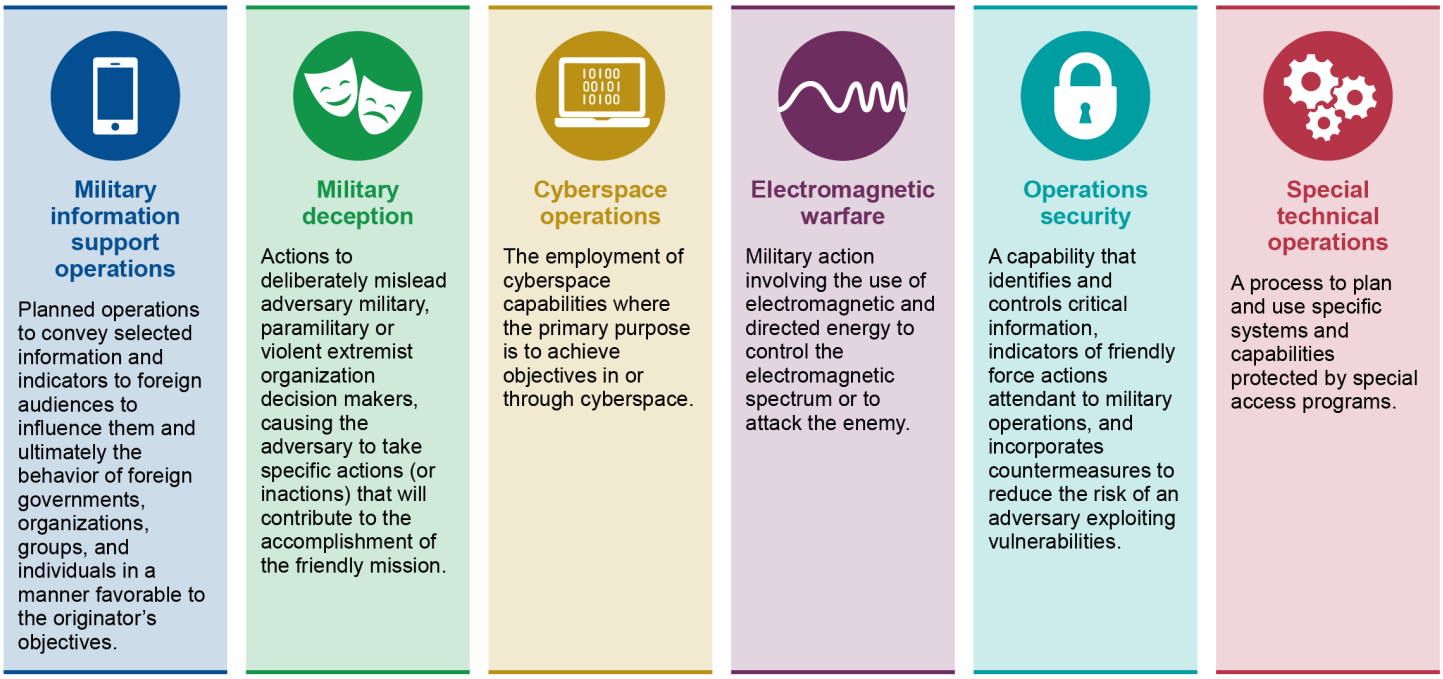
[c]Congressional Research Service, *Information Warfare: Issues for Congress*, R45142 (updated Mar. 5, 2018).

[d]GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C.: Oct. 18, 2019).

DOD can employ different information-related capabilities to achieve the commander's goals. To take advantage of the benefits of different capabilities and achieve greater effects, commanders can develop plans and execute operations that use two or more capabilities. Figure 2 highlights selected information-related capabilities that are identified in the 2016 DOD *Strategy for Operations in the Information Environment.* Others may include public affairs, civil-military operations, intelligence capabilities, and key-leader engagement.[11]

[11]DOD Directive 3600.01, *Information Operations (IO)*, also identifies "influence activities" as an example of information-related capabilities. However, the directive does not define the term or identify the type of activities that would be considered "influence activities."

Figure 2: Examples of DOD Information-Related Capabilities



Source: GAO analysis of Department of Defense (DOD) information. | GAO 21-525T

Text of Figure 2: Examples of DOD Information-Related Capabilities

- Military information support operations:
  Planned operations to convey selected information and indicators to foreign audiences to influence them and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.
- Military deception:
  Actions to deliberately mislead adversary military, paramilitary or violent extremist organization decision makers, causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.
- Cyberspace operations:
  The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.
- Electromagnetic warfare:
  Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

- Operations security:
  A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities.
- Special technical operations:
  A process to plan and use specific systems and capabilities protected by special access programs.

Although DOD has defined information environment, information operations, and information-related capabilities, DOD officials have acknowledged that DOD has had challenges agreeing to a common set of terms or definitions. For example, while neither DOD's dictionary of terms, IO policy directive, nor IO joint doctrine uses the term "Information Warfare," we previously reported that the Navy and Army are using this term.[12] We have also found that DOD does not have a complete list of information-related capabilities because, according to DOD officials, any capability could be used in a way that meets the current definition. Consequently, it could be challenging for combatant commanders to utilize IO as the principal mechanism to integrate, synchronize, employ, and adapt all information-related capabilities in the information environment to accomplish operational objectives against adversaries and potential adversaries, as required by DOD's IO policy directive.[13] DOD IO officials told us they have been working with DOD components to develop a more consistent set of IO-related terms while updating the IO strategy and joint doctrine.

Examples of Information Operations

DOD doctrine on IO describes how information-related capabilities can be used to create lethal and nonlethal effects to support achievement of the objectives to reach the desired end state. As highlighted in the following examples, DOD IO planners can *integrate* more than one information-related capability to achieve the commander's desired end state and it is

[12]*DOD Dictionary of Military and Associated Terms*, DOD Directive 3600.01, Joint Publication 3-13, and GAO-20-51SU.

[13]DOD Directive 3600.01.

this integration that enables desired effects in and through the information environment at specified times and locations.[14]

- DOD's joint doctrine on IO presents a hypothetical example where an adversary attempts to overthrow a country's government using lethal and nonlethal means to demonstrate that the government is not fit to support and protect its people.[15] To counter the adversary, DOD—working with other U.S. government agencies and the country's government and institutions—could mitigate the adversary's effectiveness through integrated planning and execution of information-related capabilities such as military information support operations, military deception, electromagnetic operations, cyberspace operations, security force assistance, combat operations, key leader engagement, and public affairs.
- The Air Force's IO doctrine highlighted that a commander could employ IO during a humanitarian assistance operation. The commander could influence host nation and regional cooperation and facilitate safe and orderly humanitarian assistance through the *integration* of public affairs activities and military information support operations messaging.[16]

DOD Has Made Limited Progress Implementing Its 2016 Strategy and Addressing IO Oversight and Integration Challenges

DOD Has Made Limited Progress Implementing Its 2016 IO Strategy

DOD's 2016 Strategy for Operations in the Information Environment was intended to "signal [the department's] commitment and resolve" and provide the Secretary of Defense's guidance on important steps that DOD must take as a department to enhance its ability to conduct military operations. Our 2019 report highlighted several actions that DOD took in

[14]*DOD Strategy for Operations in the Information Environment*.

[15]Joint Publication 3-13.

[16]Air Force, Air Force Doctrine Publication 3-13, *Information Operations* (Apr. 28, 2016).

response to its *2016 Strategy for Operations in the Information Environment.* For example:

- In March 2018, DOD issued the *Joint Concept for Integrated Campaigning* which addresses DOD's role in achieving U.S. goals outside of the traditional military sphere—such as competition below the threshold of armed conflict.[17]
- In July 2018, DOD issued the *Joint Concept for Operating in the Information Environment* to institutionalize and operationalize the military's approach to information operations so that the department can better compete with state and non-state actors.[18] The document describes how DOD can use information to influence others' behavior. For example, the concept states that DOD and its allies must be able to communicate a compelling narrative and anticipate and proactively counter an adversary's attempt to manipulate information.

However, as we reported in October 2019, DOD had not fully implemented its strategy. For example, DOD did not issue an implementation plan or an investment framework to guide the implementation of the strategy. OSD officials told us that the department was unable to fully implement the 2016 *Strategy for Operations in the Environment* because many of the tasks the department included in the strategy were not written in a way the department could execute. We reported that this may be the case with some tasks, but we determined that the primary cause of the uneven progress was in part due to the IO Executive Steering Group not implementing a process to facilitate and oversee the execution of the 2016 strategy. For example, the IO Executive Steering Group had not developed:

- an implementation plan and quarterly (or more frequent) progress reviews on the status of the strategy's implementation; and
- an investment framework that would identify planning priorities to address IO gaps.

Instead, during this timeframe, the IO Executive Steering Group shifted its focus and developed the *Joint Concept of Operations in the Information Environment,* conducted a capabilities-based assessment of DOD's ability

[17]Joint Chiefs of Staff, Jo*int Concept for Integrated Campaigning* (Mar. 16, 2018).

[18]Joint Chiefs of Staff, Joi*nt Concept for Operating in the Information Environment (JCOIE)* (July 25, 2018).

to operate in the information environment, and then started developing a new IO strategy.

We recommended that DOD establish a process that facilitates implementation of DOD's revised strategy for operations in the information environment and hold DOD components accountable for implementing this strategy. DOD did not concur with this recommendation.[19]

In April 2021, a DOD official told us that the department is updating the 2016 DOD *Strategy for Operations in the Information Environment* while it completes an analysis of capability gaps for operations in the information environment (i.e., posture review) that we had also recommended and Congress subsequently mandated the department complete.[20] According to the officials, once the Secretary of Defense issues the updated strategy, the Principal IO Advisor will use a process to oversee implementation of the IO strategy similar to one used by the DOD Principal Cyber Advisor to oversee the implementation of the DOD Cyber Strategy.[21]

DOD Has Established Roles and Responsibilities for IO, but Has Oversight and Integration Challenges

DOD Roles and Responsibilities

In our 2019 report, we highlighted that DOD had established department-wide IO roles and responsibilities and assigned many of them to the Under Secretary of Defense for Policy (USD (Policy)). The Under

[19]In our 2019 report, DOD deemed its response to this recommendation as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

[20]GAO-20-51SU and Pub. L. No. 116-92, § 1631 (2019).

[21]The DOD Principal Cyber Advisor established multiple oversight processes in support of the 2015 DOD Cyber Strategy, according to officials from the Office of the DOD Principal Cyber Advisor. These oversight processes included (1) the issuance of an overall implementation plan (or individual plans for different sections of the strategy) that identifies specific actions that will be taken and estimated completion dates, (2) assignment of senior DOD leader(s) (e.g., general and flag officers and/or civilian senior executives) who would be held accountable for implementing a specific section of the strategy, and (3) establishing progress reports (e.g., monthly, bimonthly, or quarterly) on the status of the actions identified in the implementation plan(s). The DOD Principal Cyber Advisor was able to use these oversight processes to monitor DOD's progress for the 2015 and 2018 cyber strategies.

Secretary has exercised some of those responsibilities, such as establishing the IO Executive Steering Group. However, the Under Secretary had not fulfilled other IO oversight responsibilities. Figure 3 shows the roles and responsibilities for IO established by DOD.

Figure 3: DOD Roles and Responsibilities for Information Operations

Under Secretary of Defense for Policy	**Principal Staff Advisor to the Secretary of Defense** In this role, the Under Secretary of Defense for Policy is the principal staff advisor to the Secretary of Defense and responsible for information operations (IO) oversight and management. **Senior DOD IO Official** In response to a requirement in the National Defense Authorization Act for Fiscal Year 2018, the Deputy Secretary of Defense designated the Under Secretary of Defense for Policy as the senior official for overseeing the integration of strategic IO and cyber-enabled IO. According to the memorandum, this designation was consistent with the Under Secretary's existing roles and responsibilities for IO.[a] However, as noted below the Under Secretary of Defense for Policy has largely delegated responsibilities associated with principal staff advisor and senior DOD IO official to the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, according to Office of the Secretary of Defense officials. **Co-Chair, IO Executive Steering Group** Co-chairs the primary coordination forum within DOD to inform, coordinate, and resolve IO issues among the DOD components. The Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism fulfills this role. **Principal Information Operations Advisor[b]** Responsible for the overall integration and supervision of the deterrence of, conduct of, and defense against information operations and promulgation of policies to ensure adequate coordination and deconfliction with the Department of State, the intelligence community, and other federal agencies, among other things.
IO Cross Functional Team	Consistent with Section 1631 of the National Defense Authorization Act for Fiscal Year 2020, DOD is in the process of establishing a full-time cross functional team composed of subject-matter experts selected from organizations within the Office of the Secretary of Defense, Joint Staff, military departments, defense agencies, and combatant commands, according to DOD officials.[c]
IO Executive Steering Group	**DOD's Senior Deliberative and Advisory Board for IO** Responsible for implementing the 2016 *DOD Strategy for Operations in the Information Environment* and providing input and recommendations to select Office of Secretary of Defense and Joint Staff processes.
DASD for Special Operations and Combating Terrorism	**Principal Staff Advisor to the Secretary of Defense, Senior DOD IO Official, and Co-Chair of the IO Executive Steering Group (*delegated for all*)** According to Office of the Secretary of Defense officials, the Under Secretary of Defense for Policy has largely delegated responsibilities for these roles to this official. Also, responsible for DOD policy related to special operations forces and personnel recovery, among other things.
Chairman of the Joint Chiefs of Staff	**Joint IO Proponent** The responsibilities of the Joint IO Proponent include three areas: joint policy and doctrine; planning, operations, and assessment; and force development.
Joint Staff Deputy Director for Global Operations	**Joint IO Proponent (*delegated*)** Executes the Joint IO Proponent responsibilities on the chairman's behalf. These day-to-day responsibilities include acting as co-chair of the IO Executive Steering Group and overseeing IO policy execution within the combatant commands and joint task forces.
Joint Information Operations Warfare Center	Assists the Joint IO Proponent (J39) in the execution of responsibilities and provides direct support to combatant commanders to include planning guidance. Also, provides IO support to analysis, planning and assessment of chairman plans and orders.
Military services[d]	The military services organize, train, equip, and provide forces for military operations, including IO and information-related capabilities. All military services have undertaken organizational steps to better position themselves for IO and to provide IO personnel to support combatant commands' military operations.
Combatant Commands	Utilizes IO as the principal mechanism to integrate, synchronize, employ, and adapt all information-related capabilities in the information environment to accomplish operational objectives against adversaries and potential adversaries. Develops, plans, programs and assesses IO as well as information-related capabilities execution in support of IO during all phases of military engagement and at all levels of war.

DASD Deputy Assistant Secretary of Defense

Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-525T

Text of Figure 3: DOD Roles and Responsibilities for Information Operations

Under Secretary for Defense Policy

- Principal Staff Advisor to the Secretary of Defense. In this role, the Under Secretary of Defense for Policy is the principal staff advisor to the Secretary of Defense and responsible for information operations (IO) oversight and management.
- Senior DOD IO Official. In response to a requirement in the National Defense Authorization Act for Fiscal Year 2018, the Deputy Secretary of Defense designated the Under Secretary of Defense for Policy as the senior official for overseeing the integration of strategic IO and cyber-enabled IO. According to the memorandum, this designation was consistent with the Under Secretary's existing roles and responsibilities for IO./a/ However, as noted below the Under Secretary of Defense for Policy has largely delegated responsibilities associated with principal staff advisor and senior DOD IO official to the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, according to Office of the Secretary of Defense officials.
- Co-Chair, IO Executive Steering Group. Co-chairs the primary coordination forum within DOD to inform, coordinate, and resolve IO issues among the DOD components. The Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism fulfills this role.
- Principal Information Operations Advisor/b/. Responsible for the overall integration and supervision of the deterrence of, conduct of, and defense against information operations and promulgation of policies to ensure adequate coordination and deconfliction with the Department of State, the intelligence community, and other federal agencies, among other things.

IO Cross Functional Team

- Consistent with Section 1631 of the National Defense Authorization Act for Fiscal Year 2020, DOD is in the process of establishing a full-time cross functional team composed of subject-matter experts selected from organizations within the Office of the Secretary of Defense, Joint Staff, military departments, defense agencies, and combatant commands, according to DOD officials./c/

IO Executive Steering Group

- DOD's Senior Deliberative and Advisory Board for IO. Responsible for implementing the 2016 DOD Strategy for Operations in the Information Environment and providing input and recommendations to select Office of Secretary of Defense and Joint Staff processes.

DASD for Special Operations and Combating Terrorism

- Principal Staff Advisor to the Secretary of Defense, Senior DOD IO Official, and Co-Chair of the IO Executive Steering Group (delegated for all). According to Office of the Secretary of Defense officials, the Under Secretary of Defense for Policy has largely delegated responsibilities for these roles to this official. Also, responsible for DOD policy related to special operations forces and personnel recovery, among other things.

Chariman of the Joint Chiefs of Staff

- Joint IO Proponent. The responsibilities of the Joint IO Proponent include three areas: joint policy and doctrine; planning, operations, and assessment; and force development.

Joint Staff Deputy Director for Global Operations

- Joint IO Proponent (delegated). Executes the Joint IO Proponent responsibilities on the chairman's behalf. These day-to-day responsibilities include acting as co-chair of the IO Executive Steering Group and overseeing IO policy execution within the combatant commands and joint task forces.

Joint Information Operations Warfare Center

- Assists the Joint IO Proponent (J39) in the execution of responsibilities and provides direct support to combatant commanders to include planning guidance. Also, provides IO support to analysis, planning and assessment of chairman plans and orders.

Military services/d/

- The military services organize, train, equip, and provide forces for military operations, including IO and information-related capabilities. All military services have undertaken organizational steps to better

position themselves for IO and to provide IO personnel to support combatant commands' military operations.

Combatant Commands

- Utilizes IO as the principal mechanism to integrate, synchronize, employ, and adapt all information-related capabilities in the information environment to accomplish operational objectives against adversaries and potential adversaries. Develops, plans, programs and assesses IO as well as information-related capabilities execution in support of IO during all phases of military engagement and at all levels of war.

[a]Deputy Secretary of Defense Memorandum, Designated Senior Official for the Integration of Strategic Information Operations and Cyber-Enabled Information Operations (June 13, 2018) and Pub. L. No. 115-91, § 1637 (2017). The statute requires the designated senior official to implement and oversee processes and procedures related to information operations.

[b]DOD is in the process of pursuing a full-time, Deputy Principal Information Operations Advisor, according to DOD officials. The Deputy will be a general or flag officer who oversees the Information Operations Cross-Functional Team and report directly to USD (Policy).

[c]Pub. L. No. 116-92, § 1631 (2019).

[d]For the purposes of our 2019 report, we referred to the military services as including the Army, Marine Corps, Navy, and Air Force. The Coast Guard and Space Force, although both military services, were not included in the scope of our review.

Oversight Challenges

DOD has established department-wide IO roles and responsibilities and, as noted above, assigned most to the USD (Policy). The Under Secretary has exercised some responsibilities, such as establishing an executive steering group. However, the Under Secretary had not fulfilled other IO oversight responsibilities.[22]

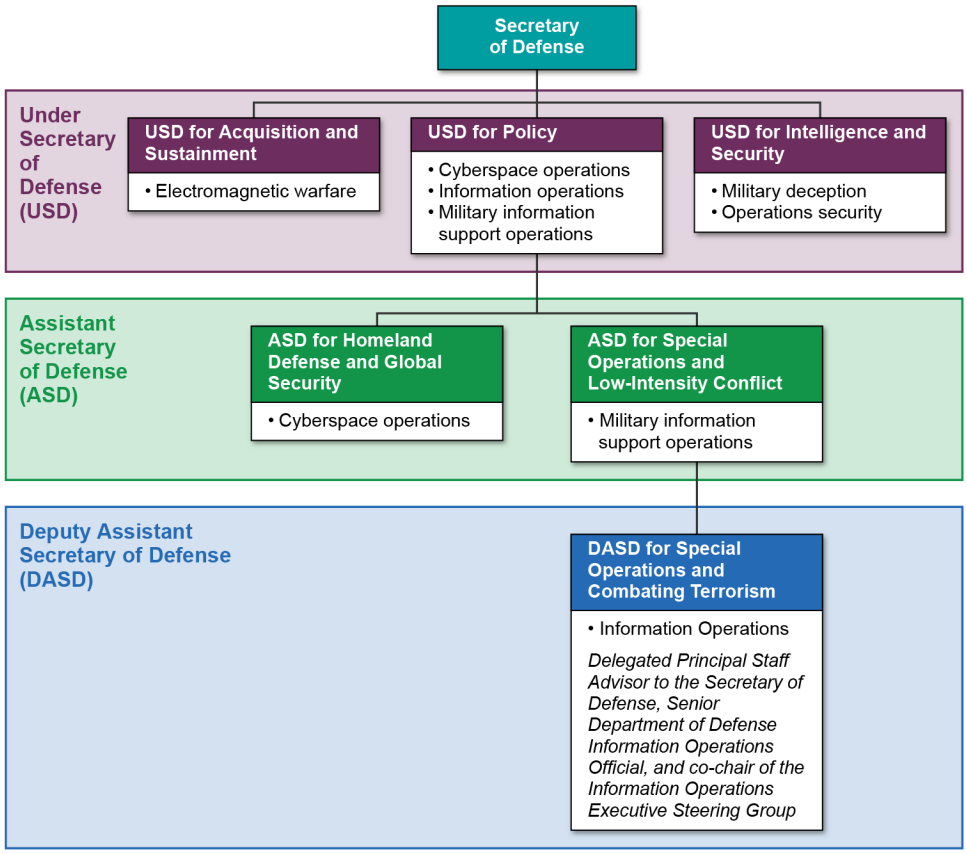
One of the challenges in managing and overseeing IO efforts is that the majority of IO responsibilities have been delegated to a Deputy Assistant Secretary of Defense (and whose primary focus is on special operations and combatting terrorism), according to DOD officials. As shown in figure 4, there are different leaders within the Office of the Secretary of Defense who are responsible for individual information-related capabilities and all

[22]In our 2019 report, DOD deemed specific examples of how the department had not implemented the strategy as sensitive information not subject to public release. As such, this written statement is unable to elaborate on specific actions not taken.

of them outrank the Deputy Assistant Secretary of Defense, report to a different Under Secretary of Defense, or both.[23]

[23]Conversely, according to the Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, "Russia sees the information domain differently than the United States and its allies and partners and that Russian publications and actions indicate its government maintains a holistic concept of 'information confrontations'." Similarly, a 2018 National Defense University paper about China's Strategic Support Force states the Strategic Support Force combines assorted space, cyber, electromagnetic, and psychological warfare capabilities from across the People's Liberation Army services and its former General Department. DOD, Joint Statement for the Record of Mr. Christopher Maier, Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Mr. Neill Tipton, Director of Defense Intelligence (Collections and Special Programs), and Mr. James Sullivan, Defense Intelligence Officer for Cyber, Defense Intelligence Agency before House Armed Services Committee Subcommittee on Intelligence and Special Operations on "Disinformation in the Gray Zone: Opportunities, Limitations, Challenges." (Mar. 16. 2021). National Defense University, China's Strategic Support Force: A Force for a New Era (Washington, D.C.: December 2018).

Figure 4: Responsibilities for Some Information-Related Capabilities across the Office of the Secretary of Defense



Source: GAO analysis of Office of the Secretary of Defense information. | GAO-21-525T

Text of Figure 4: Responsibilities for Some Information-Related Capabilities across the Office of the Secretary of Defense

1) Secretary of Defense

   a) Under Secretary of Defense for Acquisition and Sustainment. Electromagnetic Warfare

   b) Under Secretary of Defense for Policy. Cyberspace operations. Information Operations. Military information operations.

      i) Assistant Secretary of Defense for Homeland Defense and Global Security. Cyberspace operations.

ii) Assistant Secretary of Defense for Special Operations and Low-intensity Conflict. Military information support operations

(1) Deputy Assistant Secretary of Defense. DASD for Special Operations and Combating Terrorism
Information Operations. Delegated Principal Staff Advisor to the Secretary of Defense, Senior Department of Defense Information Operations Official, and co-chair of the Information Operations Executive Steering Group

c) Under Secretary of Defense for Intelligence and Security. Military deception. Operations security.

During our 2019 review, we found two underlying factors on why the USD (Policy) had not fulfilled required oversight responsibilities for managing IO across DOD.

First, we found that the USD (Policy) had not assessed the tasks, workload, or the resources needed to manage, oversee, and coordinate IO in the department, including the activities of the other offices responsible for specific information-related capabilities. In 2018, the Deputy Secretary of Defense initially designated the USD (Policy) as the senior DOD IO official and directed an analysis of new tasks, potential workload, and resource requirements of the designation.[24] However, we asked officials in the Office of the USD (Policy) about the analysis, and they said the office has not conducted such an assessment. We recommended that the USD (Policy) assess the new tasks, potential workload, and resources needed to fulfill required oversight responsibilities for managing IO across DOD and hold accountable the other offices overseeing the information-related capabilities. DOD did not concur with this recommendation.[25] However, in April 2021, a DOD official told us that the Secretary of Defense had approved additional resources to support IO leadership efforts.

Second, we found that DOD had not issued policy formalizing the IO Executive Steering Group's responsibilities for providing IO oversight and

[24]Deputy Secretary of Defense, *Designated Senior Official for the Integration of Strategic Information Operations and Cyber-Enabled Information Operations*.

[25]In our 2019 report, DOD deemed its response to this recommendation as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

management and deconflicting and resolving issues within the department in accordance with DOD's IO directive. This has left the group without authority to exercise its oversight role, according to OSD officials. We recommended that the USD (Policy) issue policy identifying the IO Executive Steering Group's formal responsibilities for providing IO oversight and management and deconflicting and resolving issues within the department. DOD did not concur with this recommendation.[26] In April 2021, a DOD official told us that the IO Executive Steering Group will maintain its advisory role. Some of the issues we heard during our 2019 review may be mitigated by the new IO Cross-Functional Team that DOD subsequently established in response to a requirement in the National Defense Authorization Act for Fiscal Year 2020.[27]

Integration Challenges

In our 2019 report, we highlighted that DOD had integrated information-related capabilities in some military operations, but had not addressed key planning, coordination, and operational challenges. Specifically, DOD had not assessed these challenges or clearly defined roles and responsibilities between geographic combatant commands and U.S. Cyber Command. Consequently, we recommended that DOD conduct a comprehensive posture review to fully assess challenges. Such a posture review would assist DOD in more effectively operating while using information-related capabilities.

We also recommended that DOD clearly define roles and responsibilities between geographic combatant commands and U.S. Cyber Command. Such action would enable DOD to more effectively plan and execute operations across boundaries and below the level of conflict. DOD did not concur with these recommendations.[28] However, the National Defense Authorization Act for Fiscal Year 2020 included a provision that required

[26]In our 2019 report, DOD deemed its response to this recommendation as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

[27]Pub. L. No. 116-92, § 1631 (2019). The IO Cross-Functional Team will report directly to a full-time Deputy Principal IO Advisor that DOD is in the process of selecting, according to DOD officials. The Deputy Principal IO Advisor will be a general officer or flag officer and report directly to the USD (Policy).

[28]In our 2019 report, DOD deemed its response to these recommendations as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

the Secretary of Defense to conduct such a posture review.[29] In April 2021, DOD officials told us that the department had taken initial steps for the posture review, but did not provide an estimated completion date. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 places a limitation on funding until DOD completes this posture review and issues an updated IO strategy.[30]

In conclusion, it is important that DOD continues to take actions that recognize the value of information as a joint function and conduct operations in the information environment. The United States remains in competition with our potential adversaries in strengthening our respective capabilities in the information environment. DOD has made some progress, but there are opportunities for improved leadership and for integration of IO. It is important that our military continue efforts to put in place the necessary people, policies, programs, and partnerships to defend against these new threats in the information environment. I look forward to continuing to work with this committee and the department to help it address these challenges and make the most of these opportunities.

Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions about this testimony, please contact Joseph W. Kirschbaum, Director, Defense Capabilities and Management, at (202) 512-9971 or Kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Tommy Baril (Assistant Director), Neil Feldman (Analyst-in-Charge), Tracy Barnes, Mallory Bryan, Jeffrey Cirillo, Benjamin Emmel, Evan Keir, Amie Lesser, Ricardo A. Marquez, Richard Powelson, Breana Stevens, and Yee Wong. GAO staff who made key contributions to the 2019 report that part of this testimony is based on are

[29]Pub. L. No. 116-92, § 1631(g).

[30]Pub. L. No. 116-283, § 1749 (2021).

Tommy Baril (Assistant Director), Jennifer Spence (Analyst-in-Charge), Tracy Barnes, Nicholas Benne, Christopher Gezon, Amie Lesser, Ned Malone, Richard Powelson, and Garrett Riba.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548