Report to Congressional Committees

May 2021

DEFENSE INTELLIGENCE AND SECURITY

DOD Needs to Establish Oversight Expectations and to Develop Tools That Enhance Accountability

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

GAO-21-295

GAO@100 Highlights

Highlights of GAO-21-295, a report to congressional committees

May 2021

DEFENSE INTELLIGENCE AND SECURITY

DOD Needs to Establish Oversight Expectations and to Develop Tools That Enhance Accountability

Why GAO Did This Study

DOD's Defense Intelligence Enterprise and Defense Security Enterprise play a vital role in supporting DOD's operations and priorities. The Under Secretary of Defense for Intelligence and Security and its corresponding office oversee these enterprises. The roles and responsibilities of the office have grown in recent years, particularly in the area of security.

Committee reports accompanying the National Defense Authorization Act for Fiscal Year 2020 and Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 included provisions for GAO to assess the office. GAO's report (1) describes how the office's responsibilities and organization have evolved, and the composition of its workforce, and (2) evaluates how the office conducts oversight and the extent to which it is able to assess the effectiveness of the enterprises.

GAO collected and analyzed workforce data; interviewed DOD officials; reviewed policies and other related documentation; and conducted four case studies of specific mission areas to assess oversight by the office.

What GAO Recommends

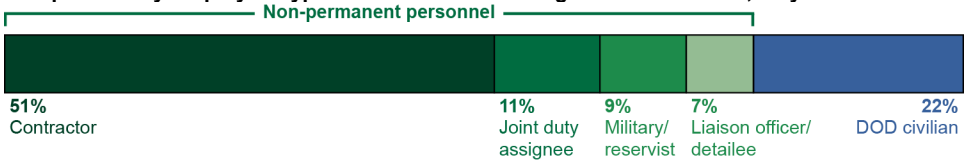
GAO recommends that the Under Secretary of Defense for Intelligence and Security establish clear oversight expectations and develop and use tools that enhance accountability for specific mission areas. DOD concurred with GAO's recommendations.

View GAO-21-295. For more information, contact Brian M. Mazanec at (202) 512-5130 or mazanecb@gao.gov.

What GAO Found

The Office of the Under Secretary of Defense for Intelligence and Security (the office) gained new responsibilities from 2017 through 2020—including in the areas of artificial intelligence, law enforcement, personnel vetting, and identity intelligence—and made structural changes within its organization. For example, in 2018, it assumed new responsibilities to oversee and to manage defense law enforcement authorities, training, and standards, in part to consolidate all authorities and capabilities for security-related missions into the office. It has also made internal organizational changes in its directorates, in part to better align its dual intelligence and security missions under its Directors for Defense Intelligence. The office's workforce is composed of largely non-permanent personnel to fulfill its responsibilities. According to GAO's analysis, as of July 2020, 78 percent of the office's workforce across the four directorates were non-permanent personnel—consisting of contractors, joint duty assignees, military/reservists, and liaison officers or detailees (see fig.).

The Office of the Under Secretary of Defense for Intelligence and Security's Workforce Composition by Employee Type across the Four Intelligence Directorates, July 2020



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-295

The office uses a variety of mechanisms to conduct oversight of the Defense Intelligence Enterprise and the Defense Security Enterprise (enterprises)—including policy development, inspections, and governance bodies. For example, it chairs the Defense Security Enterprise Executive Committee, which is the senior-level governance body for security policy coordination.

However, the office has experienced challenges in its enterprise oversight, including governance bodies not operating as intended and unclear roles and responsibilities. For example, GAO found that one mission area governance body had not met for several years and that the office had not established clear objectives for such bodies. In another area, Department of Defense (DOD) policy for open source intelligence designates an agency as the lead component and defines the term, but DOD does not outline the extent of the lead component's authority. These challenges exist in part because the office has not established clear expectations for oversight, including refining business rules for governance bodies and clarifying key terms critical to oversight. This has resulted in a lack of clarity around authorities and decision-making.

The office is not well-postured to assess the effectiveness of the intelligence and security enterprises in part because it has not developed tools to enhance accountability, such as goals, desired outcomes, and performance metrics. Without taking further actions, the office cannot fully assess the extent to which the enterprises are meeting the objectives of the *2018 National Defense Strategy* and the *2020 Defense Intelligence Strategy*.

Contents

Figures

Abbreviations

CI	Counterintelligence
CM	Collection management
DDI	Director for Defense Intelligence
DDI(CL&S)	Director for Defense Intelligence (Counterintelligence, Law Enforcement, and Security)
DDI(CSP)	Director for Defense Intelligence (Collection and Special Programs)
DDI(ISP&R)	Director for Defense Intelligence (Intelligence and Security Programs and Resources)
DDI(WS)	Director for Defense Intelligence (Warfighter Support)
DIA	Defense Intelligence Agency
DOD	Department of Defense
IC	Intelligence Community
NGA	National Geospatial-Intelligence Agency
ODNI	Office of the Director of National Intelligence
OSINT	Open source intelligence
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
USD(I&S)	Under Secretary of Defense for Intelligence and Security

441 G St. N.W.
Washington, DC 20548

May 6, 2021

Congressional Committees

The Department of Defense's (DOD) intelligence and security enterprises—the organizations that perform intelligence and security functions for the department—play a vital role in supporting DOD's operational requirements and the strategic priorities of the Secretary of Defense.[1] The *2018 National Defense Strategy* emphasizes that the long-term strategic competitions with China and Russia are the principal priorities for DOD and that such competitions require the integration of multiple elements of national power, including intelligence.[2] The Defense Intelligence Enterprise and the Defense Security Enterprise (enterprises) are integral to these strategic priorities. Congress and DOD created the position of Under Secretary of Defense for Intelligence and Security (USD(I&S)), and its corresponding Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), in the aftermath of the terrorist attacks of September 11, 2001, to better manage and oversee these enterprises and to serve as a single focal point for intelligence within the department.[3] The roles, missions, and responsibilities of OUSD(I&S) are expansive and have continued to grow in recent years. For example, in 2019, OUSD(I&S) assumed new responsibility for ensuring the DOD's Defense Counterintelligence and Security Agency had the resources to serve as the primary federal entity for conducting background investigations for the federal government.

[1]Specifically, DOD defines the Defense Intelligence Enterprise as the organizations, infrastructure, and measures to include policies, processes, procedures, and products of the intelligence, counterintelligence, and security components of the Joint Staff, combatant command, military departments, and other DOD elements that perform national intelligence, defense intelligence, intelligence-related, counterintelligence, and security functions, as well as those organizations under the authority, direction, and control of the USD(I&S). DOD defines the Defense Security Enterprise as the organizations, infrastructure, and measures—including policies, processes, procedures, and products—in place to safeguard DOD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences.

[2]Department of Defense, *2018 National Defense Strategy* (2018).

[3]Section 901 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003, Pub. L. No. 107-314 (2002) created the position of Under Secretary of Defense for Intelligence. In 2019, Congress renamed the position as the Under Secretary of Defense for Intelligence and Security. Section 1621 of the National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92 (2019).

House Report 116-120, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2020, and House Report 116-151, accompanying a bill for the Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, included provisions for GAO to provide an assessment of the roles, missions, and responsibilities of OUSD(I&S). GAO's report (1) describes how OUSD(I&S)'s responsibilities and organization have evolved since 2017, and the composition of its workforce to carry out its responsibilities; and (2) evaluates how OUSD(I&S) conducts oversight and the extent to which it is able to assess the effectiveness of the enterprises. As a result of limitations on government operations in response to the Coronavirus Disease 2019 (COVID-19), our original timeline for issuing this report was delayed by several months because of impacts to government and other operations related to COVID-19.

For both objectives, we reviewed DOD issuances, policies, and processes for intelligence and security oversight. We interviewed or received written responses on such oversight from OUSD(I&S) officials and Defense Intelligence Enterprise and Defense Security Enterprise components—including defense intelligence agencies, the military services, and combatant commands. We also collected and analyzed data from OUSD(I&S) relevant to its oversight responsibilities.

For our first objective, we reviewed documentation establishing new responsibilities and organizational changes in OUSD(I&S) since 2017 and interviewed officials about these changes. We also collected and analyzed data from the Directors for Defense Intelligence (DDI) on their workload, workforce, and funding, which we determined to be sufficiently reliable for the purposes of this report. For our second objective, we collected documents and interviewed DOD officials to assess how OUSD(I&S) oversees the Defense Intelligence Enterprise and the Defense Security Enterprise. We combined a review of DOD issuances, policies and processes for intelligence and security oversight, and senior leadership interviews, with the conduct of four case studies in the mission areas of collection management (CM), counterintelligence (CI), industrial

security, and open source intelligence (OSINT).[4] Through these four case studies, we reviewed mission area-specific documentation and interviewed specific DOD components to examine how OUSD(I&S) oversees intelligence and security activities carried out by DOD components. We compared the information we collected against relevant laws, leading collaboration practices based on prior work, and *Standards for Internal Control in the Federal Government*.[5] The control environment component of internal control—particularly the principle of exercising oversight responsibility—was significant to this objective. We assessed DOD's implementation of this component by reviewing DOD issuances and interviewing DDI officials. Specifically, federal internal control standards require clear expectations, so we assessed through our case studies and DDI interviews whether OUSD(I&S) had established clear expectations for how they would conduct oversight for the intelligence and security enterprises. See appendix I for more details on our scope and methodology and a full listing of the organizations that we interviewed, as well as the Related GAO Products page for relevant GAO reports. Appendix II contains the detailed results of our case study analyses.

We conducted this performance audit from July 2019 to May 2021 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

[4]We conducted four case studies to provide a sample of mission areas that cut across the Defense Intelligence Enterprise and the Defense Security Enterprise. We selected our case studies through a judgmental sample based on recommendations from GAO subject-matter experts and DOD entities with oversight responsibilities; we excluded some mission areas that were subjects of recent or ongoing GAO work. The assessments we made in our case studies are not generalizable across the full spectrum of OUSD(I&S) responsibilities, but rather provide examples of how OUSD(I&S) executes its oversight responsibilities in specific mission areas. See appendix II for more specific information on case studies.

[5]See section 137 of title 10, United States Code, and GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). We assessed that all leading collaboration practices were relevant to our review. GAO, *Managing For Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: September 2012) and GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005). However, we did not assess OUSD(I&S) activities against the leading collaboration practice regarding interagency resources due to the classification level of the information required.

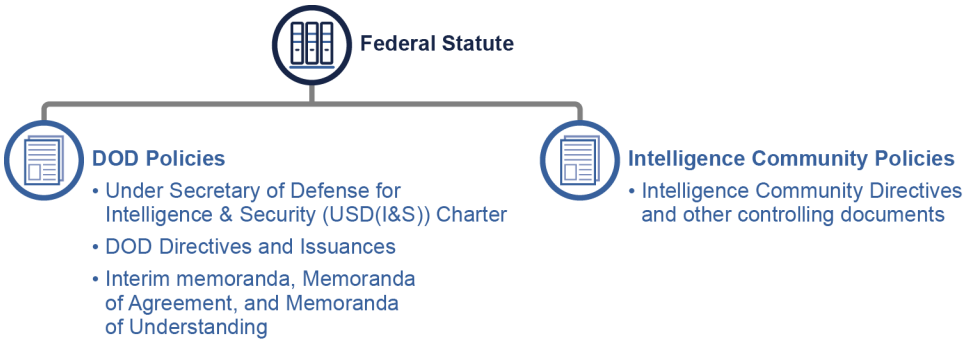
the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

OUSD(I&S) Responsibilities

Federal statute and DOD and Intelligence Community (IC) policies establish the roles, purpose, and responsibilities of the OUSD(I&S).[6] See figure 1 for more details.

Figure 1: Sources of Responsibility for the Office of the Under Secretary of Defense for Intelligence and Security



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-295

First established by Congress in 2002, the USD(I&S) provides the Secretary of Defense a single focal point for intelligence. By statute, the USD(I&S) is appointed by the President, confirmed by the Senate, and is subject to the authority, direction, and control of the Secretary of Defense. The USD(I&S) is statutorily responsible for the overall direction and supervision of policy, program planning and execution, and use of resources for DOD intelligence activities that are part of the Military Intelligence Program and execute the functions for the National

[6]*See* 10 U.S.C. § 137 and DOD Directive 5143.01, Under Secretary of Defense for Intelligence and Security (USD(I&S)) (Oct. 24, 2014) (change 2, Apr. 6, 2020) which OUSD(I&S) officials refer to as the USD(I&S) charter.

Intelligence Program of the DOD.[7] The position is also responsible for personnel security, physical security, industrial security, operations security, insider threat programs, and the protection of classified information and controlled unclassified information related to DOD activities. Lastly, the statute requires the USD(I&S) to prioritize the protection of privacy and civil liberties in accordance with federal law and DOD policy.

Issued by the Secretary of Defense, the USD(I&S) charter establishes the USD(I&S) as the principal staff assistant and advisor to the Secretary of Defense and the Deputy Secretary of Defense for intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters.[8] The charter places several defense agencies under the authority, direction, and control of the USD(I&S), including the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service, the National Reconnaissance Office, and the Defense Counterintelligence and Security Agency.

The USD(I&S) is responsible for oversight of the Defense Intelligence Enterprise and the Defense Security Enterprise, as described in its charter. The Under Secretary also issues DOD directives and instructions establishing policy, roles, and responsibilities for OUSD(I&S) and the DOD components. For example, the charter assigns USD(I&S) the responsibility to manage and oversee CI in the department, while a DOD directive on CI assigns the office nine separate responsibilities related to its management and oversight role.[9] Serving as the Director of Defense Intelligence to the Director of National Intelligence, OUSDI(I&S) also

[7]The two major components of the U.S. intelligence budget are the National Intelligence Program and the Military Intelligence Program. The National Intelligence Program includes all programs, projects, or activities of the IC as well as any other IC programs designated jointly by the Director of National Intelligence and the head of department or agency, or the Director of National Intelligence and the President. The Military Intelligence Program is devoted to intelligence activity conducted by the military departments and agencies in DOD that support tactical U.S. military operations. See "U.S. Intelligence Community Budget," IC Budget, Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/ic-budget.

[8]DOD Directive 5143.01.

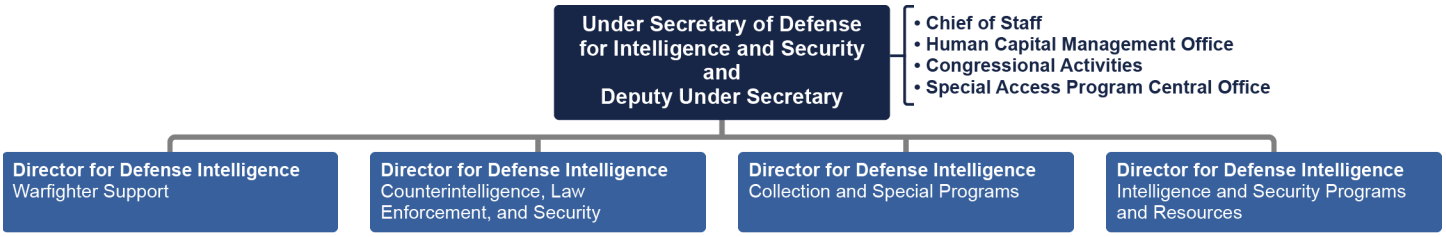
[9]DOD Directive 5240.02, *Counterintelligence (CI)* (Mar. 17, 2015) (change 1, May 16, 2018).

gains responsibilities through IC policies and directives, such as ones relating to security and budgeting.

OUSD(I&S) Organization and Directors for Defense Intelligence (DDI)

OUSD(I&S) has four directorates that are responsible for broad portfolios within the organization. Figure 2 displays an overview of the current organization of the office, as of January 2021.

Figure 2: Key Elements of the Office of the Under Secretary of Defense for Intelligence and Security



Source: GAO analysis of Department of Defense information. | GAO-21-295

The Deputy Under Secretary and four DDIs assist USD(I&S) in carrying out its core intelligence and security responsibilities. Each DDI is responsible for a staff that manages a portfolio of USD(I&S) responsibilities, including:

- **DDI, Warfighter Support (DDI(WS)).** Oversees operational support to warfighters, intelligence information sharing and foreign disclosure, policy and strategic development, assessment of enterprise performance, and engagement with allies and international partners.
- **DDI, Counterintelligence, Law Enforcement, and Security (DDI(CL&S)).** Responsible for policy, processes, and resources for counterintelligence (CI), security, and law enforcement.
- **DDI, Collection and Special Programs (DDI(CSP)).** Oversees technical collection capabilities and clandestine technical operations for all intelligence disciplines, including signals intelligence, geospatial intelligence, measurement and signature intelligence, and human intelligence.
- **DDI, Intelligence and Security Programs and Resources (DDI(ISP&R)).** Responsible for budgeting and resources—including

management of the Military Intelligence Program, battlespace awareness portfolio, and ISR capabilities.[10]

In addition to the DDIs, several offices report directly to USD(I&S) and are responsible for an individual function, such as human capital or congressional activities.

Case Study Mission Areas

We reviewed four specific intelligence and security mission areas as case studies to examine OUSD(I&S) oversight of the Defense Intelligence Enterprise and Defense Security Enterprise in practice. A brief overview of these mission areas follows. See appendix II for more details.

- **Collection management (CM).** CM is the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Within DOD, DIA serves as the Defense Collection Manager, but the agency has delegated key CM responsibilities—including strategic planning, policy development, and resource requirements—to the Joint Chiefs of Staff, Director for Intelligence, J2, as the Deputy Defense Collection Manager and the Functional Manager for Collection Management.
- **Counterintelligence (CI).** CI consists of intelligence activities conducted to identify, deceive, exploit, disrupt, and protect against espionage and foreign powers. CI missions include countering espionage and international terrorism, among others. Within DOD, OUSD(I&S) holds overall responsibility for CI matters, including developing policy and resolving issues among components, while the DIA Director serves as the DOD CI Manager and a central management organization. Three of the military services—Army, Navy, and Air Force—provide services through their respective military department CI organizations: Army Counterintelligence, Naval Criminal Investigative Service, and Air Force Office of Special Investigations.
- **Industrial security.** Industrial security refers to safeguarding classified information that is released to contractors, licensees, and grantees of the federal government. The National Industrial Security Program serves as a single, integrated security program to protect this classified information. USD(I&S) has the responsibility to oversee,

[10]The Battlespace Awareness Capability Portfolio consists of systems or programs whose primary mission is not intelligence, but has a secondary mission to provide intelligence while conducting its primary mission. USD(I&S) is responsible for policies and funds associated with the Battlespace Awareness Capability Portfolio.

manage, and issue operating standards and policy relating to industrial security. The Defense Counterintelligence and Security Agency administers the program—including investigating contractors, personnel, and facilities and certifying access to classified information—and DOD components are responsible for including the appropriate clauses in contracts requiring access to classified information.

- **Open Source Intelligence (OSINT).** OSINT is relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. It complements the other intelligence disciplines and can be used to fill intelligence gaps. While OUSD(I&S) is responsible to provide oversight and direction of defense OSINT capabilities, policies, plans, and programs, DIA serves as the DOD lead component on OSINT.

OUSD(I&S) Gained New Responsibilities, Realigned Its Organization, and Has a Workforce Composed Largely of Non-Permanent Personnel

OUSD(I&S) gained new responsibilities from 2017 through 2020, leading to structural changes within the organization that highlight the importance of its security mission. It also has a workforce composed largely of non-permanent personnel to execute its oversight responsibilities.

OUSD(I&S) Gained New Mission Responsibilities and Made Organizational Changes from 2017 through 2020 That Highlighted the Importance of Its Security Mission

As noted previously, the OUSD(I&S) charter is one of the key guiding documents for establishing responsibilities delegated to the office from the Secretary of Defense. OUSD(I&S) also gains new mission responsibilities through Executive Orders, DOD or IC directives and policies, and direct assignments from the Secretary of Defense and USD(I&S), including priority adjustments based on ongoing world events or changes in the operating environment. For example, according to OUSD(I&S) officials, in the aftermath of the Naval Air Station Pensacola terrorist attack in December 2019, OUSD(I&S)—directed by the Secretary of Defense—led a department-wide review to include pursuing any security changes needed, assessing how such changes affected DOD

components, and liaising with Congress and the press.[11] Figure 3 shows selected key changes in both OUSD(I&S)'s mission responsibilities and internal organization from 2017 through 2020.

Figure 3: Selected Key Changes in the Office of the Under Secretary of Defense for Intelligence and Security's (OUSD(I&S)) Mission Responsibilities and Organization from 2017 through 2020

Source: GAO analysis of Department of Defense information. | GAO-21-295

[a]This office merged with an office focused on integration activities with "Five Eyes" partners to form the new Commonwealth & Partner Engagement office within DDI (WS). "Five Eyes" partner countries include Australia, Canada, New Zealand, the United Kingdom, and the United States.

[b]This office was renamed the Strategy, Policy, and Enterprise Assessment office within DDI (WS).

[11]C. Todd Lopez, "DOJ Finds Pensacola Attack 'Act of Terrorism;' New Rules for Foreign Military Students," *DOD News*, U.S. Department of Defense, January 17, 2020, https://www.defense.gov/Explore/News/Article/Article/2060608/doj-finds-pensacola-attack-act-of-terrorism-new-rules-for-foreign-military-stud/ for a brief summary of the attack and the resulting investigation.

These new mission responsibilities and internal organizational changes are described in more detail below.[12]

New Mission Responsibilities

OUSD(I&S) gained new mission responsibilities every year from 2017 through 2020—including in the areas of artificial intelligence, law enforcement, personnel vetting, and identity intelligence—as seen in figure 3.

- **Artificial intelligence.** In 2017, DOD, in a memorandum from the Deputy Secretary of Defense, established the Algorithmic Warfare Cross-Functional Team, or Project Maven, and gave authority and direction over Project Maven to OUSD(I&S). In June 2020, Project Maven officials reported that their office had more than 30 personnel. OUSD(I&S)'s Project Maven office establishes policy and provides guidance for all algorithm-based technology initiatives affecting intelligence mission areas within the Defense Intelligence Enterprise. This includes overseeing implementation of a DOD data labeling effort for full-motion video and overhead imagery.[13] According to OUSD(I&S) officials, Project Maven is designed to develop mature artificial intelligence projects and facilitate their placement into permanent DOD programs.
- **Law enforcement.** In 2018, an USD(I&S) and USD(Personnel and Readiness) memorandum approved by the Deputy Secretary of Defense directed that OUSD(I&S) assume new responsibilities previously under the direction of the Under Secretary of Defense for Personnel and Readiness to oversee and to manage defense law enforcement, including law enforcement authorities, training, and standards. For example, OUSD(I&S) officials now chair the Defense Law Enforcement Council and host other key law enforcement forums. The office also is responsible for revising DOD issuances on law enforcement, including developing new policies for detention authorities and options for a DOD security force construct.
- **Personnel vetting.** In 2019, OUSD(I&S), through an Executive Order, assumed new responsibilities relating to personnel vetting. It established a temporary Personnel Vetting Transformation Office

[12]USD(I&S) made some other changes in the OUSD(I&S) organization, including the establishment of a Special Advisor for Integration and Innovation and the internal realignment of the foreign disclosure, defense analysis, and operations security missions.

[13]Project Maven gained significant support in fiscal year 2018 within OUSD(I&S), with nearly $180 million allocated in research and development funds, according to OUSDI(I&S) officials.

within its organization to facilitate the transfer of the background investigation mission, personnel, and resources from the Office of Personnel Management to the Defense Counterintelligence and Security Agency.[14] After overseeing the shift of the mission to conduct background investigations to DOD from the National Background Investigations Bureau, OUSD(I&S) transitioned the Personnel Vetting Transformation Office to the Defense Counterintelligence and Security Agency in March 2020.[15] OUSD(I&S) maintains the responsibility to develop personnel security policy and guidance for the department.

- **Identity intelligence.** In 2020, a USD(I&S) memorandum approved by the Deputy Secretary of Defense directed that DIA transfer its identity intelligence program office to OUSD(I&S), which includes new responsibilities for biometrics- and forensics-enabled intelligence.[16] Whereas previously OUSD(I&S) had only one person working on identity intelligence issues, it now has 12 personnel with such responsibilities, according to OUSD(I&S) officials. These include providing guidance on DOD biometrics- and forensics-enabled programs, activities, and initiatives and establishing priorities for such programs.

According to senior leadership in one DDI, the enterprise management or execution of programs is typically delegated to components within the enterprises, such as a service or combat support agency. OUSD(I&S)

[14]*See* Pub. L. No. 115-91, § 925 (2017) for the statutory requirements relating to the transfer of the background investigation mission, personnel, and resources. Executive Order 13869, *Transferring Responsibility for Background Investigations to the Department of Defense,* 84 Fed. Reg. 18125 (Apr. 29, 2019) (amending Exec. Order No. 13467), authorized a new office, the Personnel Vetting Transformation Office, to assist in the execution of the transfer. We have previously reported on the establishment and implementation of the office; see GAO, *Federal Management: Selected Reforms Could Be Strengthened By Following Additional Planning, Communication, and Leadership Practices*, GAO-20-322 (Washington, D.C.: Apr. 23, 2020).

[15]According to Defense Counterintelligence and Security Agency documentation and officials, the work of the Personnel Vetting Transformation Office has since been incorporated into a new Chief Strategy Office, and the former office, as previously known, no longer exists.

[16]Identity intelligence is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. Identity intelligence fuses identity attributes (e.g., biographical, biological, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes to identify and to assess threat actors and networks, among other things. Biometrics contributes to identity intelligence. See Joint Chiefs of Staff, *Identity Activities*, Joint Doctrine Note 2-16 (Aug. 3, 2016), appendix B.

officials stated that they consider certain factors such as the availability of resources (i.e., time, staff, funding) in other components when deciding whether to retain responsibilities within the office or to delegate them to other DOD components. For example, officials said they are planning to transfer the geospatial intelligence component of Project Maven to another DOD component based on such factors. According to Project Maven officials, OUSD(I&S) centralized the Defense Intelligence Enterprise's artificial intelligence effort in Project Maven to more rapidly attain higher levels of technology in data management and algorithm protection and to avoid the costs and challenges of the military services progressing individually on artificial intelligence. In January 2021, USD(I&S)—according to OUSD(I&S) officials—directed Project Maven to begin a period where geospatial-intelligence technology initiatives would transfer to NGA by fiscal year 2023, and non-geospatial intelligence technology initiatives would remain with OUSD(I&S) through fiscal year 2025, unless transferred sooner to another DOD component.[17] Similarly, as previously noted, OUSD(I&S) also gained responsibilities relating to personnel vetting in 2019 and then delegated these functional management duties to the Defense Counterintelligence and Security Agency in 2020.

In June 2018, the Under Secretary highlighted the elevation of defense security as one of his top priorities, including the transformation of personnel vetting to a responsive, risk-based enterprise and the implementation of a comprehensive approach to protect critical technology and infrastructure, mitigate cyber threats, and strengthen industrial security. To give greater emphasis to the importance of the Under Secretary's security responsibilities, Congress subsequently re-designated the position of USD(I) as USD(I&S) in the National Defense Authorization Act for Fiscal Year 2020.[18] According to senior OUSD(I&S) officials, the Under Secretary at the time emphasized security as a "no-

[17]According to Project Maven officials, DOD will assess and score potential components against five criteria to make a delegation decision: mission ownership, technical capabilities, workforce and culture, resources, and security.

[18]*See* Pub. L. No. 116-92, § 1621 (2019). Although the redesignation helps to emphasize the USD(I&S)'s security mission, this provision states that nothing in this section shall be construed to modify or expand the authorities, resources, responsibilities, roles, or missions of the USD(I&S), as redesignated.

fail" mission.[19] In October 2020, the Under Secretary told us that the current global security environment and competition demands greater information security, including information residing with defense contractors, government funded research centers, and information included in academic research. He also emphasized that if DOD does not secure its enterprise, the United States risks losing any conflict it enters.

Internal Organizational Changes

OUSD(I&S) has also made internal organizational changes within its directorates, in part to better align its dual security and intelligence missions under its DDIs, as seen in figure 3 above. In 2018, OUSD(I&S) conducted an assessment of its activities and tasks to determine whether any organizational realignment or structural modifications were needed.[20] Emerging from this assessment, OUSD(I&S) established the DDI(CL&S)—from the previous DDI Intelligence and Security—to bring a tighter focus on security in part by consolidating all authorities and capabilities for security, counterintelligence, and law enforcement into one directorate, according to OUSD(I&S) senior leadership. As part of this process, OUSD(I&S) helped DDI(CL&S) transfer responsibilities unrelated to security and made changes that affected other directorates as well. For example:

- The Human Intelligence and Sensitive Activities office moved from the previous DDI(Intelligence and Security) to DDI(CSP) in part to enable the former to focus more on security and the latter to consolidate intelligence disciplines.
- The Partner Engagement office moved from the previous DDI(Intelligence and Security) to DDI(WS)—and was renamed Commonwealth and Partner Engagement—in part to enable the former to focus more on security.

[19]OUSD(I&S) officials noted this was due in part to the new focus on security in the *2018 National Defense Strategy* and the Under Secretary's belief that the security portfolio is integral to success in all areas of the defense strategy. See DOD, *2018 National Defense Strategy* (2018).

[20]OUSD(I&S) officials referred to this assessment as a "Troop-to-Task" review; it was initiated in January 2018, and senior OUSD(I&S) leadership announced changes emerging from the assessment in late 2018. According to officials, they conducted a review of OUSD(I&S)'s personnel, budget and structure to assess their organization's alignment with OUSD(I&S)'s fundamental mission—guiding and directing the intelligence agencies and setting policies and priorities for the Defense Intelligence Enterprise and the Defense Security Enterprise.

- A Security Program Portfolio within DDI(ISP&R) was established to facilitate a comprehensive approach to managing security programs and resources.
- The Strategy, Policy, and Integration office moved from DDI(ISP&R) to DDI(WS)—and was renamed the Strategy, Policy, and Enterprise Assessment office—to allow the former to focus more on program and budget issues, according to OUSD(I&S) officials.

With these organizational changes and realignment, 3 of the 4 DDIs now focus predominantly on intelligence activities, while DDI(CL&S) predominantly focuses on security activities.[21] For example, DDI(ISP&R) officials reported to us that 27 of the 32 actions, or specific tasks, they take within their directorate to execute their oversight and management responsibilities are intelligence actions rather than security ones. DDI(WS) officials similarly reported that 60 of the 69 actions they take within their directorate are intelligence actions.

Relating to the directorates, we also collected and analyzed data on the number of personnel within each DDI. Our analysis showed that, in July 2020, DDI(WS) had the most personnel—146—of the four DDIs whereas DDI(CL&S) had the least number—73. See table 1 for more details.

Table 1: Number of Personnel Reported in July 2020 in Four Intelligence Directorates

Director for Defense Intelligence (DDI)	Number of personnel
DDI(Warfighter Support)	146
DDI(Collection and Special Programs)	113
DDI(Intelligence and Security Programs and Resources)	79
DDI(Counterintelligence, Law Enforcement, and Security)	73

Source: GAO analysis of Department of Defense information. | GAO-21-295

Note: Personnel reported include assigned government personnel and onsite contractors.

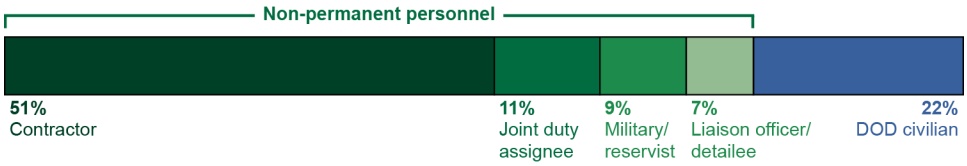
[21]We collected and analyzed workload information for this report from the four DDIs, including their primary oversight and management responsibilities and how these responsibilities break down into specific actions to execute these responsibilities. Two examples of actions reported by the DDIs include: 1) "*Develop and update policy on all aspects of controlled unclassified information*", and 2) "*Host a workshop to develop roadmap for commercial digital ecosystem*." We then asked the DDIs to identify whether these actions are intelligence or security actions.

OUSD(I&S) Has a Workforce Composed Largely of Non-Permanent Personnel

We found that OUSD(I&S) relies largely on non-permanent personnel to fulfill its responsibilities.

According to our analysis, 78 percent of the workforce across the four DDIs in OUSD(I&S) in July 2020 was non-permanent—consisting of contractors, joint duty assignees, military/reservists, and liaison officer or detailees.[22] We focused our analysis on personnel in the DDIs as they comprise around 80 percent of OUSD(I&S)'s workforce and conduct intelligence and security responsibilities.[23] See figure 4 for more details.[24]

Figure 4: Workforce Composition by Employee Type across the Four Intelligence Directorates in July 2020



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-295

[22]For purposes of our report, we refer to non-permanent personnel—personnel who normally only work for a year or several years in an organization before rotating elsewhere or are employed by a contract. Such personnel would include contractors, joint duty assignees, active duty military or reservists, and liaison officers or detailees. Our analysis is based on workforce data, which covered full-time personnel, provided by the four DDIs in July 2020. The Office of the Director of National Intelligence (ODNI) prescribes the guidelines for joint duty assignees as part of the IC Civilian Joint Duty Program. An IC civilian joint duty rotation is defined as (a) the detail of IC civilian personnel to a position in another IC element or other relevant organization that provides an IC civilian joint duty qualifying experience, or (b) the assignment of IC civilian personnel to an approved internal position at the individual's employing element that provides an IC civilian joint duty qualifying experience. One of the requirements of the program is to serve a minimum amount of time for the gaining component so this does not entail a permanent assignment. See Office of the Director of National Intelligence, *Intelligence Community Civilian Joint Duty Program*, IC Directive 660 (Feb. 11, 2013).

[23]OUSD(I&S) reported a total workforce of 514 personnel—excluding offsite contractors—and the four DDIs reported a total workforce of 411 personnel in the same year. The workforce outside the DDIs are part of offices that report directly to USD(I&S) and are responsible for individual functions, such as human capital or congressional activities.

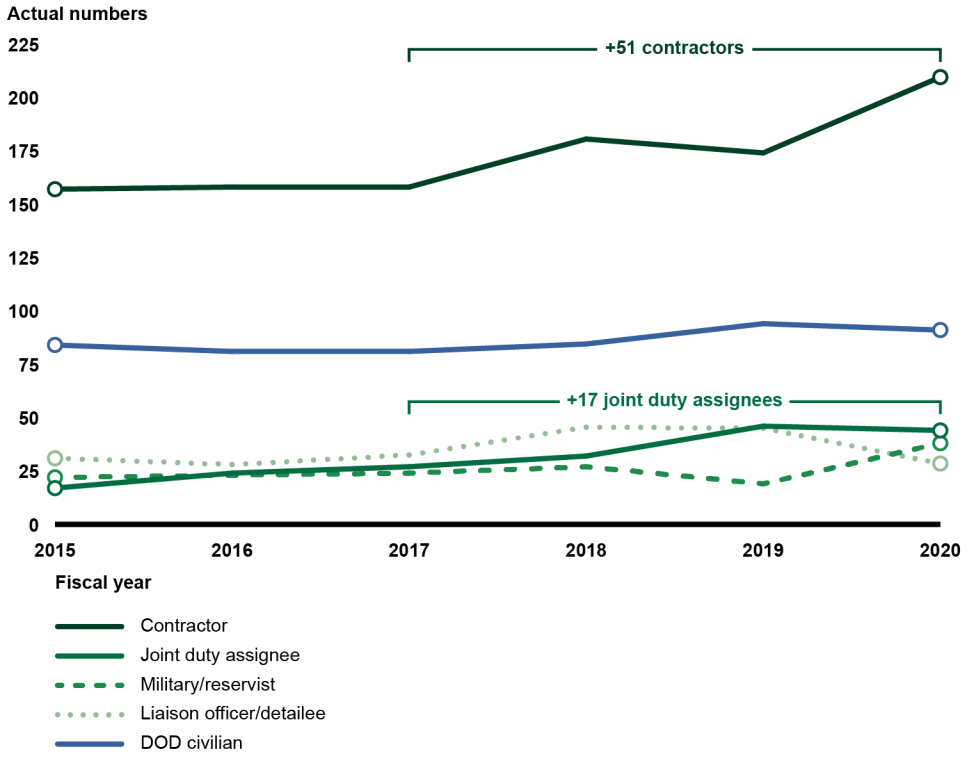
[24]OUSD(I&S) also conducted an assessment in 2019 of its roles and workforce and found similar results. The assessment reported that, in 2017, 76 percent of OUSD(I&S) personnel were contractors, military assignees, and liaison officers or detailees—a proportion of non-permanent personnel similar to the proportion in the fiscal year 2020 workforce that we found. The assessment concluded that the difference between career and temporary employees at OUSD(I&S) is at its highest level since 2004.

About half of the DDI workforce, or 51 percent, is composed of contractors, and nearly a quarter, or 22 percent, is composed of DOD civilians as of July 2020.[25] The remainder of the workforce, over a quarter or 27 percent, consists of non-permanent joint duty assignees, active duty military or reservists, and liaison officers or detailees.

OUSD(I&S) data we collected and analyzed also showed that from fiscal years 2015 through 2017 overall workforce numbers remained relatively flat. However, from fiscal years 2017 through 2020, the number of contractors and joint duty assignees—two categories of non-permanent personnel—increased the most, while the number of DOD civilians increased marginally. Across the four DDIs, from fiscal years 2017 through 2020, OUSD(I&S) added more than 50 contractors, an increase of nearly a third, and added 17 joint duty assignees, or a 63 percent increase (see fig. 5).

[25]Within the four DDIs, the proportion of contractors ranges from 46 to 57 percent; for DOD civilians, the proportion ranges from 18 to 32 percent.

Figure 5: Workforce Numbers by Employee Type across the Four Intelligence Directorates from Fiscal Years 2015 through 2020



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-295

OUSD(I&S) also added 10 DOD civilians, an increase of 12 percent, across the four DDIs from fiscal years 2017 through 2020.

Lastly, OUSD(I&S) officials expressed, and our review of an OUSD(I&S) assessment identified, differing perspectives on the advantages and disadvantages of the office relying on a workforce with a significant proportion of non-permanent personnel. On one hand, OUSD(I&S)'s 2019 assessment concluded that its workforce composition—specifically its reliance on non-permanent personnel—could have a significant adverse effect on institutional knowledge and productivity as a result of

onboarding, training, and turnover.[26] According to senior officials in one DDI, they sought to mitigate their personnel shortfall by using available joint duty assignees and reservist support, but they would have preferred to mitigate some of their staffing challenges with more DOD civilian jobs. Senior officials in another DDI emphasized that their biggest resource challenge is personnel, particularly their limited control over DOD civilian allocation and the time-consuming process of defending their civilian billets on an annual basis.[27] On the other hand, the Under Secretary stated that there is a good balance of temporary to permanent staff in OUSD(I&S) with the institutional knowledge of long-term personnel balanced by newer personnel on rotation. For example, regarding joint duty assignees, the Under Secretary emphasized that these personnel bring unique perspectives into OUSD(I&S) and that when the assignees return to their home agencies they bring back cross-enterprise knowledge and sharing.

OUSD(I&S) Uses Mechanisms to Oversee Enterprises, but Has Not Established Clear Expectations for Oversight or Postured Itself to Assess the Effectiveness of the Enterprises

OUSD(I&S) uses a variety of mechanisms to conduct oversight of the Defense Intelligence Enterprise and the Defense Security Enterprise, including policy development, inspections and governance bodies. However, OUSD(I&S) faces challenges in its oversight of the enterprises in part because it has not established clear expectations for oversight activities, including clarifying key oversight terms. OUSD(I&S) also is not well-postured to assess the effectiveness of the enterprises because it lacks tools to ensure accountability.

[26]We have previously reported on service contracts within the Department of Homeland Security, including concerns with the oversight of contractors, the planning process for contracts, and limited visibility into service contract costs. See GAO, *DHS Service Contracts: Increased Oversight Needed to Reduce the Risk Associated with Contractors Performing Certain Functions*, GAO-20-417 (Washington, D.C.: May 7, 2020).

[27]DDI officials we interviewed stated that OUSD(I&S) is still in a billet reduction mode initiated by former Secretary of Defense Robert Gates in 2013. This process requires that when a government civilian retires or otherwise departs their position, the associated billet goes into a pool for reallocation and their office must defend the billet—a process that is time consuming and creates uncertainty about their billets.

OUSD(I&S) Uses Mechanisms such as Policy Development and Governance Bodies to Conduct Oversight of the Two Enterprises

OUSD(I&S) uses various mechanisms, such as policy development and governance bodies, to conduct oversight of the Defense Intelligence Enterprise and the Defense Security Enterprise and to address responsibilities outlined in its charter. OUSD(I&S) officials stated that there is no single way to conduct oversight of intelligence and security activities. Through our case studies, we identified how the office uses different mechanisms that vary by mission area, dependent on requirements in DOD policy and the decisions of its leadership and staff. These include

- **Policy development.** The USD(I&S) charter delegates authority to OUSD(I&S) to establish policies, which officials told us serves as an essential oversight activity. For example, in June 2019 OUSD(I&S) issued a new DOD policy on publicly available information, which established roles, responsibilities, and definitions for publicly available information.[28] Officials in DDI(CL&S) also stated that in order to address emerging issues, they draft policies and solicit input from the DOD components. In our four case studies, we found that the office had disseminated written guidance to DOD components for specific mission areas (see appendix II for more details).
- **Governance bodies.** OUSD(I&S) leverages governance bodies that enable oversight and share a variety of different names—including councils, committees, working groups, and boards of directors. These generally include participation from OUSD(I&S), the defense agencies, the military services, and the combatant commands. In three of our four case studies, we found that OUSD(I&S) had ensured the relevant participants in the DOD were included for specific mission areas (see appendix II for more details). For example, OUSD(I&S) participates in the Defense Open Source Council, established by DOD policy as the primary governance mechanism for OSINT.[29] Similarly, the DDI(CL&S) serves as chair of the Defense Security Enterprise Executive Committee, the senior-level governance body for security policy coordination.[30] The Defense Security Enterprise Executive Committee is used as a venue to resolve disagreements and to promote communication between different organizations with security

[28]DOD Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)* (June 11, 2019) (incorporating change 1, Aug. 20, 2020).

[29]DOD Instruction 3115.12, *Open Source Intelligence (OSINT*) (Aug. 24, 2010) (incorporating change 2, July 16, 2020).

[30]DOD Directive 5220.43, *Management of the Defense Security Enterprise* (Oct. 1, 2012) (incorporating change 3, July 14, 2020).

responsibilities, according to a DDI(CL&S) official. OUSD(I&S) officials said they conduct oversight by engaging other agency officials at governance bodies established to coordinate DOD efforts on a particular mission.

- **Inspections.** OUSD(I&S) conducts on-site reviews, evaluations, and inspections in some mission areas to determine whether intelligence and security activities are effective and operate in accordance with policy, according to officials. OUSD(I&S) officials stated that they conduct inspections both on their own authority, and by partnering with other DOD organizations. For example, a Senior Intelligence Oversight Official told us that teams of subject-matter experts from OUSD(I&S) accompanied oversight staff to inspect intelligence activities at DOD components.[31] OUSD(I&S) officials reported they provided technical assistance to the then-Senior Intelligence Oversight Official during these inspections for specific mission areas like human intelligence and counterintelligence and conducted their own evaluation of intelligence activities during the visit. In addition, OUSD(I&S), according to officials, has assisted the Joint Staff in reviews of intelligence combat support agencies as part of the Combat Support Agency Review Team process.[32]
- **Review of data and information.** DOD policies require DOD components to submit regular reports or data to OUSD(I&S) for review.[33] OUSD(I&S) officials described making regular requests to

[31]As of January 2021, DOD has re-established the Assistant to the Secretary of Defense for Intelligence Oversight to replace the functions of the previous Senior Intelligence Oversight Official. The Assistant is responsible for conducting independent oversight of all DOD intelligence and intelligence-related activities in order to ensure that these activities comply with federal law, executive orders, presidential directives, IC directives, and DOD policy. This includes conducting administrative investigations into alleged violations of law, inspecting intelligence activities, reviewing oversight reports from DOD components, and reporting any significant or highly sensitive matters to the Secretary of Defense, Deputy Secretary of Defense, Intelligence Oversight Board, and Director of National Intelligence. See DOD Directive 5148.13, *Intelligence Oversight* (Apr. 26, 2017).

[32]Combat support agencies are DOD agencies or activities designated by Congress or the Secretary of Defense to provide combat support or combat service support functions to joint operating forces, in support of combatant commanders executing military operations. Section 193 of Title 10, United States Code requires the Chairman of the Joint Chiefs of Staff to conduct a biennial assessment of each combat support agency's responsiveness and readiness to support operating forces in the event of a war or threat to national security. The combat support agencies under OUSD(I&S) oversight include DIA, the National Security Agency, and NGA; see Chairman of the Joint Chiefs of Staff Instruction 3460.01D, *Combat Support Agency Review Team Assessments* (Sept. 30, 2019).

[33]See DODI 3115.12 and DODD 5220.43.

DOD components for data in order to assist with specific policy and strategic development. For example, in 2019, the Director of National Intelligence directed a study to examine CM modernization, and OUSD(I&S) subsequently requested data from DOD components, according to office officials. After compiling the results, office officials reported that they recommended improvements to CM throughout DOD. OUSD(I&S), according to officials, also collects, reviews, and reports information on sensitive activities to Congress through the Clandestine Quarterly Activities Report.[34]

OUSD(I&S) Has Experienced Challenges with Oversight Because It Has Not Established Clear Expectations

OUSD(I&S) has experienced challenges in its oversight of the enterprises, in part because it has not established clear expectations for oversight to guide officials' efforts, including refining business rules for governance bodies and clarifying key terms critical to oversight. Though the OUSD(I&S) charter identifies oversight as a critical function of the office, with the terms *oversight* or *oversee* appearing more than 60 times in the document, the charter does not clearly describe what oversight should entail. A senior OUSD(I&S) official stated that perspectives on OUSD(I&S)'s oversight role and the oversight activities that it should conduct differ throughout the Defense Intelligence Enterprise. Another senior OUSD(I&S) official also stated that the extent to which OUSD(I&S) conducts oversight over a particular mission and the mechanisms used in doing so are dependent on both leadership and resources.

We observed several oversight challenges within our case studies and interviews with OUSD(I&S) officials due in part to this lack of clarity around expectations, including: governance bodies not operating as intended; insufficient guidance; and unclear roles, responsibilities, and authorities. (See appendix II for more details of the case study analysis, where we assess mission areas against collaboration leading practices for bridging organizational cultures and clarity of roles and responsibility).

Governance bodies not operating as intended. In the CM mission area, we found that the Defense Collection Management Board, designed to function as the CM mission area's governance body, had not met for a number of years. As noted in our case study analysis (see appendix II), this issue links to the collaboration leading practice of bridging

[34]DOD is required by statute to periodically report or brief Congress on various sensitive activities, such as sensitive military operations, sensitive cyber operations, and deployments and collection activities of the Defense Clandestine Service. According to an OUSD(I&S) official, the *Clandestine Quarterly Activities Report* is a compilation of information on sensitive activities and also includes additional information on special access programs.

organizational cultures where working across organizational boundaries is key. In addition, we found that some governance bodies serve as decision-making bodies, whereas others primarily serve to share and coordinate information among the enterprise. OUSD(I&S) officials who had completed an analysis of oversight activities found that OUSD(I&S) had not established clear objectives or expectations for governance bodies, creating the potential for overlapping or duplicative efforts and tasks among each group. The assessment found that, in the absence of clear objectives and business rules, governance bodies carried out varied responsibilities depending on the mission area and operated inconsistently. OUSD(I&S) officials stated they needed to refine business rules for their governance bodies across mission areas and set expectations for these bodies so that they operate as intended.

Insufficient guidance. In the OSINT mission area, OUSD(I&S) officials responsible for overseeing OSINT said they focus their oversight on issuing policy and monitoring compliance with and DOD component implementation of OSINT policies. However, Army officials responsible for OSINT told us that OUSD(I&S)'s recent policy on publicly available information did not meet their needs for more explicit and complete guidance on OSINT. Other DOD OSINT officials noted that more proactive oversight could be provided to ensure the availability of joint tools and compatibility of systems among different DOD components.

In the CM mission area, OUSD(I&S) officials noted that oversight responsibility is shared among three directorates that collaborate on policy, acquisitions, and the specific needs of the combatant commands. However, according to office officials, combatant commands are primarily driving current policy development efforts in CM. For example, OUSD(I&S) officials said that the combatant commands raised CM concerns at a department-wide summit in 2019, and the Joint Staff issued a report recommending that OUSD(I&S) enforce CM standards and revise CM guidance; as a result, OUSD(I&S) began taking steps to improve its oversight of CM, such as directing DIA to revise CM-related guidance. The officials acknowledged that OUSD(I&S) oversight of CM has been insufficient because no individual or directorate within OUSD(I&S) had been assigned overall responsibility for the mission area.

Unclear roles, responsibilities, and authorities. OUSD(I&S) has issued DOD policies to establish roles, responsibilities, and authorities for oversight of intelligence and security mission areas, but key terms in the policies are sometimes unclear and at times applied inconsistently. In two of our four case studies, we found that OUSD(I&S) had not consistently

provided clear roles and responsibilities for mission areas, which links to the collaboration leading practice of clarity of roles and responsibility. For example, DOD policy for OSINT designates DIA as the lead component for OSINT and defines the term in the context of OSINT.[35] The definition of the term also identifies activities DIA may take as the lead component but does not clearly outline the extent of its authority. This creates uncertainty relating to DIA's exercise of its authority for the development of an enterprise approach for the mission area, the employment of standards, and resourcing of OSINT tools, according to DOD officials. As noted in our case study analysis (see appendix II), this issue also links to the collaboration leading practice of bridging organizational cultures where agreement on common terms is important. According to an Indo-Pacific Combatant Command official, OSINT practitioners use different tactics, techniques, tools, and procedures in part because it is not clear whether DIA, as lead component, has the authority to establish binding requirements or to coordinate the purchase of commercial tools and data sets.

Additionally, with regard to the term functional manager, DIA officials stated that DOD policy assigns the DIA Director functional manager roles in different mission areas, but the actual responsibilities and authorities of each of these roles differs in practice despite bearing the same title. As an example, DIA officials compared DIA's role as functional manager for analysis, which is more of an advisory role, to DIA's functional manager role for human intelligence, which has greater authority and is directive in nature. DIA officials noted that each document assigning a functional manager creates a role with its own distinct responsibilities and authorities, which can create confusion about the manager's role since it can vary from one mission area to another.

OUSD(I&S) officials acknowledged that their organization needed to clarify their expectations for oversight, including identifying expectations for governing boards and defining key terms. The *2020 Defense Intelligence Strategy* further highlighted the importance of establishing expectations around oversight, stating that to operate effectively, the enterprise requires a process for conducting oversight of its components

[35]DOD Instruction 3115.12 defines lead component as one that leads collaboration and facilitates coordination within a specific intelligence discipline or set of intelligence activities. The instruction also states that a lead component may also advise on and develop technical architectures, programmatic resources, or performance metrics on behalf of a collective whole.

and programs.[36] The strategy also includes an objective for which OUSD(I&S) has responsibility focused on reforming and modernizing management structures—which entails codifying roles, responsibilities, and authorities—but OUSD(I&S) has not established any detailed plans or timeframes to implement corrective action.

In addition, section 1626 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 required the Secretary of Defense and the Director of National Intelligence to establish a framework that includes a lexicon of relevant terms to ensure that consistent definitions are used and reconciles jointly used definitions in determinations to help ensure that the missions, roles, and functions of the DOD combat support agencies that are also elements of the IC, and other intelligence components of the department, are appropriately balanced and resourced.[37] In response to this direction, OUSD(I&S) produced a report that recognized the need to clarify a list of important terms, but did not produce a lexicon to operationalize this.[38] The report stated that DOD and ODNI still needed to resolve lexical inconsistencies and clarify defense intelligence roles and responsibilities to support enterprise management functions. OUSD(I&S) officials acknowledged this issue, stating that poorly defined terms have constrained the Defense Intelligence Enterprise and the Defense Security Enterprise capacity to change and modernize—limiting the articulation of new standards that would make the enterprises more effective and efficient.

Leading practices for collaboration among government agencies state that participating agencies in an interagency effort—such as the DOD components working together across the enterprises—should establish common outcomes and set expectations for participation. The practices also recommend that participating agencies bridge organizational cultures through the development of shared concepts and terms, and clarify, define, and agree on their roles and responsibilities.[39] Similarly, federal standards for internal control state that an oversight body, like OUSD(I&S), should work with key stakeholders—such as components

[36]DOD, *2020 Defense Intelligence Strategy* (August 2020).

[37]Pub.L. No. 115–232, § 1626 (2018).

[38]DOD and ODNI, *Report on the Framework on Governance, Mission Management, Resourcing, and Effective Oversight of Combat Support Agencies that are also Elements of the Intelligence Community* (August 2019).

[39]GAO-12-1022.

throughout the enterprises—to understand their expectations and help the entity fulfill these expectations if appropriate.

The *2020 Defense Intelligence Strategy* states that the Defense Intelligence Enterprise has yet to fully pivot to address the changing intelligence needs of the department and the nation, and that continued progress must be embraced. Without establishing clear expectations for oversight, including refining business rules for governance bodies and clarifying key terms, OUSD(I&S) risks confusion and potential inaction due to unclear responsibilities and authorities throughout the Defense Intelligence Enterprise and the Defense Security Enterprise. It also cannot ensure that it is focusing its limited resources on the most critical areas, balancing oversight across mission areas, or streamlining how decisions are made as it guides the enterprises.

OUSD(I&S) Is Not Well-Postured to Assess the Effectiveness of the Enterprises

OUSD(I&S) is not well-postured to assess the effectiveness of the intelligence and security enterprises in part because it has not consistently established tools to enhance accountability, such as goals, desired outcomes, and performance metrics to measure progress in specific mission areas. OUSD(I&S) has taken recent action in this area. For example, its *2020 Defense Intelligence Strategy* describes over-arching goals and outcomes for the Defense Intelligence Enterprise for which OUSD(I&S) is accountable, and some broad goals related to certain specific mission areas. For example, the strategy highlights a broad goal—relating to OSINT—to develop an open source strategy and institute an integrated and flexible approach in part to leverage and access publicly available information.

However, OUSD(I&S) lacks detailed goals, outcomes, and metrics to guide the enterprises toward the overall goals listed in the *2020 Defense Intelligence Strategy* or other longer-term priorities. We found in all four case studies that OUSD(I&S) did not identify outcomes or tools that enhance accountability for specific mission areas—tools it could use to conduct oversight. (See appendix II for more details of the case study analysis, where we assess mission areas against the collaboration leading practice for outcomes and accountability). For example,

- **Collection management.** An OUSD(I&S) official stated that they do not currently conduct systematic monitoring, assessment, and evaluation across the CM mission area in part because OUSD(I&S) does not have any performance metrics specific to CM. To begin to address this, OUSD(I&S) has directed the production of a strategy document for the CM mission area that should contain certain high-

level goals, outcomes, and metrics. This work remains in progress and, as of January 2021, the Joint Staff Directorate for Intelligence had not yet produced any specific goals or outcomes with associated metrics for CM.

- **Open Source Intelligence.** Neither OUSD(I&S) nor DIA has developed enterprise goals and metrics, which could drive the collection of useful performance-related OSINT data, according to DIA officials. OUSD(I&S) reviews data on DOD OSINT activities collected by DIA in its role as lead component for OSINT, but these data are limited in their utility. For example, DIA officials responsible for OSINT said they collect only limited information on OSINT resources because lead components do not manage resources. In addition, they stated that data provided in OSINT reports and analysis by components cannot be aggregated because each agency, combatant command, and military service has a slightly different reporting format. NGA officials responsible for OSINT said that it was unclear whether the data collected were useful or utilized. DOD has also acknowledged the need to mature this mission area by directing the development of an open source strategy and the institution of an integrated and flexible approach to leverage and access publicly and commercially available information.[40]
- **Industrial security.** According to OUSD(I&S) officials, they do not conduct systematic monitoring of industrial security activities by the DOD components. While OUSD(I&S) has created priorities for their office operations, it has not provided any short- or long-term outcomes for industrial security programs within the DOD components or established any goals and metrics for the program. OUSD(I&S) officials responsible for industrial security stated that given limited staff resources they instead focus on issuing industrial security policies. While there is a DOD Security Enterprise Strategic Plan—published in 2013—it includes only broad security goals, such as standardizing security functions across DOD to achieve efficient execution and enhance operations, rather than goals or outcomes specific to the industrial security mission area.[41]
- **Counterintelligence.** According to OUSD(I&S) officials responsible for CI, there is ongoing work to develop CI-specific goals, outcomes and performance metrics—as part of a CI strategy—but this work

[40]DOD, *2020 Defense Intelligence Strategy* (August 2020).

[41]Defense Counterintelligence and Security Agency officials—responsible for administering the program—also noted that they do not oversee the actual application of policy by DOD components.

remains in progress. According to DOD components in the CI mission area, DOD lacks a CI strategy and has not had one since at least 2013. OUSD(I&S) officials stated that they directed DIA to coordinate the production of a new strategy, and the effort began in October 2019.

Leading collaboration practices state that interagency efforts need tools to ensure accountability and organizational outcomes.[42] We have found that agencies that leverage tools—such as strategic plans and metrics—to monitor, evaluate, and report the results of collaborative efforts can better identify areas for improvement.[43] In addition, agencies should clearly articulate short- and long-term outcomes.[44]

According to the Under Secretary, OUSD(I&S) needs to ensure that the Defense Intelligence Enterprise and the Defense Security Enterprise are demonstrating progress toward strategic outcomes, are operating effectively, and are using money appropriately.[45] Without developing tools that enhance accountability, such as specific outcomes, goals, and performance metrics for its specific mission areas, and using these tools to conduct oversight, OUSD(I&S) cannot effectively monitor the progress of the Defense Intelligence Enterprise and the Defense Security Enterprise and risks falling short of the objectives of the *2018 National Defense Strategy* and the *2020 Defense Intelligence Strategy*.

Conclusions

The *2020 Defense Intelligence Strategy* stated that the Defense Intelligence Enterprise must be reformed and that the enterprise has yet to fully pivot to address the changing intelligence needs of the department and the nation. Further, OUSD(I&S) has also emphasized the need to elevate the role of defense security in achieving the goals of the *2018 National Defense Strategy*. OUSD(I&S) plays the central role in overseeing and managing the Defense Intelligence Enterprise and Defense Security Enterprise and the many intelligence and security elements within DOD. While OUSD(I&S) has realigned its organization to address new responsibilities in recent years and uses a number of oversight mechanisms, additional oversight actions would position it to effectively guide the enterprises through these challenges. By

[42]GAO-12-1022.

[43]GAO-12-1022.

[44]GAO-12-1022.

[45]We interviewed the USD(I&S) in October 2020 in part to discuss metrics and accountability for intelligence mission areas.

establishing clear expectations for oversight, including refining business rules for governance bodies and clarifying key terms, and developing tools that enhance accountability, OUSD(I&S) can lay a stronger foundation for overseeing and assessing DOD intelligence and security resources. This in turn can result in better meeting the evolving intelligence and security needs of the department and the nation.

Recommendations

The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence and Security establishes clear expectations for oversight, including refining business rules for governance bodies and clarifying key oversight terms. (Recommendation 1)

The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence and Security develops tools to enhance accountability—such as through strategies or other mechanisms with identified goals, desired outcomes, and performance metrics—for specific intelligence and security mission areas and uses these tools to conduct oversight. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD. DOD provided written comments, in which it concurred with our recommendations. DOD's written comments are reprinted in their entirety in appendix III. DOD also provided technical comments, which we incorporated into the report where appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and the Under Secretary of Defense for Intelligence and Security. In addition, the report is available at no charge on the GAO website http://www.gao.gov.

If you or members of your staff have any questions regarding this report, please contact me at (202) 512-5130 or mazanecb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Brian M. Mazanec
Director, Defense Capabilities and Management

List of Committees

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mark Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Jon Tester
Chairman
The Honorable Richard Shelby
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Adam Schiff
Chairman
The Honorable Devin Nunes
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Betty McCollum
Chair
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

To describe how the Office of the Under Secretary of Defense for Intelligence and Security's (OUSD(I&S)) responsibilities and organization have evolved since 2017 and the composition of the OUSD(I&S) workforce to carry out its responsibilities, we collected and analyzed documentation and interviewed officials from the Directors for Defense Intelligence (DDIs) on new responsibilities gained and organizational changes made in OUSD(I&S) in recent years. For example, we reviewed documentation on the 2018 OUSD(I&S) organizational realignment (also known as the Troop to Task Review), the establishment of Project Maven, and the Personnel Vetting Transformation Office to better understand these changes and new responsibilities.[1] We interviewed officials from all four DDIs to understand the context, rationale, and details behind these changes and new responsibilities. DDIs included the following:

- DDI (Warfighter Support, or DDI(WS))
- DDI (Counterintelligence, Law Enforcement, and Security, or DDI(CL&S))
- DDI (Collection and Special Programs, or DDI(CSP))
- DDI (Intelligence and Security Programs and Resources, or DDI(ISP&R))

Additionally, to describe the composition of OUSD(I&S)'s workforce, we focused on personnel in the DDIs as the directorates comprise around 80 percent of OUSD(I&S)'s workforce and conduct intelligence and security responsibilities. We submitted individual data requests to the four DDIs soliciting data on a number of items including oversight responsibilities and related actions, the number of employees conducting specific actions, DDI funding from fiscal years 2015 to 2020, and the DDI allotment of full time employees across several personnel categories—including Department of Defense (DOD) civilians, joint duty assignees, contractors, and military personnel and reservists—in the same fiscal year period. The DOD—as part of the Future Years Defense Program—typically budgets for its programs and costs over a five year period so we requested data over a similar period. We analyzed and compiled this data to understand the relative proportion across the DDIs of different personnel categories and any areas where changes to personnel had occurred. To assess the reliability of these data, we submitted written

[1]See Deputy Secretary of Defense memorandum, *Algorithmic Warfare Cross-Functional Team (AWCFT)*, Directive-type Memorandum-18-002 (Mar. 23, 2018) and Office of the Secretary of Defense, *Charter for the Personnel Vetting Transformation Office (PVTO)* (October 2018).

questions relating to the reliability and accuracy of specific data provided by OUSD(I&S) and cross-checked this analysis with an OUSD(I&S)-conducted assessment in 2019 of its roles and workforce and found similar results. We determined that the data were sufficiently reliable for the purposes of this report. Lastly, we interviewed DDI officials as well as the USD(I&S) to understand their perspectives on the composition of the OUSD(I&S) workforce, particularly the proportion of non-permanent personnel.

To assess how OUSD(I&S) conducts oversight and to what extent it assesses the effectiveness of the defense intelligence and security enterprises, we collected documents and interviewed DOD officials in OUSD(I&S), combatant commands, defense intelligence agencies, and services. See later in this appendix for a full listing of DOD components we interviewed. We first identified through interviews and documents the key mechanisms DOD officials leverage to conduct oversight, including governance bodies and inspections. We then combined a review of DOD issuances, policies, and processes for intelligence and security oversight, and senior leadership interviews with four case studies in the mission areas of collection management (CM), counterintelligence (CI), industrial security, and open source intelligence (OSINT).

We developed four case studies to provide a sample of mission areas that cut across the Defense Intelligence Enterprise and the Defense Security Enterprise. We selected our case studies through a judgmental sample based on recommendations from GAO subject-matter experts and DOD entities with oversight responsibilities.[2] We selected the organizations with whom we conducted our case study interviews to assure sufficient subject matter depth in each mission area. For each case study, we interviewed officials from the responsible OUSD(I&S) directorate, the agency responsible for functional management, and select DOD components also active in each mission area. Each case study included at least one defense agency, military service, geographic combatant command, and functional combatant command. We also included all of the military services, with at least one in each case study. See appendix II for the detailed case study assessments.

As part of the case study analysis, we reviewed mission area-specific documentation and interviewed specific DOD components to examine how OUSD(I&S) oversees intelligence and security activities carried out

[2]We excluded some mission areas based on recent or ongoing GAO work.

by DOD components in specific mission areas. OUSD(I&S) officials reported that they conduct oversight primarily through collaboration with DOD stakeholders and related collaborative mechanisms in order to make policy changes and other adjustments in specific mission areas; thus, we used leading collaboration practices, based on prior work, to inform our assessment of OUSD(I&S)'s oversight. Specifically, we used these leading practices to assess the extent to which they were collaborating in these specific mission areas and collected information on the collaborative mechanisms used by OUSD(I&S).[3] These leading collaboration practices include:

- Outcomes and accountability
- Bridging organizational cultures
- Leadership
- Clarity of roles and responsibilities
- Participants
- Written guidance and agreements

We did not assess OUSD(I&S) oversight against the leading collaboration practice regarding interagency resources due to the security classification of information regarding funding and information systems and a limited ability to review this information following changes in agency operations due to coronavirus disease (COVID-19). See appendix II for details on the questions relating to the leading collaboration practices assessments. The assessments we made in our case studies are not generalizable across the full spectrum of OUSD(I&S) responsibilities, but rather provide examples of how OUSD(I&S) executes its oversight responsibilities in specific mission areas.

Lastly, we compared the information from our case studies and information we collected from our interviews with officials in all four DDIs against relevant laws, *Standards for Internal Control in the Federal Government*, and selected leading collaboration practices based on prior

[3]GAO, *Managing For Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: September 2012) outlines leading collaboration practices. For a list of the DOD stakeholders interviewed for each case study, see later in this appendix.

work.[4] The control environment component of internal control—particularly the principle of exercising oversight responsibility—was significant to this objective. We assessed DOD's implementation of this component by reviewing DOD issuances and interviewing DDI officials. Specifically, federal internal control standards require clear expectations so we assessed through our case studies and DDI interviews whether OUSD(I&S) had established clear expectations for how they would conduct oversight for the intelligence and security enterprises. This included assessing whether key oversight terms were clear and whether oversight bodies operated consistently. We also compared information collected from our case studies and DDI interviews to the leading collaboration practices' emphasis on accountability and clear roles to determine whether OUSD(I&S) had established metrics and definitions for key roles in the enterprises.

DOD Organizations with Whom GAO Conducted Interviews

In support of our work, we interviewed officials from OUSD(I&S), combatant commands, Services, and intelligence agencies listed here. The full list of organizations follows:

- USD(I&S)
- OUSD(I&S)
  - Deputy USD(I&S)
  - Chief of Staff
  - Congressional Activities
  - DDI(WS)
  - DDI(CL&S)
  - DDI(CSP)
  - DDI(ISP&R)
  - Human Capital Management Office
  - Special Access Program Central Office
- DOD Senior Intelligence Oversight Official
- Joint Staff J2 Directorate For Intelligence

[4]See 10 U.S.C. § 137, and GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). We selected leading practices for collaboration based on their relevance from GAO-12-1022, and GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005).

- Combatant Commands
  - Indo-Pacific Command
    - Intelligence, J2X
    - Industrial Security representatives
    - Open Source Intelligence representative
    - Joint Intelligence Operations Center
  - Special Operations Command
    - Counterintelligence Branch
    - Open Source Intelligence Manager
    - J2 Collection Management
- Defense Counterintelligence and Security Agency
- Defense Intelligence Agency
  - Directorate of Operations
  - Open Source Intelligence Integration Center
  - Strategic Planning, Policy, and Performance Management Office
- National Geospatial-Intelligence Agency
  - Counterintelligence Division
  - Industrial Program and Acquisitions Security Program Branch
  - Open Source Collection Operations and Governance Division
  - Strategic Engagement Division
- National Security Agency
- U.S. Air Force
  - Headquarters Air Force Intelligence
  - Air Force Air Combat Command
  - Air Force Headquarters A2/6
  - Office of Special Investigations
- U.S. Army
  - Intelligence and Security Command
  - Army G2

- U.S. Navy
  - Office of the Deputy Under Secretary of the Navy for Policy
  - Naval Criminal Investigative Service
  - Office of the Chief of Naval Operations N2N6I
- U.S. Marine Corps
  - Headquarters Marine Corps Deputy Commandant for Information
  - Marine Corps Intelligence Activity

We conducted this performance audit from July 2019 to May 2021 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. Our original timeline for issuing this report was delayed for several months because of impacts to government and other operations related to COVID-19.

Appendix II: GAO Case Study Analysis

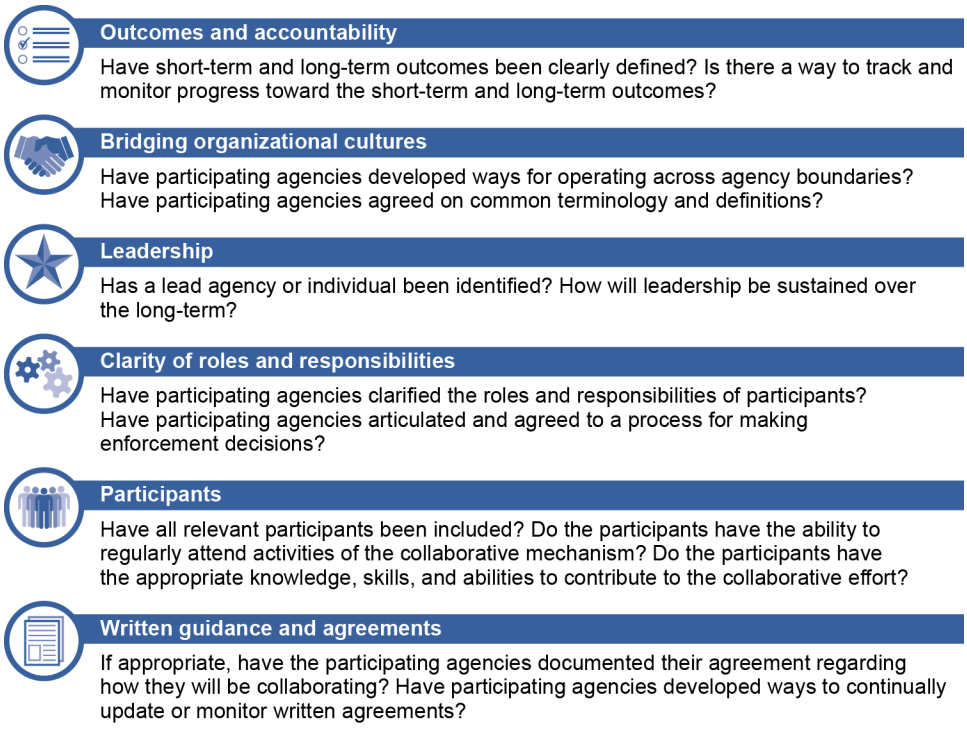
The Under Secretary of Defense for Intelligence and Security (USD(I&S)), and its corresponding office, OUSD(I&S), oversee the Defense Intelligence Enterprise and the Defense Security Enterprise, which consist of multiple components across the Department of Defense (DOD). As noted by senior leadership in OUSD(I&S), the complexity of this structure requires OUSD(I&S) and the DOD components to work collaboratively to oversee and manage DOD's intelligence and security enterprises. Although collaborative mechanisms differ in complexity and scope, our prior work has shown that they all benefit from certain key features, such as leadership, clarity of roles and responsibilities, and written guidance and agreements.[1]

To inform our assessment of OUSD(I&S) oversight over the Defense Intelligence Enterprise and the Defense Security Enterprise, we conducted case studies in four mission areas: counterintelligence (CI), collection management (CM), industrial security, and open source intelligence (OSINT). We examined OUSD(I&S) oversight over each mission area by evaluating whether it had ensured participating components demonstrated and followed leading collaboration practices.[2] See figure 6 below.

[1]GAO, *Managing For Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: September 2012).

[2]GAO-12-1022.

Figure 6: Selected Leading Collaboration Practices



Source: www.gao.gov. | GAO-21-295

Note: We excluded the leading collaboration practice regarding interagency resources due to the classification of the information regarding funding and information systems.

Our assessment used three categories: (1) met, (2) partially met, or (3) not met. We define these categories in the following manner:

1. **Met.** We assessed a leading collaboration practice as "met" if OUSD(I&S) ensured that participating components in the respective mission area—including OUSD(I&S)—demonstrated examples of all, or almost all, considerations associated with the practice.
2. **Partially met.** We assessed a leading collaboration practice as "partially met" if participating components in the mission area demonstrated examples of some, but not all, considerations associated with the practice.
3. **Not met.** We assessed a leading collaboration practice as "not met" if participating components in the mission area did not demonstrate any considerations associated with the practice. This includes instances where OUSD(I&S) had plans to take action consistent with a practice, but had not yet done so during the period of our review.

Table 2 summarizes our assessments for each mission area.

Table 2: GAO Assessments of Four Intelligence and Security Mission Areas against Leading Collaboration Practices

	Counter intelligence	Collection management	Industrial security	Open source intelligence
Outcomes and accountability	○	○	○	○
Bridging organizational cultures	◒	◒	●	◒
Leadership	●	●	●	●
Clarity of roles and responsibilities	●	◒	●	◒
Participants	●	◒	●	●
Written guidance and agreements	●	●	●	●

Legend: ●: Met
◒: Partially met
○: Not met

Source: GAO analysis of Department of Defense information. | GAO-21-295

Counterintelligence (CI)

CI consists of intelligence activities conducted to identify, deceive, exploit, disrupt, and protect against espionage and foreign powers. CI missions include countering espionage and international terrorism; support to force protection; support to the defense critical infrastructure program; and support to research, development, and acquisition. According to joint doctrine, there are both offensive and defensive CI activities that are to be considered whenever US intelligence and national security capabilities are deployed.[3]

Within DOD, OUSD(I&S) holds overall responsibility for CI matters, including developing CI policy, resolving issues among components, and representing the Secretary of Defense in national-level CI bodies. The Director of the Defense Intelligence Agency (DIA) serves as the DOD CI Manager and a central management organization of CI. This includes promulgating CI standards, validating intelligence requirements, providing training within DOD, and recommending strategy and policy changes to USD(I&S). Three of the military services—Army, Navy, and Air Force—provide CI services through their respective military department counterintelligence organizations: Army Counterintelligence, Naval Criminal Investigative Service, and Air Force Office of Special

[3]Chairman of the Joint Chiefs of Staff, Joint Publication 2-0, *Joint Intelligence* (Oct. 22, 2013).

Investigations. These organizations provide CI support to the combatant commands and other DOD components, which may also develop their own CI functions in coordination with their assigned military service CI organization.[4]

We examined OUSD(I&S) oversight of CI by reviewing CI policy documents and interviewing select subject-matter experts across the Defense Intelligence Enterprise and Defense Security Enterprise. Table 3 provides the organizations that we interviewed.

Table 3: Department of Defense Components Interviewed for GAO's Counterintelligence Case Study

Counterintelligence	Under Secretary of Defense for Intelligence and Security Directorate	Counterintelligence, Law Enforcement, and Security
	Functional Manager	Defense Intelligence Agency
	Military Services	Army, Navy, Air Force
	Defense Agencies	National Geospatial-Intelligence Agency
	Combatant Commands	Indo-Pacific Command, Special Operations Command

Source: GAO summary of counterintelligence organizations interviewed. | GAO-21-295

Assessment summary. The CI mission area's participating components consistently demonstrated four out of six leading collaboration practices. CI responsibilities for USD(I&S), DIA, and the DOD components are established in DOD policies, and all stakeholders actively participate in CI activities, according to our analysis. In addition, CI organizations such as the Naval Criminal Investigative Service and Army Counterintelligence have established agreements detailing roles and responsibilities for conducting investigations. However, no goals, outcomes, or metrics have been established for the CI mission area as a whole, and components shared different understandings of key terms such as "DOD Counterintelligence Manager." Table 4 describes our assessments in more detail.

[4]Department of Defense Instruction O-5240.10, *Counterintelligence (CI) in the DoD Components* (Apr. 27, 2020).

Table 4: GAO Assessment of Counterintelligence (CI) Mission Area

Leading collaboration practice	GAO assessment	Explanation
Outcomes and accountability	○	There are no established short- or long-term outcomes, nor any method for tracking progress toward outcomes. According to Defense Intelligence Agency (DIA) officials, a forthcoming Defense CI Strategy and accompanying implementation guidance will establish goals and metrics, but this effort has not yet been completed.
Bridging organizational cultures	◒	Key terms have been documented in Department of Defense (DOD) policy, but components did not consistently agree or express understanding of defined terms in practice, such as Command Counterintelligence Coordinating Authority where each command that we spoke to views the position's duties differently.
Leadership	●	DOD CI policy establishes the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) as the focal point for CI activities in the DOD components, and names DIA as the DOD CI Manager.
Clarity of roles and responsibilities	●	DOD has established a collaborative leadership model, clarified roles and responsibilities for OUSD(I&S), DIA, the military services, combatant commands, and other DOD organizations. In addition, DOD policy states that the Under Secretary of Defense for Intelligence and Security is the ultimate decision-making authority for resolving issues among DOD components for CI.
Participants	●	Relevant DOD components participate in the CI mission area and its relevant governance bodies and conduct CI activities.
Written guidance and agreements	●	DOD policy assigns the military CI organizations cognizant authority and responsibility for CI in specific DOD components. The military services and the components have created memoranda of agreement documenting roles and responsibilities.

Legend: ● Met ◒ Partially Met ○ Not Met

Source: GAO analysis of DOD information. | GAO-21-295

Collection Management (CM)

CM is the process of converting intelligence requirements into collection requirements. CM requires establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Within DOD, DIA serves as the Defense Collection Manager, but the agency has delegated key CM responsibilities—including strategic planning, policy development, and resource requirements—to the Joint Chiefs of Staff, Director for Intelligence, J2, as the Deputy Defense Collection Manager and the Functional Manager for Collection Management. In policy, all three organizations are to collaborate through the Defense Collection Management Board.

We examined OUSD(I&S) oversight of CM by reviewing CM policy documents and interviewing select subject-matter experts across the Defense Intelligence Enterprise and Defense Security Enterprise. Table 5

provides the organizations that we contacted and interviewed, or from whom we received written responses.

Table 5: Department of Defense Components Interviewed for GAO's Collection Management Case Study

Collection Management	Office of the Under Secretary of Defense for Intelligence and Security Directorates	Collection and Special Programs; Warfighter Support; Intelligence and Security Programs and Resources
	Functional Manager	Defense Intelligence Agency / Joint Staff
	Military Services	Air Force
	Defense Agencies	National Geospatial-Intelligence Agency, National Security Agency
	Combatant Commands	Indo-Pacific Command, Special Operations Command

Source: GAO summary of organizations interviewed. | GAO-21-295

Assessment summary. Participating agencies in the CM mission area consistently demonstrated two of the six leading collaboration practices. DOD's CM stakeholders have written policies establishing a shared leadership structure, and OUSD(I&S) follows DOD's standard policy update process. However, the mission area lacks desired outcomes with associated metrics for accountability. Additionally, the Defense Collection Management Board—the primary forum established for coordination and collaboration across the enterprise—does not meet regularly, and there is no formal process for making and enforcing mission area decisions. Table 6 describes our assessments in more detail.

Table 6: GAO Assessment of Collection Management (CM) Mission Area

Leading collaboration practice	GAO assessment	Explanation
Outcomes and accountability	○	The documents governing the mission area do not currently include short- or long-term outcomes, nor metrics tied to outcomes tracking performance and accountability. The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) has directed Joint Staff to produce strategy documents that contain outcomes, but this work remains ongoing.
Bridging organizational cultures	◒	The Defense Collection Management Board, the primary forum established for coordination and collaboration across the mission area, had not met in a number of years.
Leadership	●	Department of Defense (DOD) CM policy establishes the shared leadership structure in this mission area.
Clarity of roles and responsibilities	◒	DOD has established roles and responsibilities for the CM mission area, but has not established a process for making and enforcing enterprise decisions.
Participants	◒	In policy, DOD includes all relevant participants in the collaborative oversight process. However, in practice, all relevant stakeholders are not brought together in a single forum because the Defense CM Board—the primary forum established in policy for coordinating activities and resolving issues related to DOD CM—does not meet. OUSD(I&S) has identified this as a problem and directed Joint Staff to stand up this forum.
Written guidance and agreements	●	DOD policy provides guidance to OUSD(I&S), the Defense Intelligence Agency, and DOD components, and DOD has a standard policy document update process, which CM stakeholders and OUSD(I&S) follow.

Legend: ● Met ◒ Partially Met ○ Not Met

Source: GAO analysis of DOD information. | GAO-21-295

Industrial Security

Industrial security refers to safeguarding classified information that is released to contractors, licensees, and grantees of the United States government. Established by executive order, the National Industrial Security Program serves as a single, integrated security program to protect this classified information while addressing economic and technological interests. The Secretary of Defense serves as the Executive Agent for the program and is responsible for issuing authoritative guidance to cleared contractors. By DOD policy, USD(I&S) is assigned the responsibility to oversee, manage, and issue operating standards and policy. The Defense Counterintelligence and Security Agency administers the program—including investigating contractors, personnel, and facilities and certifying access to classified information—and DOD components are responsible for including the appropriate clauses in contracts requiring access to classified information.

We examined OUSD(I&S) oversight of industrial security by reviewing relevant policy documents, strategies, and interviewing select subject-

matter experts from the Defense Counterintelligence and Security Agency, the military services, combatant commands, and defense agencies. Table 7 provides the organizations which we contacted and interviewed, or from whom we received written responses.

Table 7: Department of Defense Components Interviewed for GAO's Industrial Security Case Study

Industrial Security	Office of the Under Secretary of Defense for Intelligence and Security Directorate	Counterintelligence, Law Enforcement, and Security
	Functional Manager	Defense Counterintelligence and Security Agency
	Military Services	Army, Navy
	Defense Agencies	National Geospatial-Intelligence Agency
	Combatant Commands	Indo-Pacific Command, Special Operations Command

Source: GAO summary of organizations interviewed. | GAO-21-295

Assessment summary. Participating components in the industrial security mission area consistently demonstrated five of six leading collaboration practices. Specifically these included the bridging organizational cultures, leadership, roles and responsibilities, participants, and written guidance and agreements practices. However, OUSD(I&S) has not established any short- and long-term goals nor metrics for industrial security, in part because, according to OUSD(I&S) officials, they primarily work on policy updates, such as changes to the operating manual. Director for Defense Intelligence Counterintelligence, Law Enforcement, and Security (DDI(CL&S)) officials said that OUSD(I&S) has oversight of industrial security implementation, but does not have the personnel resources that would allow oversight activities beyond policy development.[5] Defense Counterintelligence and Security Agency officials agreed that OUSD(I&S) oversees the application of industrial security by DOD components, while their agency oversees private industry whose government contracts require access to classified information. Table 8 describes our assessments in more detail.

[5]OUSD(I&S) officials stated there were 2 full-time employees responsible for industrial security: one civilian employee and one Defense Counterintelligence and Security Agency employee on a joint-duty assignment.

Table 8: GAO Assessment of Industrial Security Mission Area

Leading collaboration practice	GAO assessment	Explanation
Outcomes and accountability	○	The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) has not established any short- or long-term outcomes nor metrics for industrial security nor are there strategies or plans currently in progress to address desired outcomes and accountability.
Bridging organizational cultures	●	Department of Defense (DOD) components routinely participate in meetings of the National Industrial Security Program Advisory Committee, or resolve questions and issues by contacting OUSD(I&S) personnel. Officials from components we interviewed stated that key terms for industrial security were clearly defined in policy and demonstrated a common understanding of terms and responsibilities.
Leadership	●	Interagency leadership for industrial security has been clearly established by presidential and national-level directives, such as Executive Order 12829.[a]
Clarity of roles and responsibilities	●	Roles and responsibilities are assigned in national- and department-level policy. Officials from components we interviewed expressed a shared understanding of organizational roles for overseeing, managing, and implementing industrial security policy. In addition, OUSD(I&S) has published DOD policy specifically delineating responsibilities and procedures for DOD components, in addition to national policy such as the National Industrial Security Program Operating Manual.
Participants	●	Both the national and department governance bodies include representatives of DOD components. In addition, meetings are regularly attended by senior DOD officials responsible for industrial security.
Written guidance and agreements	●	The activities of the National Industrial Security Program Advisory Committee are established in Executive Order 12829 and approved by the Director of the Information Security Oversight Office. According to OUSD(I&S) officials, the office has entered into agreements with non-DOD agencies (currently 33) to provide industrial security services, and the Defense Counterintelligence and Security Agency provides oversight of the contractors with access to classified information for those non-DOD agencies based on those interagency agreements.

Legend: ● Met ◒ Partially Met ○ Not Met

Source: GAO analysis of DOD information. | GAO-21-295

[a]Executive Order 12829 establishes the National Industrial Security Program, establishes requirements for government contractors, grantees, and licensees who require access to classified information or facilities, and assigns responsibilities for the program to several government agencies including the National Security Council, the National Archives and Records Administration, and DOD. Exec. Order No. 12829, *National Industrial Security Program*, 58 Fed. Reg. 3479 (Jan. 6, 1993) as amended by Exec. Order No. 13691, *Promoting Private Sector Cybersecurity Information Sharing*, 80 Fed. Reg. 9349 (Feb. 13, 2015).

Open Source Intelligence (OSINT)

OSINT is relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. OSINT complements the other intelligence disciplines and can be used to fill intelligence gaps. Within DOD, responsibility for OSINT oversight is shared between

OUSD(I&S) and DIA. OUSD(I&S) is responsible for providing oversight and direction of Defense OSINT capabilities, policies, plans, and programs, and DIA is the DOD Lead Component on OSINT. DIA and OUSD(I&S) coordinate guidance and procedures for DOD OSINT through the DOD Open Source Council—the primary governance mechanism for OSINT in DOD.

We examined OUSD(I&S) oversight of OSINT by reviewing relevant policy documents and interviewing select subject-matter experts across the Defense Intelligence Enterprise and Defense Security Enterprise. Table 9 provides the organizations that we interviewed.

Table 9: Department of Defense (DOD) Components Interviewed for GAO's Open Source Intelligence Case Study

Open Source Intelligence	Office of the Under Secretary of Defense for Intelligence and Security Directorate	Collection and Special Programs
	Lead DOD Component	Defense Intelligence Agency
	Military Services	Army, Marine Corps
	Defense Agencies	National Geospatial-Intelligence Agency
	Combatant Commands	Indo–Pacific Command, Special Operations Command

Source: GAO summary of organizations interviewed. | GAO-21-295

Assessment summary. Participating components in the OSINT mission area consistently demonstrated three of the six leading collaboration practices. OUSD(I&S) has established in policy a mechanism for how DOD OSINT components will collaborate, garner participation by DOD OSINT components, and follow the DOD policy update process. However, the OSINT mission area lacks defined outcomes with associated metrics for accountability and, according to DOD officials, could benefit from additional formalization and standardization of terminology and key definitions. This includes further clarification of leadership authorities, roles, and responsibilities. Table 10 describes our assessments in more detail.

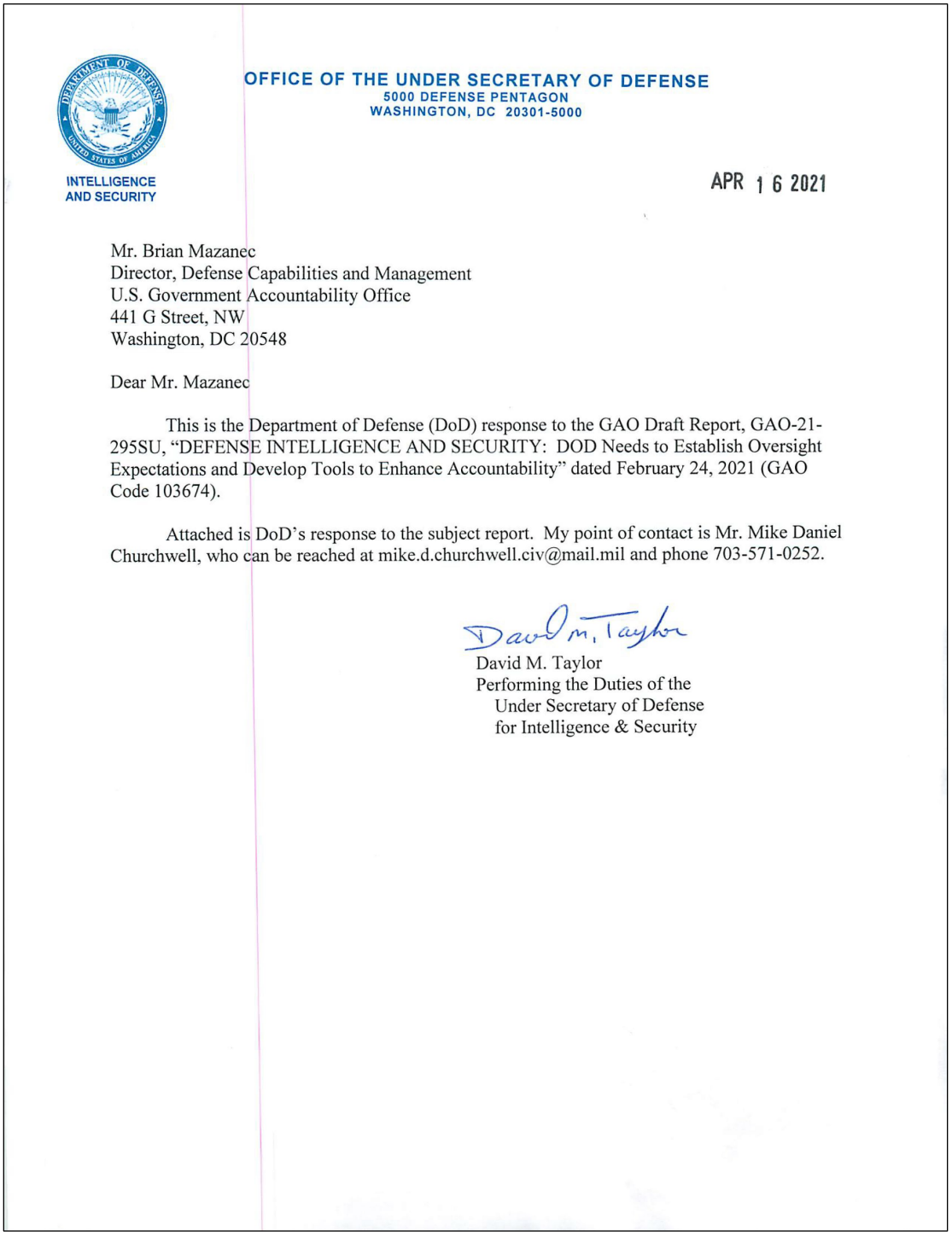
Table 10: GAO Assessment of Open Source Intelligence (OSINT) Mission Area

Leading collaboration practice	GAO assessment	Explanation
Outcomes and accountability	○	The documents governing the OSINT mission area do not currently include short- or long-term outcomes, nor metrics tied to outcomes tracking performance and accountability.
Bridging organizational cultures	◒	The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) has established roles and responsibilities for working across agency boundaries, primarily via the Department of Defense (DOD) Open Source Council. However, key OSINT roles—such as the role of the Defense Intelligence Agency (DIA) as lead component—need to be formalized and standardized, according to DOD OSINT stakeholders.
Leadership	●	According to DOD policy, OUSD(I&S) and DIA share leadership responsibilities for OSINT.
Clarity of roles and responsibilities	◒	Though DOD policy establishes roles and responsibilities for OSINT, in practice roles and responsibilities are not clear to OSINT components. DOD components stated that DIA's OSINT authorities and responsibilities to set OSINT standards and requirements are unclear and not well understood.
Participants	●	DOD policy establishes a structure to include all relevant OSINT participants. This structure consists of the DOD Open Source Council and various associated subcommittees, and working groups.
Written guidance and agreements	●	DOD policy assigns specific roles and responsibilities to OUSD(I&S), DIA, and DOD components, and DOD has a standard policy document update process, which OSINT stakeholders and OUSD(I&S) follow. OUSD(I&S) officials also write interim OSINT guidance in time-sensitive situations.

Legend: ● Met ◒ Partially Met ○ Not Met

Source: GAO analysis of DOD information. | GAO-21-295

Appendix III: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE
AND SECURITY

APR 16 2021

Mr. Brian Mazanec
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Mazanec

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-21-295SU, "DEFENSE INTELLIGENCE AND SECURITY: DOD Needs to Establish Oversight Expectations and Develop Tools to Enhance Accountability" dated February 24, 2021 (GAO Code 103674).

Attached is DoD's response to the subject report. My point of contact is Mr. Mike Daniel Churchwell, who can be reached at mike.d.churchwell.civ@mail.mil and phone 703-571-0252.

David M. Taylor
Performing the Duties of the
Under Secretary of Defense
for Intelligence & Security

GAO Draft Report Dated February 24, 2021

GAO-21-295SU (GAO CODE 103674)

"DEFENSE INTELLIGENCE AND SECURITY: DOD NEEDS TO ESTABLISH OVERSIGHT EXPECTATIONS AND DEVELOP TOOLS TO ENHANCE ACCOUNTABILITY"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence and Security establishes clear expectations for oversight, including refining business rules for governance bodies and clarifying key oversight terms.

DoD RESPONSE: The Department concurs. The Department is committed to improving its oversight performance through refined governance approaches, including the development and adoption of a common lexicon for jointly used definitions with the Office of the Director of National Intelligence. The GAO findings provide objective input that will assist the Department as it revises the applicable governance frameworks and established business rules for the oversight bodies assessed in this report.

RECOMMENDATION 2: The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence and Security develops tools to enhance accountability - such as through strategies or other mechanisms with identified goals, desired outcomes, and performance metrics - for specific intelligence and security mission areas and use these tools to conduct oversight.

DoD RESPONSE: The Department concurs, and has already begun developing new methodologies and metrics for evaluating the performance of the Defense Intelligence and Security Enterprises, and their effectiveness in achieving National Defense Strategy objectives.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Brian M. Mazanec, (202) 512-5130 or mazanecb@gao.gov.

Staff Acknowledgments

In addition to the contact named above, key contributors to this report were Kasea Hamar, Assistant Director; Robert Breitbeil, Analyst-in-Charge; Tracy Barnes; Benjamin Emmel; Christopher Gezon; Chad Hinsch; Lori Kmetz; Joanne Landesman; Kirsten Lauber; Clarice Ransom; Eli Stiefel; Christopher Turner; and Sarah Veale.

Related GAO Products

DHS Service Contracts: Increased Oversight Needed to Reduce the Risk Associated with Contractors Performing Certain Functions. GAO-20-417. Washington, D.C.: May 7, 2020.

Federal Management: Selected Reforms Could Be Strengthened By Following Additional Planning, Communication, and Leadership Practices. GAO-20-322. Washington, D.C.: April 23, 2020.

Standards for Internal Control in the Federal Government. GAO-14-704G. Washington, D.C.: September 2014.

Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms. GAO-12-1022. Washington, D.C.: September 27, 2012.

Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies. GAO-06-15. Washington, D.C.: October 21, 2005.

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/fraudnet/fraudnet.htm

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